CERTIFICATES ISSUED BY « CERTIGNA ENTITY CODE SIGNING CA »

1. OBJECT

The purpose of these conditions is to specify modalities of request and use of a « Certigna Entity Code Signing CA » certificate, proposed to a future Certificate Manager and/or a Certificate Manager (CM), as well as the respective commitments and obligations of the related parties. The Terms and conditions arise from the Certification Policy identified by the 1.2.250.1.177.2.8.1 OID available at the address: http://politique.certigna.fr/PCcertignaentitycsca.pdf. Certificates covered by this Certificate Policy and these Terms and conditions have the following OIDs:

Seal for code signing	level *	: 1.2.250.1.177.2.8.1.1.1
Seal for code signing	level **	: 1.2.250.1.177.2.8.1.2.1

2. DEFINITIONS

- **CA**: « Certigna Entity Code Signing CA » Certification Authority of the DHIMYOTIS company, issuing the CERTIFICATE;
- **ROOT CA**: Higher level Authority of the Certigna PKI which certifies the CAs;
- **ISSUING CA**: Authority whom the certificate has been signed by the ROOT CA. The CA is an ISSUING CA in the Certigna PKI;
- **RA**: Registration Authority of DHIMYOTIS company controlling certificate requests and eventually revocation requests;
- **DELEGATED REGISTRATION AUTHORITY (DRA)**: Third party external to the PKI with which DHIMYOTIS has concluded a delegation contract by which it subcontracts part of the RA activity, namely, the collection and control of certificate requests, identification of certificate requesters and the submission of revocation requests;
- **CERTIFICATE**: Electronic certificate constituted of a file of electronic data signed, conforming to X.509 v3 standard, containing SEAL service information for which the CM is responsible;
- **CERTIFICATE REQUEST**: Set consisting of the request form (accepting the present General conditions of use) accompanied by the evidence documents, and the request generated by computer;
- **CERTIFICATION AGENT**: Person designated and placed under the responsibility of the Client entity. It is in direct contact with the RA and ensures for it a certain number of verifications concerning the identity, possibly the attributes of the CM and of the SEAL service of this entity.
- **CERTIFICATE MANAGER (CM)**: Natural person in charge and responsible for the electronic certificate and the associate private key used by a SEAL service.
- **CONTRACT**: Relations between the CA and the CM;
- **CRYPTOGRAPHIC DEVICE**: USB key, smart card or cryptographic module;
- **REVOCATION**: Operation consisting in anticipating the end of validity of a CERTIFICATE initially foreseen and the date of which is recorded in the CERTIFICATE;
- **SEAL**: Data in electronic form which is logically associated with other data in electronic form to ensure the origin and integrity of the data;
- **USER**: Certificate user. It can be:
  - A user recipient of signed data by a seal application service that uses the electronic seal certificate and a seal verification module to authenticate the origin of the transmitted data.
  - An application service recipient of data from another application service and which uses the electronic seal certificate and a seal verification module to authenticate the origin of the transmitted data.
  - An application service which signs electronic data.

3. COMPLIANCE

THE CERTIFICATE is issued in compliance with:

- the CP « *Certificats électroniques de Services Applicatifs* » for a seal usage at the levels * and ** of the « Référentiel Général de Sécurité » (RGS) developed by the National Agency for the information systems security (ANSSI);
- The eIDAS Regulation (EU) N°910/2014 at the ETSI EN 319 411-1 LCP level and EN 319 411-2 QCP-l-qscd level;
- The requirements of the document « *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates* » from CA/BROWSER FORUM.

4. DURATION

The CONTRACT is concluded for a period chosen by the future CM (maximum 3 years) and starts the day of the CERTIFICATE issuance by the RA.

5. PRICE

Except with the prior written agreement of the CA, the pricing and payment conditions are as follows:

- The selling price of the CERTIFICATE is that defined in the price schedule available on request from the sales department of Certigna,
- The selling price of the CERTIFICATE must be paid at the CERTIFICATE REQUEST with one of the following means of payment:
  - credit card on the site https://certigna.fr;
  - bank transfer, attaching the receipt provided by the bank;
  - check payable to DHIMYOTIS,
  - cash for any amount not exceeding € 1000;
  - administrative order, for public institutions only, by attaching a purchase order on behalf of the Institution.
- REGENERATION of a software CERTIFICATE is free of charge during the 3 months following the issuance of the CERTIFICATE by the CA;
- UNBLOCKING of the CRYPTOGRAPHIC DEVICE in which the CERTIFICATE is eventually provided is invoiced;

Except with the prior written agreement of the CA, any CERTIFICATE whose sale price has not been paid in full may, either not be issued, or revoked after its issuance by the CA. In accordance to article L.441-6 of the French Commercial Code, in case of non-payment at the due date indicated on the invoice, without obligation to send a reminder, penalties will be applied for delay calculated on rate of 3 times the statutory interest rate in force on the due date of the invoice, and a lump sum indemnity of € 40 for collection charges.

6. OBLIGATIONS OF CERTIFICATE MANAGER

The CM has the following obligations:

- Request the CERTIFICATE by following all procedure steps provided on the website: https://www.certigna.fr.
- Provide accurate and up-to-date information during the request or renewal of the CERTIFICATE;
- Send to RA, if applicable to the DRA or to a Certification Agent of the entity, by hand or by post, the registration form generated at the time of the CERTIFICATE request online on the website: https://www.certigna.fr, the payment, as well as the evidence documents.
- Generate the key pair associated with the CERTIFICATE in a device or CRYPTOGRAPHIC DEVICE meeting the requirements of Chapter 11 of the Associated Certification Policy and with the following qualifications:
  - For seal level **, the CRYPTOGRAPHIC DEVICE is “QSealCD” qualified by ANSSI; In the event that the device is managed by a Trust Service Provider other than Certigna, the Certificate Manager must provide at the certificate request, the evidences (E.g: Certificate of qualification as a Certification Operator, certificate of qualification in as PSCE for the QCP-l-QSCD level and associated signed contractual agreement between the entity and that service provider, etc.) certifying that the provider is able to meet the requirements of the Certification Policy and in particular Chapter 11.
  - For seal level *, the CRYPTOGRAPHIC DEVICE is:
    - Either a hardware device as a smart card or a cryptographic module qualified by ANSSI.
    - Or a software solution complying with the requirements of chapter 11.1 of the associated Certification Policy via the implementation of additional security measures specific to the environment in which the private key is deployed. This environment in which the private key is deployed must have undergone a security audit.

  Evidence that the device complies with the requirements of Chapter 11 of Certification Policy (At a minimum, the device's purchase invoice and the screen shots / prints of the hardware and software features of the device and the associated serial number) must be provided, when the application, by the Certificate Manager to attest to the possession of the device. The CA reserves the right to refuse the certificate application if it is found that this device does not meet these requirements.

  The CA records the characteristics of the device, whether or not it is provided by the CA and checks monthly until the end of the validity period of the entity's certificate, maintaining the certification status of the device. In case of loss of the certification of the device, the CA will ask the Certificate Manager for proof that the key pair is stored in a device that meets the requirements of Chapter 11. The Certificate Manager undertakes to provide these evidences (E.g: Invoice of purchase of a new device certified QSCD, Minutes of ceremony of the keys in case of key migration, Minutes of update of the device for the maintenance of the certification, etc.) within a deadline 15 days following the request. In the event that no evidence is provided or that the latter do not make it possible to determine if the storage conditions of the key pair, and transfer in another device if any, meet the requirements of the Certification Policy, the CA gives himself the right to revoke the certificate.
- Inform the RA in case of non-receipt of an e-mail confirming the CERTIFICATE REQUEST or REVOCATION request.
- Following receipt of an e-mail from the RA indicating the non-conformity of the request or that the request is incomplete, make the modifications within 7 calendar days after receipt of this e-mail.
- Download his certificate within 30 days of the validation of his request which is notified by e-mail to the CM. Beyond this period, the CERTIFICATE is automatically revoked by the RA;
- Accept explicitly the CERTIFICATE from its CERTIGNA customer area during the process of downloading the CERTIFICATE or by paper mail signed by the CM on

the express request of the RA. In the event of explicit non-acceptance, the certificate is automatically revoked by the RA;
- Protect the private key associated with the CERTIFICATE for which it is responsible by means appropriate to its environment;
- Protect its activation data and, if necessary, implement it;
- Protect access to the certificate base of the SEAL application service;
- Respect the conditions of use of the CERTIFICATE and of the associated private key mentioned in chapter 10 of this document;
- Inform the CA of any changes to the information contained in the CERTIFICATE;
- Immediately make a CERTIFICATE revocation request for which it is responsible to the RA, the DRA to which the CERTIFICATE request has been made or, where appropriate, the Certification Agent of the entity, when one of the causes of revocation of Chapter 9 is encountered.
- Save the private key associated with the CERTIFICATE. If it is stored on a hard disk, it must create a complex password for its protection (consisting of a combination of at least 8 characters among digits, lower case and uppercase letters, and special characters).
- Take all appropriate measures to ensure the security of the computer (s) on which the CERTIFICATE is installed. The CM is solely responsible for the installation of the CERTIFICATE;
- no longer use a CERTIFICATE and delete the associated key pair after the expiry or revocation of this CERTIFICATE;
- Inform RA of its departure from the entity or change of responsibilities and the need to register a new CM.

7. OBLIGATIONS OF CA AND RA

The CA is under an obligation of means for all obligations relating to the management of the lifecycle of the CERTIFICATE it issues. The CA agrees to:
- Can demonstrate to the users of the CERTIFICATE that it has issued the CERTIFICATE for a given SEAL application service and that the corresponding CM has accepted the CERTIFICATE;
- Take all reasonable means to ensure that CM are aware of their rights and obligations with respect to the use and management of keys, certificates, and equipment and software used for PKI.
- Provide technical support service by phone during business hours;
- Provide an on-line consultation service at https://www.certigna.fr allowing third parties to verify the validity of the CERTIFICATE issued by the CA at any time (see chapter 12).
- Carry out any collection and use of personal data in strict compliance with the laws and regulations in force in France, in particular with respect to the CNIL and Article 226-13 (Ordinance 2000-916 Of 19 September 2000, article 3, Official Journal of 22 September 2000, in force on 1 January 2002) of the Penal Code.

The RA is committed to:
- Verify and validate CERTIFICATE and revocation requests;
- Generate and provide the CM the CERTIFICATE within 30 days in case the CERTIFICATE request is compliant and complete.
- Revoke the certificate within 24 hours if the REVOCATION request is compliant and the requester is authenticated and authorized.

8. CERTIFICATE PUBLICATION

The SEAL CERTIFICATE is not published by the CA.

9. REVOCATION

The main causes of revocation are:
- The Certificate Manager, the legal representative of the entity to which it belongs, if any Certification Agent or DRA operator request the revocation of the certificate (especially in the case of destruction or alteration of the service's private key and / or its support);
- The legal representative of the entity to which it belongs notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The Certificate Manager did not comply with applicable Terms and Conditions of the certificate or the CA obtains evidence that the certificate was misused;
- The CA is made aware that a Certificate Manager has violated one or more of its material obligations under the Terms and Conditions;
- The service information contained in its certificate is not in accordance with the identity or purpose in the certificate (eg, change in the identity or function of the service), this before the normal expiry of certificate;
- The Certificate Manager, the entity, if any Certification Agent or DRA operator, has not fulfilled its obligations under the CP or the CPS;
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- The CA signing the certificates is revoked (which results in the revocation of all valid certificates signed by the corresponding private key);
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.
- The final judgment of the service or the cessation of activity of the entity attached to the server and the Certificate Manager;
- An error (intentional or not) was detected in the registration files;
- The server's private key is suspected of being compromised, is compromised, lost or stolen (or possibly the activation data associated with the private key);
- For technical reasons (failure to send the certificate ...).

The revocation request can be made by:
- The CM;
- A legal representative of the entity in charge of the SEAL application service, or if applicable a Certification Agent of that entity;
- The CA or the RA.

The revocation request may be made:
- By signed letter, accompanied by a photocopy of an official identity document of the requester;
- Online, on the site https://www.certigna.fr from the customer area of the CM or the Certification Agent if applicable.

10. CONDITIONS OF USE OF CERTIFICATE AND ASSOCIATED PRIVATE KEY

The uses of the CERTIFICATE are the electronic signature of application code and the electronic signature verification. The CERTIFICATE is used for applications where security needs are moderate (for level *) and strong (for level **) given the risks that threaten them. In case of non-respect of the uses, the CM or its entity could be held liable.

11. OBLIGATIONS OF USERS

USERS must :
- Respect the authorized uses of the CERTIFICATE and the associated private key. Otherwise, their liability could be incurred.
- Verify, prior to its use, the status of the certificates of the whole of the corresponding certification chain via the means offered for the verification of the certificates cited below.
- If the Certigna root CA certificate is not installed on the USER's machine, the USER must download it from the website https://www.certigna.fr , precisely at the following addresses:
  - http://autorite.certigna.fr/ACcertignarootca.crt ;
  - http://autorite.dhimyotis.com/ACcertignarootca.crt.

  The CA certificate can be downloaded from the following addresses:
  - http://autorite.certigna.fr/entitycsca.crt ;
  - http://autorite.dhimyotis.com/entitycsca.crt.

12. CERTIFICATE STATUS CHECKING MEANS

To verify the certification chain, the USER of a CERTIFICATE can download the authority certificates (ROOT CA and ISSUING CA) from the website: https://www.certigna.fr.

The ROOT CA certificate can already be installed on the workstation of the USER according to the software configuration.

To verify the REVOCATION status of a CERTIFICATE, the CA periodically publishes the CRL and offers an information service on the revocation status of the CERTIFICATES (OCSP server, for On-line Certificate Status Protocol).

This list of revoked certificates and these services are accessible for applications using certificates at the addresses contained in the CERTIFICATES:

To access the CRL :	To access the OCSP server:
http://crl.certigna.fr/entitycsca.crl	http://entitycsca.ocsp.certigna.fr
http://crl.dhimyotis.com/entitycsca.crl	http://entitycsca.ocsp.dhimyotis.com

13. LIMIT OF LIABILITY

The CA cannot be held liable if the private key associated with the CERTIFICATE is compromised. The CA shall under no circumstances be held responsible for any damage caused using the CERTIFICATE. The CA cannot be implicated by delays or losses that the transmitted data on which a SEAL is applied by the application service can be impacted. The CA cannot be held responsible for problems related to force majeure, within the meaning of the Civil Code. If a case of force majeure has a duration exceeding fifteen days, the CM will be authorized to terminate the CONTRACT and there will be no prejudice.

14. CONTRACT AND MODIFICATIONS

The CONTRACT cancels any previous commitment.

The CM agrees that during the term of the CONTRACT, the CA may modify the general conditions of use. However, the conditions accepted and signed by the CM remain valid throughout the duration of the CONTRACT unless the CM explicitly accepts the new conditions issued and published by the CA on the website https://www.certigna.fr. In this case, a letter must be sent to the CA together with the new general conditions of use marked "read and approved", the date and signature of the CM. In the event of renewal of the CONTRACT (renewal of the

CERTIFICATE at the end of its validity or after its revocation), the new CERTIFICATE is subject to the applicable general conditions of use.

15. TERMINATION

If one of the parties fails to fulfil one of the obligations arising from these general conditions, the other party may notify him of the performance of the said obligation. Failing that for the defaulting party to have executed within fifteen days of such notification, the other party may terminate the CONTRACT.

16. CONDITIONS OF REFUND

The CERTIFICATE command cannot be cancelled when the CERTIFICATE request is being processed. Any CERTIFICATE issued cannot be the subject of a refund request.

17. PRIVACY POLICY

Electronic certificate application files containing personal data are archived for at least seven years and as long as necessary for the purposes of providing proof of certification in legal proceedings, in accordance with applicable law. The personal identity information can be used as authentication data in the event of a request for revocation or information.

In addition, DHIMYOTIS retains the personal data for a period of three years from the end of the commercial relationship with the customer and 3 years from the last contact with the prospect. The delay starts from the last connection to the customer account or the last sending of an email to customer service, or from a click on a hypertext link of an email sent by DHIMYOTIS, a positive response to an email requesting if the client wishes to continue to receive commercial prospecting at the end of the three-year period.

In order to monitor the quality of our services, calls made to our customer service are likely to be registered and kept for a period of 30 days.

In accordance with the law n ° 78-17 of January 6, 1978 relating to data, files and freedoms, modified and the European regulation "2016/679 / EU of April 27, 2016" relating to the protection of natural persons to the processing of personal data and the free movement of such data, you have the right to access, oppose, rectify, delete and portability of your personal data. You can exercise your right by sending an email to: privacy@certigna.com, or by mail to the following address:
DHIMYOTIS, Service du DPO,
20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France
Your request must indicate your surname and first name, e-mail or postal address, be signed and accompanied by a valid proof of identity.

18. ASSIGNMENT OF THE CONTRACT

The CM cannot assign its rights to the CONTRACT.

19. DISPUTE RESOLUTION

The CONTRACT is subject to French law.

Parties undertake to try to resolve amicably any dispute which may arise between them, either directly or through a mediator, within 2 months of receipt of the letter with acknowledgment of receipt of the dispute. Half of the costs of mediation shall be borne by each of the parties. If necessary, the case will be brought before the Commercial Court of Lille.

20. DHIMYOTIS CONTACT INFORMATION

Dhimyotis S.A.
Zone de la plaine,
20 allée de la râperie 59650 Villeneuve d'Ascq, FRANCE
Phone : +33 806 115 115
Email : contact@dhimyotis.com