CERTIGNA CERTIFICATES
General Conditions of Sale and Use - Version 2.1

1. OBJECT

The purpose of these General Conditions of Sale and Use (GCSU) is to specify the terms and conditions for a CERTIFICATE issued by CERTIGNA and the respective commitments and obligations of the PARTS related hereto. These GCSU arise from a Certification Policy (CP) associated to the issued CERTIFICATE. Each CP is published online and identified by a unique OID identifier from which the various associated CERTIFICATES flow. These GCSU and this CONTRACT are listed below under the following representation:

NAME OF THE CERTIFICATION AUTHORITIE	CP's OID
Type of certificate: Level(s) of qualification	Certificate's OID
Link to the CP	**Concerned profile**

The CERTIFICATES cover by these GCSU and this CONTRACT are the follows:

CERTIGNA IDENTITY CA	1.2.250.1.177.2.3.1.
Encipherment RGS * + LCP	1.2.250.1.177.2.3.1.1.1
Encipherment RGS * + LCP	1.2.250.1.177.2.3.1.3.1
Authentication & signature RGS * + LCP	1.2.250.1.177.2.3.1.2.1
Authentication & signature RGS * + LCP	1.2.250.1.177.2.3.1.4.1
http://politique.certigna.fr/PCcertignaidentityca.pdf	**SUBJECT**
CERTIGNA IDENTITY PLUS CA	**1.2.250.1.177.2.4.1.**
Authentication & signature RGS ** + QCP-n-qscd	1.2.250.1.177.2.4.1.1.1
Authentication RGS *** + QCP-n-qscd	1.2.250.1.177.2.4.1.2.1
Signature RGS *** + QCP-n-qscd	1.2.250.1.177.2.4.1.3.1
Authentication & signature RGS ** + QCP-n-qscd	1.2.250.1.177.2.4.1.4.1
Authentication RGS *** + QCP-n-qscd	1.2.250.1.177.2.4.1.5.1
Signature RGS *** + QCP-n-qscd	1.2.250.1.177.2.4.1.6.1
http://politique.certigna.fr/PCcertignaidentityplusca.pdf	**SUBJECT**
CERTIGNA ENTITY CA	1.2.250.1.177.2.6.1
Seal for mails and documents RGS * + LCP	1.2.250.1.177.2.6.1.1.1
Seal for mails and documents RGS ** + QCP-l-qscd	1.2.250.1.177.2.6.1.4.1
Seal for mails and documents RGS **	1.2.250.1.177.2.6.1.42.1
Seal for mails and documents QCP-l-qscd	1.2.250.1.177.2.6.1.41.1
Seal for mails and documents QCP-l	1.2.250.1.177.2.6.1.7.1
Seal for mails and documents QCP-l + DSP2	1.2.250.1.177.2.6.1.8.1
Seal for timestamping tokens RGS * + LCP	1.2.250.1.177.2.6.1.3.1
Seal for timestamping tokens RGS ** + QCP-l-qscd	1.2.250.1.177.2.6.1.6.1
http://politique.certigna.fr/PCcertignaentityca.pdf	**CM**
CERTIGNA ENTITY CODE SIGNING CA	1.2.250.1.177.2.8.1
Seal for code signing RGS * + LCP	1.2.250.1.177.2.8.1.1.1
Seal for code signing RGS ** + QCP-l-qscd	1.2.250.1.177.2.8.1.2.1
http://politique.certigna.fr/PCcertignaentitycsca.pdf	**CM**
FR03	**1.2.250.1.177.2.2.1**
Seal for documents (2D-DOC)	1.2.250.1.177.2.2.1.1
http://politique.certigna.fr/PCfr03.pdf	**CM**
CERTIGNA SERVICES CA	**1.2.250.1.177.2.5.1**
Authentication for server RGS * + OVCP	1.2.250.1.177.2.5.1.1.1
Authentication for client RGS * + OVCP	1.2.250.1.177.2.5.1.2.1
Authentication for server QCP-w	1.2.250.1.177.2.5.1.3.1
http://politique.certigna.fr/PCcertignaservicesca.pdf	**CM**
CERTIGNA WILD CA	**1.2.250.1.177.2.7.1**
Authentication for client/server OVCP	1.2.250.1.177.2.7.1.1.1
Authentication for client/server wildcard OVCP	1.2.250.1.177.2.7.1.2.1
http://politique.certigna.fr/PCcertignawildca.pdf	**CM**

2. DEFINITIONS

The terms below, used throughout the present GCSU, and beginning with a capital letter have, unless otherwise stipulated, the following meaning whether they are indifferently used in the singular or the plural:

- **CA**: Certification Authority of the CERTIGNA company, issuing the CERTIFICATE;
- **ROOT CA**: Higher level Authority of the Certigna Public Key Infrastructure (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 CERTIGNA 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 information:
  - on the SERVER whose CM is responsible for a server and / or client authentication CERTIFICATE;
  - on the SEAL service for which the CM is responsible for a SEAL CERTIFICATE;
  - on the SUBJECT for a CERTIFICATE of encryption or authentication and / or signature.
- **CERTIFICATE REQUEST**: Set consisting of the request form (accepting the present GCSU) 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 SUBJECT or the CM of this entity.
- **CERTIFICATE MANAGER (CM)**: Natural person in charge and responsible for the electronic CERTIFICATE and the associate private key used by a SERVER or a SEAL service.
- **CRYPTOGRAPHIC DEVICE**: USB key, smart card or cryptographic module;
- **CONTRACT**: Relations between the CA and the SUBJECT or the CM framed by these GCSU expressly accepted by the SUBJECT or the CM during each CERTIFICATE REQUEST. Also included in the CONTRACT are all the documents to which these GCSU refer, in particular the Policy on the use of personal data available on Certigna.com.
- **OCSP STAPLING**: Mechanism which consists of configuring the client's secure server so that it acts as a proxy for the OCSP request, to drastically reduce the number of requests transmitted to the CA OCSP responder.
- **PART(S)**: Individually the SUBJECT or the CM or the CA, and collectively, the CA and the SUBJECT or the CA and the CM.
- **PUBLIC KEY INFRASTRUCTURE**: means all components, functions and procedures dedicated to the management of cryptographic keys and certificates used for trusted services. PKI can be composed of a CA, a certification operator, a centralized registration authority and / or local certification agents, an archiving entity, a publishing entity, …
- **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;
- **SERVER**: Computer server hosting a service secured by a CERTIFICATE, enabling the authentication of this service by USERS and securing exchanges therewith;
- **SUBJECT**: Natural person for who the CERTIFICATE REQUEST has been accepted and processed by CA, and who is responsible for the CERTIFICATE and for the private key corresponding;
- **UNLOCK**: Operation consisting of resetting the PIN code of a CRYPTOGRAPHIC DEVICE blocked following the entry of 3 incorrect PIN codes;
- **USER**: CERTIFICATE USER. It can be:
  - For encipherment CERTIFICATE, it can be:
    - An online service that uses an encryption device to encrypt data or a message to the certificate subject;
    - A person who transmits an encrypted message for the certificate subject.
  - For authentication CERTIFICATE, it can be:
    - An online service that uses a certificate and an authentication verification device to validate an access request made by the certificate subject in the context of an access control or to authenticate the origin of a message or data transmitted by the subject of the certificate;
    - A user recipient of a message or data and who uses a certificate and an authentication verification device to authenticate the origin.
  - For signature CERTIFICATE, it can be:
    - An online service that uses a signature verification device to verify the electronic signature on the data or a message of the subject of the certificate;
    - A user who electronically sign a document or a message;
    - A user recipient of a message or data and who uses a certificate and a signature verification device to verify the electronic signature by the subject of the certificate on this message or data.
  - For authentication and signature certificate, it can be the same users than an authentication or signature certificate.
  - For a SEAL CERTIFICATE
  - 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.
  - For authentication of SSL/TLS server CERTIFICATE, a natural person accessing to a server and using the server CERTIFICATE and an authentication verification module to authenticate the server it is accessing, which is identified in the server CERTIFICATE to establish a shared session key between his system and the server.
  - For authentication of client server, an application service accessing to a server and using the server CERTIFICATE and an authentication verification module to authenticate the server it is accessing, which is identified in the server CERTIFICATE to establish a shared session key between the servers.

3. DELIVERY, WARRANTY AND NORMATIVE COMPLIANCE

3.1 Delivery and guarantees

Any CERTIFICATE ordered must be accepted by the CM on the customer space created from the CA website or from one of its DRA. Before generating the CERTIFICATE, the SUBJECT or the CM must verify that the information stated in his CERTIFICATE REQUEST is accurate. Failing this, the SUBJECT or the CM must contact a member of the staff of the CA either by telephone at 0 806 115 115 (free service cost of a local call), or by email at the following address: contact@certigna.fr. Telephone support is available from Monday to Friday, except holidays, from 9 AM to 6 PM without interruption. The SUBJECT or the CM is aware that in case of error during the order in the nature of the CERTIFICATE, no modification can be made by the CA and the SUBJECT or the CM will have to make a new CERTIFICATE REQUEST. If a payment had already been made, the CA would not be required to pay any refund.

Once the CERTIFICATE REQUEST validated, the CERTIFICATE is generated. The SUBJECT or the CM is then brought to confirm the accuracy of said information, which means acceptance of the CERTIFICATE. Otherwise, the SUBJECT or the CM will have to make a new CERTIFICATE REQUEST and the CERTIFICATE generated will not give rise to any refund.

Once the CERTIFICATE accepted, the CERTIFICATE is available to the SUBJECT or the CM either on his customer area or on a CRYPTOGRAPHIC DEVICE. The installation of the CERTIFICATE is done under the sole responsibility of the SUBJECT or the CM. In case of any difficulty during this last phase, the SUBJECT or the CM can contact the CA at the telephone number and the email address indicated above or via contact details available on the DRA website. The CA does not guarantee the operation of the CERTIFICATE in the case of use outside the uses provided for in article 10 hereof.

3.2 Normative compliance

The CERTIFICATE is issued in compliance with one or many of the following standards:

- the CP « *Certificats électroniques de Services Applicatifs* » for a seal or server and / or client authentication use or the CP « *Certificats électroniques de Personnes* » for an encipherment, authentication or signature use, 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 ETSI EN 319 411-1OCVP / PTC level;
- The requirements from ETSI EN 319 411-1 LCP, NCP, NCP+, DVCP, OVCP or EVCP level;
- The requirements from ETSI EN 319 411-2 QCP, QCP-n, QCP-l, QCP-n-qscd or 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.
- The requirements of the document « *Guidelines For The Issuance and Management Of Extended Validation Certificates* » from CA/BROWSER FORUM for qualified server authentication CERTIFICATES.

The levels of qualifications and of certifications obtained for each CERTIFICATE are described in the following tables :

CERTIGNA IDENTITY CA		RGS	ETSI
Encipherment	1.2.250.1.177.2.3.1.1.1	*	LCP
Encipherment	1.2.250.1.177.2.3.1.3.1	*	LCP
Authentication & signature	1.2.250.1.177.2.3.1.2.1	*	LCP
Authentication & signature	1.2.250.1.177.2.3.1.4.1	*	LCP

CERTIGNA IDENTITY PLUS CA		RGS	ETSI
Authentication & signature	1.2.250.1.177.2.4.1.1.1	**	QCP-n-qscd
Authentication	1.2.250.1.177.2.4.1.2.1	***	QCP-n-qscd
Signature	1.2.250.1.177.2.4.1.3.1	***	QCP-n-qscd
Authentication & signature	1.2.250.1.177.2.4.1.4.1	**	QCP-n-qscd
Authentication	1.2.250.1.177.2.4.1.5.1	***	QCP-n-qscd
Signature	1.2.250.1.177.2.4.1.6.1	***	QCP-n-qscd

CERTIGNA ENTITY CA		RGS	ETSI
Seal for mails & documents	1.2.250.1.177.2.6.1.1.1	*	LCP
Seal for mails & documents	1.2.250.1.177.2.6.1.4.1	**	QCP-l-qscd
Seal for mails & documents	1.2.250.1.177.2.6.1.42.1	**	
Seal for mails & documents	1.2.250.1.177.2.6.1.41.1		QCP-l-qscd
Seal for mails & documents	1.2.250.1.177.2.6.1.7.1		QCP-l
Seal for mails & documents	1.2.250.1.177.2.6.1.8.1		QCP-l
Seal for timestamping tokens	1.2.250.1.177.2.6.1.3.1	*	LCP
Seal for timestamping tokens	1.2.250.1.177.2.6.1.6.1	**	QCP-l-qscd

CERTIGNA ENTITY CODE SIGNING CA		RGS	ETSI
Seal for code signing	1.2.250.1.177.2.8.1.1.1	*	LCP
Seal for code signing	1.2.250.1.177.2.8.1.2.1	**	QCP-l-qscd

FR03		RGS	ETSI
Seal for 2D-DOC documents	1.2.250.1.177.2.2.1.1	*	NCP+

CERTIGNA SERVICES CA		RGS	ETSI
Authentication for server	1.2.250.1.177.2.5.1.1.1	*	OVCP
Authentication for client	1.2.250.1.177.2.5.1.2.1	*	OVCP
Authentication for server	1.2.250.1.177.2.5.1.3.1		QCP-w

CERTIGNA WILD CA		RGS	ETSI
Authentication for client/server	1.2.250.1.177.2.7.1.1.1		OVCP
Authentication for client/server wildcard	1.2.250.1.177.2.7.1.2.1		OVCP

This compliance of the CERTIFICATE can be verified through the list published by the LSTI certification body on its website lsti.fr in the "Certification / PSCe" section.

4. DURATION

The CONTRACT is concluded for a period chosen during the CERTIFICATE REQUEST. This duration begins the day of the CERTIFICATE issuance by the CA and cannot exceed

- Eight hundred and twenty-five (825) days for a server and / or client authentication CERTIFICATE;
- Three (3) years for a professional CERTIFICATE;
- Five (5) years for a CERTIFICATE for individual;

This CONTRACT automatically terminates upon revocation or expiry of the CERTIFICATE, except for clauses that are intended to continue beyond.

5. PRICE AND CONDITIONS OF REFUNDS

5.1. 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 or from its DRA as appropriate;
- 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,
  - administrative order, for public institutions only, by attaching a purchase order on behalf of the Institution.
- REGENERATION of a CERTIFICATE, containing the same validated information, 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 provided, if any, is invoiced service;

All prices are expressed without taxes and majored of VAT or other applicable tax at the rate in effect on the date of invoice. All prices include delivery charges included, unless information to the contrary is communicated during the CERTIFICATE REQUEST. The SUBJECT or the CM cannot under any circumstances compensate, reduce or modify prices or suspend payment in advance.

Except with the prior written agreement of the CA or the DRA, 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.441-10 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.

5.2. Refund conditions

The CERTIFICATE order cannot be cancelled once the CERTIFICATE REQUEST has been made. Then, So, each CERTIFICATE issued cannot be the subject of a request for reimbursement due to implementation difficulties related in particular to the technical operating environment of the CERTIFICATE (Eg: non-compliance of software or hardware storing and using the CERTIFICATE with the standards and norms in force). However, in the event that the CERTIFICATE does not correspond to the CERTIFICATE REQUEST, following an error exclusively attributable to the CA, the CA undertakes to provide a CERTIFICATE compliant, or if it is unable to do so, to proceed with the reimbursement amounts already paid under the CONTRACT.

6. OBLIGATIONS OF SUBJECT OR OF THE CM

The SUBJECT or the CM has the following obligations:

- Make its CERTIFICATE REQUEST by following all procedure steps provided on the website: https://www.certigna.fr.
- Provide accurate and up-to-date information during the CERTIFICATE REQUEST or its renewal;
- 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 or on the DRA's website where appropriate, 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.
  Evidence that the device compliance could be required by the CA durung the CERTIFICATE REQUEST (in particular for a SEAL CERTIFICATE. These evidences to provide will be 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.

The CA reserves the right to refuse the CERTIFICATE REQUEST if it is found that this device does not meet these requirements.
- In the case where the CA would be informed or would identified the loss of the compliance of the device, the CA will ask the SUBJECT or the CM for proof that the key pair is stored in a device that meets the requirements of Chapter 11 of the CP associated to the CERTIFICATE.
- The SUBJECT or the CM 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 fifteen (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 itself 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 CERTIFICATE REQUEST or that the request is incomplete, make the modifications within seven (7) calendar days after receipt of this e-mail.
- Download the generated CERTIFICATE, available on its customer area where appropriate, within thirty (30) days of the validation of the CERTIFICATE 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 or form the DRA"s website where appropriate. This acceptation can also be done by sending a paper form signed by the SUBJECT or 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 he is responsible by means appropriate to its environment and in compliance with the requirements from chapter 11 of the associated CP;
- Protect its activation data and, if necessary, implement it;
- Protect access to the CERTIFICATE database of the SERVER for server and / or client authentication CERTIFICATE;
- 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.
- Take all appropriate measures to ensure the security of the device(s) on which the CERTIFICATE is installed. The SUBJECT or 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 SUBJECT or CM.
- Check the suitability of the CERTIFICATE and its characteristics;
- Ensure that the hardware and / or software prerequisites recommended by the CA are met in view of the installation and use of the CERTIFICATE;
- Have all the skills and means necessary to use the CERTIFICATES;
- Implement measures to prevent any unauthorized person from physically accessing the device storing the keys and the CERTIFICATE;
- Immediately notify the person in charge of the security of the information systems of his entity (example: CISO) in case of loss or theft of the device storing the keys and the CERTIFICATE; and
- For applications deemed to be the most critical at the business level, implement measures to detect potentially fraudulent transactions (inconsistency of signed business data, etc.) and to provide, if necessary, an alternative procedure.
- For a server and / or client authentication CERTIFICATE, and in the case where, for one or more domain names to be included in the CERTIFICATE, the "DNS CAA" option is enabled, the RC must update the associated DNS records to include the CA, prior to the request for a CERTIFICATE.

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 SUBJECT, SERVER or SEAL service and that the corresponding SUBJECT or CM has accepted the CERTIFICATE;
- Take all reasonable means to ensure that the SUBJECT or the 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, and with the personal data use policy available on Certigna.com;
- At the time of issuance, implement and follow the requirements describes at sections 3.2 and 3.3 of the associated CP for verifying that the Subject authorized the issuance of the CERTIFICATE and that the Applicant Representative is authorized to request the CERTIFICATE on behalf of the Organization attached to the server.
- At the time of issuance, implement and follow the requirements describes at sections 3.2 and 3.3 of the CP for verifying the accuracy of all of the information contained in the CERTIFICATE.
- At the time of issuance, implement and follow the requirements describes at sections 3.2 and 3.3 of the CP for verifying the identity of the organization, the legal representative and the SUBJECT or the CM designated.
- If the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements,
- If the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
- Maintain a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired CERTIFICATES; and
- Revoke the CERTIFICATE for any of the reasons specified at section 4.9 of the CP.
- At the time of issuance, implement and follow the requirements describes at sections 3.2 and 3.3 of the associated CP for verifying that the SUBJECT or the CM either had the right to use, or had control of, the Domain Name(s) listed in the CERTIFICATE's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control).

The RA is committed to:
- Verify and validate CERTIFICATE and REVOCATION requests;
- Generate and provide the SUBJECT or the CM the CERTIFICATE within thirty (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 CERTIFICATE is not published by the CA except in the case of a SEAL CERTIFICATE of 2D-DOC documents. In this case the CM explicitly accepts that the CERTIFICATE issued by the CA is published in a directory at the following address: http://certificates.certigna.fr.

9. REVOCATION

The following circumstances may cause the revocation of a SERVER CERTIFICATE:
- The SUBJECT or the CM, 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 private key and / or its support);
- The legal representative of the entity to which the SUBJECT, the SERVER or the SEAL service belongs notifies the CA that the original CERTIFICATE REQUEST was not authorized and does not retroactively grant authorization;
- The CA obtains evidence that the private key corresponding to the public key in the CERTIFICATE is suspected of being compromised, is compromised, lost or stolen (or possibly the activation data associated with the private key);
- In the case of a server and / or client authentication CERTIFICATE, the CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

The CA will revoke a Certificate within five (5) days if one or more of the following occurs:
- The CERTIFICATE no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the Certification Policy;
- The CA obtains evidence that the CERTIFICATE was misused;
- The CA is made aware that the SUBJECT or the CM has violated one or more of its material obligations under these GCSU;
- In the case of a server and / or client authentication CERTIFICATE, the CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

- The information of the SUBJECT, the SERVER or the SEAL service, 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 server), this before the normal expiry of certificate;
- The CA is made aware that the CERTIFICATE was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
- The CA determines or is made aware that any of the information appearing in the CERTIFICATE is inaccurate or misleading;
- 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;
- REVOCATION is required by the CA's Certification Policy and/or Certification Practice Statement;
- The CA is made aware of a demonstrated or proven method that exposes the Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed. Methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys),
- The SUBJECT or the CM, the entity, if any Certification Agent or DRA operator, has not fulfilled its obligations under the CP or the CPS;
- 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 (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such CERTIFICATES should be revoked and replaced by CA within a given period of time).
- The SEAL service or server stop or the cessation of activity of the entity attached to the server and the CM;
- The departure of the SUBJECT from the entity or the cessation of activity of the entity attached to the SUBJECT;
- An error (intentional or not) was detected in the CERTIFICATE REQUEST and the associated registration files;
- For technical reasons (failure to send the CERTIFICATE ...).

The REVOCATION request can be made by:

- The SUBJECT or the CM, a legal representative of the entity attached to the CERTIFICATE, or if applicable a Certification Agent of that entity;
- The CA, the RA or a DRA.

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 or which of the DRA, from the customer area of the CM or the Certification Agent if applicable.

10. CONDITIONS OF USE OF CERTIFICATE AND ASSOCIATED PRIVATE KEY

- Encipherment CERTIFICATE is used for:
  - Decipherment: using its private key, a SUBJECT decrypts the data that were transmitted through electronic exchanges, enciphered with his public key;
  - Encipherment: using the recipient's public key, several individual data.
- Authentication CERTIFICATE is used for:
  - Authentication of subjects on remote Subjects or to other people. It may be authentication in the framework of an access control to a Subject or an application, or authentication of data's origin as part of the electronic mail.
- Signature CERTIFICATE is used for:
  - Data electronic signature. Such electronic signature brings, besides the authenticity and integrity of signed data, the manifestation of consent of the signatory for the content of these data.
- Authentication and signature CERTIFICATE, the uses are the same than authentication or signature CERTIFICATE.
- SEAL CERTIFICATE for emails and documents signing, the uses are the electronic signature of data and the electronic signature verification. This data can be, for example, an acknowledgment following the transmission of information by a user to an application service, an automatic response to a request by a user, an email, a document or an archive.
- SEAL CERTIFICATE for timestamp token signing, the uses are the electronic signature of timestamp tokens and the electronic signature verification.
- Authentication of SSL/TLS server CERTIFICATE (qualified or not) is used for SERVER authentication with people or other servers, as part of establishing secure sessions, such as SSL / TLS or IPsec to establish a symmetric session key to encrypted the exchanges in this session.
- Authentication of client server CERTIFICATE is used for SERVER authentication from other servers, as part of establishing secure sessions, such as SSL / TLS or IPsec to establish a symmetric session key to encrypted the exchanges in this session.

In case of non-respect of the uses, the SUBJECT, the CM or the entity designated in the CERTIFICATE 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; and
- 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 CERTIFICATE of each Certification Authority can be downloaded from the following links:

CERTIGNA IDENTITY CA
http://autorite.certigna.fr/identca.crt
http://autorite.dhimyotis.com/identca.crt

CERTIGNA IDENTITY PLUS CA
http://autorite.certigna.fr/identityplusca.crt
http://autorite.dhimyotis.com/identittyplusca.crt

CERTIGNA ENTITY CA
http://autorite.certigna.fr/entityca.crt
http://autorite.dhimyotis.com/entityca.crt

CERTIGNA ENTITY CODE SIGNING CA
http://autorite.certigna.fr/entitycsca.crt
http://autorite.dhimyotis.com/entitycsca.crt

FR03
http://autorite.certigna.fr/2ddoc.crt
http://autorite.dhimyotis.com/2ddoc.crt

CERTIGNA SERVICES CA
http://autorite.certigna.fr/servicesca.crt
http://autorite.dhimyotis.com/servicesca.crt

CERTIGNA WILD CA
http://autorite.certigna.fr/wildca.crt
http://autorite.dhimyotis.com/wildca.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:

CERTIGNA IDENTITY CA	
Accès aux LCR	http://crl.certigna.fr/identca.crl http://crl.dhimyotis.com/identca.crl
Accès à l'OCSP	http://identca.ocsp.certigna.fr http://identca.ocsp.dhimyotis.com

CERTIGNA IDENTITY PLUS CA	
Accès aux LCR	http://crl.certigna.fr/identityplusca.crl http://crl.dhimyotis.com/identityplusca.crl
Accès à l'OCSP	http://identityplusca.ocsp.certigna.fr http://identityplusca.ocsp.dhimyotis.com

CERTIGNA ENTITY CA	
Accès aux LCR	http://crl.certigna.fr/entityca.crl http://crl.dhimyotis.com/entityca.crl
Accès à l'OCSP	http://entityca.ocsp.certigna.fr http://entityca.ocsp.dhimyotis.com

CERTIGNA ENTITY CODE SIGNING CA	
Accès aux LCR	http://crl.certigna.fr/entitycsca.crl http://crl.dhimyotis.com/entitycsca.crl
Accès à l'OCSP	http://entitycsca.ocsp.certigna.fr http://entitycsca.ocsp.dhimyotis.com

FR03	
Accès aux LCR	http://crl.certigna.fr/2ddoc.crl http://crl.dhimyotis.com/2ddoc.crl
Accès à l'OCSP	http://2ddoc.ocsp.certigna.fr http://2ddoc.ocsp.dhimyotis.com

CERTIGNA SERVICES CA	
Accès aux LCR	http://crl.certigna.fr/servicesca.crl
	http://crl.dhimyotis.com/servicesca.crl
Accès à l'OCSP	http://servicesca.ocsp.certigna.fr
	http://servicesca.ocsp.dhimyotis.com
CERTIGNA WILD CA	
Accès aux LCR	http://crl.certigna.fr/wildca.crl
	http://crl.dhimyotis.com/wildca.crl
Accès à l'OCSP	http://wildca.ocsp.certigna.fr
	http://wildca.ocsp.dhimyotis.com

As part of the Certigna OCSP Responder service, up to 250,000 OCSP requests are allowed per CERTIFICATE per day. If this threshold is exceeded, Certigna reserves the right to impose to the SUBJECT or the CM the implementation of the OCSP Stapling mechanism on the service secured by the CERTIFICATE. If the OCSP stapling is refused, CERTIGNA may revoke the CERTIFICATE to maintain and guarantee the availability of the OCSP responder for all its customers.

13. LIABILTY AND INSURANCE

3.1. Liability

The CA is subject to a general obligation of means. The CA cannot be held liable for the SUBJECT or the CM for direct damage that may be attributed to it for the services entrusted to it under these GCSU.

The CA's responsibility cannot be sought for any indirect loss, such as, in particular, loss of turnover, loss of profit, loss of orders, loss of data, loss of opportunity, disturbance to the image or any other special damage or events beyond its control or any fact not attributable to it.

The CA is only responsible for the tasks specifically assigned to it under this CONTRACT.

The CA cannot be held responsible in any way for the use made by the SUBJECT or of the CM of the CERTIFICATES, nor the contents of the documents and the data which are given to it by the CM or the applicant.

In any case, the responsibility of the CA cannot be sought in case of:

- Fault, negligence, omission or default of the CA, which would constitute the exclusive cause of the occurrence of the damage,
- Malfunction or unavailability of tangible or intangible property in the case where it has been provided by the SUBJECT or the CM,
- Delay in providing the data to be processed due to the SUBJECT or the CM;
- Loss of the qualification of a third-party provider that is beyond the control of CERTIGNA (Ex: the supplier of CRYPTOGRAPHIC SUPPORT).

By express agreement between the PARTIES, the liability of the CA is limited, by CERTIFICATE REQUEST, all damages, to the sum of two (2) times the amount paid under the CONTRACT.

13.2. Insurance

The CA holds an insurance policy in the field of professional civil liability, guaranteeing direct material or immaterial consequential damages caused in the exercise of his professional activity.

14. CONTRACT AND MODIFICATIONS

The CONTRACT cancels any previous commitment.

The SUBJECT or the CM agrees that during the term of the CONTRACT, the CA may modify the general conditions of sale and use unilaterally and at any time. However, the conditions accepted and signed by the SUBJECT or the CM remain valid throughout the duration of the CONTRACT unless the SUBJECT or the CM explicitly accepts the new conditions issued and published by the CA on the website https://www.certigna.fr or on the DRA's website. The new version of the CONTRACT will apply to any new CERTIFICATE REQUEST.

15. TERMINATION

In the event of a breach by one or other of the PARTIES to one of its obligations hereunder, the other PARTY shall be authorized thirty (30) days after formal notice sent by registered letter with acknowledgment of receipt. had no effect, to terminate these by operation of law by registered letter with acknowledgment of receipt without prejudice to any damages and interests to which it could claim due to the deficiencies invoked.

16. PRIVACY POLICY

Electronic CERTIFICATE REQUEST 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, CERTIGNA retains the personal data for a period of three (3) years from the end of the commercial relationship with the customer and three (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 CERTIGNA, 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 thirty (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:

CERTIGNA, 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 copy of a valid proof of identity.

17. ASSIGNMENT OF THE CONTRACT

The SUBJECT or the CM cannot assign its rights to the CONTRACT.

18. DISPUTE RESOLUTION

The validity of these GCSU and any other question or dispute relating to its interpretation, performance or termination shall be governed by French law.

The PARTIES undertake to devote their best efforts to the amicable resolution of all questions or disputes that may divide them, prior to the seizure of the jurisdiction hereinafter designated.

The PARTIES agree, in the event that an amicable agreement is impossible to stop, that the courts of Lille will have exclusive jurisdiction to hear any dispute resulting from the validity, interpretation, execution or termination of these, and more generally any litigation proceeding hereunder that could divide them, notwithstanding pluralities of defendants or warranty claim.

19. CERTIGNA CONTACT INFORMATION

CERTIGNA S.A.S
Zone de la plaine,
20 allée de la râperie 59650 Villeneuve d'Ascq
Tél : +33 806 115 115
Email : contact@certigna.com

20. REPORT A MALICIOUS OR DANGEROUS CERTIFICATE

For reporting a malicious or dangerous CERTIFICATE (suspected Private Key compromise, CERTIFICATE misuse, or other types of fraud, compromise, misuse, inappropriate conduct, etc.) or any other matter related to CERTIFICATES, use the contact form available at https://www.certigna.fr/contact.xhtml by selecting "CERTIFICATE considered malicious or dangerous".

21. LOSS OF QUALIFICATION/CERTIFICATION OF THE SUPPORT

The CRYPTOGRAPHIC DEVICE, delivered if necessary, by CERTIGNA to the SUBJECT or the CM to store and use the private key and the CERTIFICATE, benefits from one or more qualifications and / or certifications. In the event that one of these qualifications or certifications is no longer maintained or suspended for reasons such as the identification of a vulnerability or the stopping of the manufacture of the device, CERTIGNA will inform the SUBJECT or the CM and revoke its CERTIFICATE, without condition of reimbursement.