SIGNATURE AND AUTHENTICATION CA NC Certification Authority: Terms and Conditions for Certificates

version v1.5, 18/04/2018, Réf. : MPKIG045, Public

1. INTRODUCTION

The present document is the almerys public “PKI Disclosure statement” (PDS) for the « ALMERYS SIGNATURE AND AUTHENTICATION CA NC ». Throughout this document, the use of the term “PDS” refers to the present document, unless otherwise specified.

The purpose of the PDS is to:

- summaries the key points of the CPs and CPS for the benefit of Subscribers and Relying Parties
- Provide additional detail and further provisions that apply to the CPs.

2. TSP CONTACT INFO

Gouvernance IGC be-ys
be-ys marque déposée groupe be-invest, et g2s
almerys Groupe g2s – 46 rue du Ressort – 63967 CLERMONT-FERRAND CEDEX 9 FRANCE
Téléphone : +334 73 74 82 98
gouvernance.igc@be-ys.com

The Certificate Holder has no direct access to the revocation service. For revoking a certificate, he or she shall either:

➔ Contact the Registration Authority by visiting its agency, or by phone. In this case, the Registration Authority will identify the Holder if it has the means to do it or will revoke the concerned certificate;

➔ Contact the support center identified by the corresponding Client, or almerys support by phone: +33-825-306-015 (schedule: 9:00 am - 12:00 pm / 1:30 pm -5:30 pm). In this case, the support center will identify the Holder, if it has the means to revoke the Certificate, or shall transmit the application to the corresponding Registration Authority;

➔ Use the registry service revocation requests available online 24/7 at http://pki.almerys.com/revoquer.html. Revocation Authentication applications are handled via an OTP code.

3. CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGE

Certificates issued by ALMERYS SIGNATURE AND AUTHENTICATION CA NC are certificates aiming at

- Signature and Authentication of natural person.
- Remote signature of natural person.
- eSeal creation by an Organization
- Time-stamps generation by Almerys qualified time-stamping service

Certificate Family	**Issued to the public**	**OID**	**Short Description**
Qualified Electronic Signature (for Natural Persons).	yes	1.3.6.1.4.1.48620.41.1.7.3.1.1.1	Qualified electronic signature Certificates in accordance with eIDAS European Regulation. The certificates are issued in conformity with ETSI EN 319411-2 and are issued on a QSCD Hardware Token with creation of the keys by the CSP, 2048 bit key size and with maximal three (3) years validity, and with a key usage limited to the support of qualified electronic signature.
NCP+ Authentication	yes	1.3.6.1.4.1.48620.41.1.7.3.1.2.1	ETSI TS 319 411-1 NCP+ Certificate on QSCD Hardware token with creation of the keys by the CSP, 2048-bit key size and three (3) years validity, and with a key usage limited to authentication purpose.
Remote Signature	yes	1.3.6.1.4.1.48620.41.1.7.3.1.3.1	ETSI TS 319 411-2 QCP-n Certificate with creation of the keys on a remote service, 2048-bit key size and three (3) years validity, and with a key usage limited to signature purpose.

Certificate Family	Issued to the public	OID	Short Description
eSeal	yes	1.3.6.1.4.1.48620.41.1.7.3.1.4.1	ETSI TS 319 411-2 QCP-l Certificate with creation of the keys on a remote service, 2048-bit key size and three (3) years validity, and with a key usage limited to eSeal creation purpose.
Time-stamping unit	No	1.3.6.1.4.1.48620.41.1.7.3.1.5.1	ETSI TS 319 411-2 QCP-l Certificate with creation of the keys on HSM, 2048-bit key size and three (3) years validity, and with a key usage limited to Time-stamp creation purpose.

4. RELIANCE LIMIT

Certificates issued by ALMERYS SIGNATURE AND AUTHENTICATION CA NC CA may only be used for the respective purposes defined in the above section.

Certificates are issued for a maximum period of 3 years.

These Certificates are not usable beyond their period of validity;

The Almerys CA keeps registration data and event logs for at least five years.

5. OBLIGATION OF SUBSCRIBERS

Certificate holders are responsible for the accuracy of the information they provide during their relationship with Almerys. They especially must:

- Provide accurate and up-to-date information upon Certificate request or renewal,
- Meet face-to-face with the Registration Authority to verify their ID information,
- Securely manage the secrets and elements which are handed over to them at the end of certificate generating procedures, in particular the Holder shall keep its private key under its sole control,
- Accept conditions of usage of the key and corresponding certificate,
- Inform the RA of any changes concerning the information contained in their Certificate,
- Submit, without delay, an application for certificate revocation to the RA in the event of loss, or suspected compromise of their private key (or activation data).

6. CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES:

Third Party Applications using certificates shall:

- Verify that the key usage for which the Certificate was issue is appropriate for its certificate usage;
- Verify that the used Certificate has been issued by the CA ALMERYS SIGNATURE AND AUTHENTICATION CA NC ;
- Verify the download access to the list of revoked certificates (CRL) of ALMERYS SIGNATURE AND AUTHENTICATION CA NC ;
- Verify the Certificate signature, and the Certification chain, up to the "ALMERYS ROOT CA" Certificate and check the validity of each certificate with respect to the CRL of each involved CA.

The certification chain Certificates of the CAs ALMERYS SIGNATURE AND AUTHENTICATION CA NC and « ALMERYS ROOT CA are available at the following address : http://pki.almerys.com

7. LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY:

Subject to the provisions of applicable law and Regulations, ALMERYS SIGNATURE AND AUTHENTICATION CA NC CA is not responsible for any unauthorized use of certificate or misusage of Certificates. This limit of responsibility is also applicable for the activation data, CRL and any software or hardware provided by the CA.

Almerys is, particularly, not responsible for any damage resulting of:

- ➔ The use of a key pair for another usage than the one agreed;
- ➔ The use of expired certificates ;
- ➔ « Force majeure » as defined in the French Law.

ALMERYS SIGNATURE AND AUTHENTICATION CA NC CA is also not responsible for any damage resulting from errors or inaccuracies in the information contained in Certificates, where these errors or inaccuracies result directly from the erroneous nature of the information provided.

Almerys subscribes to a professional insurance service covering the services of electronic certification services.

8. APPLICABLE AGREEMENTS, CPS, CP

See Section 3, which provide the list of applicable CP.

9. PRIVACY POLICY

Any collection and processing of personal data relating to the Holder is carried out in strict compliance according the European General Data Protection Regulation (EU) 2016/679 (the "GDPR"), and with the applicable law and regulations, and in particular Law n° 78-17 January 6th 1978 related to IT System processing personal data and Freedom, modified by the law n° 2004-801 of August 6th 2004, (known as « Loi Informatique et Liberté »)

10. REFUND POLICY

No refund will be made.

11. APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

These Terms & Conditions are governed by French law.

The parties shall endeavor to amicably settle any dispute concerning the interpretation or execution of the contract as soon as possible. In the absence of conciliation, any dispute concerning the validity, interpretation or execution of the present Terms & Conditions will be submitted to the qualified courts of Clermont-Ferrand.

12. TSP AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT

With regard to the provision of Qualified Signature and Authentication Certificate, TSU Certificates, Remote Signature Certificate and eSeal Signature Certificates, Almerys acting as TSP through its Qualified CA operates:

- Following the terms of the eIDAS Regulation,
- According to the ETSI EN 319 411-1 and ETSI EN 319 411-2,
- According to its Certification Policy identified by the OID 1.3.6.1.4.1.48620.41.1.7.3.1

A conformity assessment ALMERYS SIGNATURE AND AUTHENTICATION CA NC to the applicable CP and CPS may be carried out at the request of the Almerys PKI Governance Authority.

The GE ensures that such conformity assessment is performed at least once every 3 years.

On the other hand, from the date of certification, as part of the ETSI EN 319 401 and ETSI 319 411 certification, an assurance and compliance audit will be carried out annually by the accredited conformity assessment body LSTI.