General Conditions of Sales and of Use
Certificates & Timestamps – 3.1 Public 10/11/2023

1. OBJECT

The purpose of these conditions is to specify the general conditions of online sale on the site www.certigna.com and of use (GCSU) of the following products delivered by CERTIGNA as well as the respective commitments and obligations of the PARTIES related to these:

- **CERTIFICATES.** For certificates, the GCSU result from a Certification Policy (CP) associated with the CERTIFICATES issued. The CP is published online and is identified by a unique identifier OID from which the OIDs of the various associated CERTIFICATES are derived. The CERTIFICATES covered by this CONTRACT are listed in Appendix 2 of these GCSU.
- **TIME-STAMPING TOKENS**. For TIME-STAMPING TOKENS, the GCSU derive from a Time-Stamping Policy (TP) associated with the TIME-STAMPING TOKENS issued. This TP is identified by the following unique identifier (OID): 1.2.250.1.177.2.9.1 and is published at the following address: http://politique.certigna.fr/PHcertignaTSA.pdf

2. SCOPE AND ENFORCEABILITY

2.1. Scope

These GCSU apply only in the presence of the following cumulative conditions:

(a) sales to buyers acting in a professional capacity, that is to say any natural or legal person who acts for purposes which fall within the framework of his commercial, industrial, craft or liberal activity (the "Customer(s)");

(b) wishing to acquire the products offered for sale on the CERTIGNA website accessible at the following address: https://www.certigna.com (the "Website").

2.2. Enforceability

These GCSU become enforceable against Customers from the moment they tick the box provided for this purpose. They then acknowledge having been aware of them and having accepted them without restriction or reservation. The validation of the order by its confirmation implies acceptance by the Customer of the GCSU in force on the day of the order, the conservation and reproduction of which are ensured by CERTIGNA in accordance with article 1127-1 of the civil code. They will prevail over any other version or any other contradictory document having the same purpose.

3. DEFINITIONS

The terms used throughout these GCSU, and written in capital letters have, unless otherwise stipulated, the meaning given to them in Appendix 1 to these GCSU whether they are used indifferently in the singular or in the plural.

4. ORDERING PROCESS ON THE WEBSITE

4.1. Creation of the customer account

To order products on the Website, the Customer must first create an account. To do this, the Customer must enter a valid email address, his name, his first name, his title, his telephone number, his professional email address as well as the contact details of the Customer's professional entity.

The Customer will be solely responsible for the consequences of the use of his customer account, until it is deactivated. The Customer undertakes to provide true and sincere information and to inform CERTIGNA of any change concerning them.

4.2. Deactivation of the customer account

In the event of non-compliance with all or part of these GCSU, CERTIGNA reserves the right to automatically deactivate the Customer's account after sending an e-mail that has remained ineffective for a period of 15 days and without no compensation. In the event of fraud on the part of a Customer, the deactivation of the account will be done automatically, without notice and without compensation.

4.3. Order placement

To place an order, the Customer must follow the instructions on the Website. The order is first subject to a summary which includes all the products selected by the Customer. The latter then validates his order by "clicking" on the "Order" icon.

4.4. Order confirmation

The online sales contract is concluded when the Customer clicks on the button to confirm the order to go to payment after viewing the detail thereof and in particular its total price including tax with the applicable shipping costs and having received the possibility of correcting any errors.

4.5. Order modification

Any modification of an order by the Customer after confirmation of his order is subject to the prior written acceptance of CERTIGNA.

4.6. Acknowledgment of receipt of the order

CERTIGNA then confirms that the order has been considered by sending an automatic e-mail, including (i) the essential characteristics of the products ordered (ii) the indication of the price including tax and shipping costs (iii) if applicable, any difficulties or reservations relating to the order placed. CERTIGNA reserves the right to refuse any order for legitimate reasons.

5. DELIVERY, GUARANTEE AND STANDARDS COMPLIANCE

5.1. Issue and issue of CERTIFICATES

Any CERTIFICATE ordered must be accepted by the SUBJECT or the CERTIFICATE MANAGER (CM) on the customer account created from the Webite or from the website of one of the DRAs. Before the generation of the CERTIFICATE, the APPLICANT, the SUBJECT or the CM must verify that the information stated in the CERTIFICATE APPLICATION is correct. Failing this, the APPLICANT, the SUBJECT or the CM must contact a member of the CA or DRA staff. If it is the CA, either by telephone on 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 Monday to Friday, except holidays, from 9 a.m. to 6 p.m. non-stop. The APPLICANT, the SUBJECT or the CM is aware that in the event of an error when ordering in the nature of the CERTIFICATE, no modification can be made by the CA and a new CERTIFICATE REQUEST must be made by the APPLICANT, the SUBJECT or the CM. If a payment had already been made, CERTIGNA would not be liable for any refund.

Once the CERTIFICATE REQUEST has been validated, the CERTIFICATE is generated. The SUBJECT or the CM is then required to confirm the accuracy of said information, which constitutes acceptance of the CERTIFICATE. At this stage, no modification of the information can be made by the CA. It is therefore the responsibility of the SUBJECT or the CM to verify the accuracy of their information the first time they are asked to do so. Failing this, the SUBJECT or the CM will have to make a new CERTIFICATE REQUEST and the CERTIFICATE generated will not give rise to any reimbursement.

Once the CERTIFICATE has been accepted, it is made available to the SUBJECT or the CM either from their customer account or on a CRYPTOGRAPHIC DEVICE. The installation of the CERTIFICATE is done under the sole responsibility of the SUBJECT or the CM. In the event of any difficulty during this last phase, the SUBJECT or the CM can contact the AC or DRA at the phone number and email address of the CA indicated above or at the contact details available on the DRA website. CERTIGNA does not guarantee the functioning of the CERTIFICATE in the case of use outside the uses provided for in Article 13 hereof.

5.2. Normative compliance of CERTIFICATES

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;
- The requirements from ETSI EN 319 411-1 LCP, NCP, NCP+, OVCP or EVCP level;
- The requirements from ETSI EN 319 411-2 QCP, QCP-n, QCP-l, QCP-w, 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 requirements of the document « *Baseline Requirements for the issuance and Management of Publicly-Trusted S/MIME Certificates* » from CA/BROWSER FORUM.

CERTIGNA is audited by LSTI, a french certification body The status of CERTIGNA's product qualifications and certifications can be consulted on the following websites:

- RGS qualifications: Link to the LSTI website
- ETSI certifications: Link to the LSTI website
- eIDAS qualifications: Link to the European TSL

5.3. Normative compliance of TIME-STAMPING TOKENS

TIME-STAMPS are issued targeting the compliance with the following requirements:

- eIDAS Regulation (EU) N°910/2014 for qualified time-stamping service ;
- the « Time-stamp policy » of the « Référentiel Général de Sécurité » (RGS) developed by the National Agency for the information systems security (ANSSI);
- Best Practices Policy for Time-Stamp (BTSP) described by ETSI EN 319 421 specifications and identified by the following OID: 0.4.0.2023.1.1.

The trust service practices under which the CA operates are non-discriminatory.

6. DURATION

The CONTRACT is concluded for the period determined when ordering on the Website.

For CERTIFICATES, this duration starts on the day of issue of the CERTIFICATE by the CA and cannot exceed three (3) years except for server and / or client authentication CERTIFICATES, the duration of which cannot exceed three hundred and eighty-eighteen (398) days.

For TIME-STAMPING TOKENS, this period starts on the day of the order and may not exceed one (1) year. This duration is reset when ordering any new TIME-STAMPING TOKENS.

7. PRICE AND CONDITIONS OF REFUNDS

7.1. PRICE IN FORCE

CERTIGNA may be required to modify its prices at any time, but the products available on the Website will be invoiced to the Customer at the rates in force appearing on the Website when the Customer places the order. The prices indicated on the Website:

(a) are expressed in Euros, excluding VAT and including VAT;
(b) include applicable taxes in force;
(c) do not include the costs related to the mode of authentication and the delivery costs, which are invoiced in addition, according to the choices of the Customer at the time of the order as for the modes of authentication and delivery of the CERTIFICATES ordered. These costs (depending on the Customer's choice) will be indicated at the latest when the Customer confirms the order.

The REFABRICATION of a CERTIFICATE, containing the same validated information, is free during the 3 months following the issuance of the CERTIFICATE by the CA;

Unlocking the CRYPTOGRAPHIC DEVICE in which the CERTIFICATE is provided, if applicable, is a service invoiced at the current rate appearing on the Website.

7.2. PRICE CHARACTERISTICS

The prices applicable on the day the order is placed are closed and non-revisable during their period of validity as indicated on the Website. The period of validity of the offers and prices of the products available on the Website is determined by the updating of the Website.

7.3. ORDER PAYMENT

The price is due and payable in cash, in full on the day the order is placed by the Customer, by one of the following means:

- Payment by bank card secured by SOGENACTIF.

  Payments by credit card are debited at the time of order confirmation.

  Any order with payment by credit card is only considered effective when the payment centers concerned have given their consent. When the order is debited, in the event of irregular, incomplete or non-existent payment, for any reason whatsoever, CERTIGNA reserves the right to block the delivery of the products ordered. The Customer is informed by e-mail.

  Payment card details are encrypted using SSL (Secure Socket Layer), and never pass unencrypted over the network. Payment is made directly to the bank.
- bank transfer, by attaching the proof of transfer provided by the bank when ordering for TIME-STAMPING TOKENS and when submitting the supporting documents to the CERTIFICATE application file;

- Administrative mandate, for public establishments only, by attaching an order form in the name of the Establishment. It is specified that the total invoicing of the order will be carried out as soon as the CERTIFICATES or TIME-STAMPING TOKENS are made available on the Website.

CERTIGNA will not be required to deliver the products ordered by the Customer if the latter does not pay him the full price under the conditions indicated herein.

The SUBSCRIBER, the SUBJECT, the CM or the APPLICANT may in no case offset, reduce or modify the prices or suspend payment in advance.

Except with the prior written consent of CERTIGNA, any CERTIFICATE for which the sale price has not been paid in full may either not be issued or be revoked after its issue by the CA.

7.4. BILL

The invoice is issued by CERTIGNA and is given to the Customer upon delivery of the ordered products or on the next monthly due date for customers who have opted for the monthly billing system. In accordance with Article L.441-10 of the French Commercial Code, in the event of non-payment on the due date indicated on the invoice, without the obligation to send a reminder, late payment penalties shall be applied, calculated at a rate of three times the legal interest rate in force on the day the invoice is due, as well as a fixed indemnity of €40 for collection costs.

7.5. REFUND CONDITIONS

The order of products cannot be canceled once the CERTIFICATE REQUEST has been made or the subscription to the TIME-STAMPING SERVICE has been made. Thus, any product issued cannot be the subject of a request for reimbursement, in particular following implementation difficulties related in particular to the technical operating environment of the CERTIFICATE or the TIME-STAMPING SERVICE (Ex: non-the standards and norms in force for the software or hardware used to request the supply of a TIME-STAMPING TOKEN from a TSU) . However, in the event that the CERTIFICATE does not correspond to the CERTIFICATE REQUEST or the TIME-STAMPING TOKEN does not correspond to the CONTRACT following an error exclusively attributable to the CA or the TSA, the CA or the TSA undertakes to provide a conforming CERTIFICATE or TIME-STAMPING TOKEN, or if applicable if it is unable to do so, to reimburse the sums already paid under the CONTRACT.

8. OBLIGATIONS OF THE PARTIES FOR CERTIFICATES

8.1 OBLIGATIONS OF THE SUBSCRIBER

The SUBSCRIBER has the duty to:

- Apply for a CERTIFICATE by following all the steps of the procedure appearing on the Website.
- Communicate exact, complete and up-to-date information for the creation of his customer account, the REQUEST FOR CERTIFICATE or its renewal;
- Confirm that the information to be placed in the CERTIFICATE is correct;
- Send to the RA, if applicable to the DRA, or to a Certification Agent of the legal entity attached to the CERTIFICATE, by hand or by post (at its expense), the registration form generated during the REQUEST FOR CERTIFICATE online on the Website or on the DRA Website where applicable, payment, as well as supporting documents.
- Comply with the conditions of use of the CERTIFICATE and the associated private key set out in Article 13 hereof and prohibit any unauthorized use of the CERTIFICATE and the associated private key of the SUBJECT, the SEAL service or the SERVER;
- If necessary, generate the key pair with a 2048 or 3072 bits RSA modulus and in compliance with ETSI 119 312 specifications;
- If necessary, generate the key pair associated with the CERTIFICATE in a CRYPTOGRAPHIC DEVICE which complies with the security requirements of chapter 11 of the Certification Policy associated with the CERTIFICATE.
- Supporting documents attesting to the conformity of the CRYPOGRAPHIC DEVICE may be requested by the CA when requesting a CERTIFICATE (in the case of a SEAL CERTIFICATE). These supporting documents will be at a minimum the purchase invoice of the device and photos / screenshots of the hardware and software characteristics of the device and the associated serial number. The CA reserves the right to refuse the CERTIFICATE REQUEST in the absence of supporting documents or if it has been proven that this device does not meet these requirements.
- Keep the SUBJECT's private key under his sole control;
- Maintain the private key of the SEAL or SERVER service under the control of the associated legal person;
- Immediately inform the CA of any loss, theft or compromise of the SUBJECT's private key, SEAL or SERVER service;
- Immediately inform the CA if control of the private key of the SUBJECT, service or SERVER has been lost due to the compromise of activation data (for example, the PIN code) or other reasons;
- Immediately inform the CA of any modification concerning the information contained in the CERTIFICATE;
- Inform the RA in the event of non-receipt of an email confirming that the REQUEST FOR CERTIFICATE or REVOCATION has been taken into account;
- Following receipt of an email from the RA indicating the non-compliance of the CERTIFICATE APPLICATION or that the file is incomplete, make the changes within seven (7) calendar days after receipt of said email;
- Make sure that the CERTIFICATE of the SUBJECT, the SEAL service or the SERVER is no longer used following the expiration or REVOCATION of this CERTIFICATE (Except for encipherment keys).
- Check the suitability of the CERTIFICATE and its characteristics to its needs.

8.2 OBLIGATIONS OF THE SUBJECT OR CM

The SUBJECT or the CM has the following obligations:

- Make its CERTIFICATE REQUEST by following all procedure steps provided on the Website:
- 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: or on the DRA's website where appropriate, the payment, as well as the evidence documents.

- If necessary, generate the key pair with a RSA modulus size of 2048 or 3072 bits and in compliance with ETSI 119 312 specifications;
- 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 during 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 Certification Policy;
- 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 11 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 10.2 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.

8.3 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 on the Website allowing third parties to verify the validity of the CERTIFICATE issued by the CA at any time (see chapter 13).
- 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 personal data use policy available on the Website;

- 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 chapter 10.2.
- 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.

8.3 OBLIGATIONS OF CERTIFICATE 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_rootca.crt
http://autorite.dhimyotis.com/identca_rootca.crt

CERTIGNA IDENTITY PLUS CA

http://autorite.certigna.fr/identityplusca_rootca.crt
http://autorite.dhimyotis.com/identityplusca_rootca.crt

CERTIGNA ENTITY CA

http://autorite.certigna.fr/entityca_rootca.crt
http://autorite.dhimyotis.com/entityca_rootca.crt

CERTIGNA ENTITY CODE SIGNING CA

http://autorite.certigna.fr/entitycsca_rootca.crt
http://autorite.dhimyotis.com/entitycsca_rootca.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

9. OBLIGATIONS OF THE PARTIES FOR TIME-STAMPING TOKENS

9.1 OBLIGATIONS OF APPLICANT

The APPLICANT has the duty to issue a request using a hash algorithm supported by the TSA (SHA256, SHA384 or SHA512). It is recommended that the APPLICANT, at the time of obtaining a TIME-STAMP, verify that the CERTIFICATE of the TIME-STAMP unit is not revoked.

9.2 OBLIGATIONS OF USERS OF TIME-STAMPS

To trust a TIME-STAMP, the USERS must:

- Verify that the TIME-STAMP has been successfully signed, and that the certificate of the TSU is valid at the time of the TIME-STAMP generation.
- Consider the limitations on the use of the time-stamp indicated in the TP and these GCSU.

9.3 OBLIGATIONS OF THE TSA

The TSA performs all or part of these functions directly or by subcontracting them. In any case, the TSA retains the responsibility. The TSA undertakes to comply with the obligations described in this Time-stamp Policy and ensures that these requirements are met. It also undertakes that the components of the TSA, internal or external to the TSA, to which they are applicable also respect them. The TSA:

- ensures the compliance with the requirements and procedures prescribed in this policy, even when the time-stamp features are implemented by subcontractors.
- adheres to any additional obligations indicated in the time-stamp either directly or incorporated by reference.
- provides time-stamping services in accordance with this TP and the associated TPS.
- fulfils all its commitments as stipulated in these GCSU.

10. CERTIFICATE PUBLICATION AND REVOCATION

10.1 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.

10.2 REVOCATION

The following circumstances may cause the revocation of the certificate:

- **Key compromise** (RFC 5280 CRLReason #1)
  - The CM or the Subject, the legal representative of the entity to which he/she belongs, where applicable the 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) because they have reason to believe that the private key of the certificate has been compromised, e.g. an unauthorized person has had access to the private key of the certificate.
  - The CA obtains verifiable evidence that the private key corresponding to the public key in the certificate is suspected of being compromised or is compromised,
  - 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 CA revokes a Certificate within 24 hours and use the corresponding CRL Reason if one or more of the following occurs:

- **Key compromise** (RFC 5280 CRLReason #1)
  - The CM or the Subject, the legal representative of the entity to which he/she 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) because they have reason to believe that the private key of the certificate has been compromised, e.g. an unauthorized person has had access to the private key of the certificate.
  - The CA obtains verifiable evidence that the private key corresponding to the public key in the certificate is suspected of being compromised or is compromised,
  - 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),
- **Privilege withdrawn** (RFC 5280 CRLReason #9)
  - The CA obtains evidence that the certificate was misused,
  - The cryptographic device used to store the certificate and the private key of the Subject or of the CM no longer complies or will no longer comply with the requirements of chapter 11 of the CP (Ex: a qualification or certification would no longer be maintained or would be suspended),
  - The CA is made aware of a material change in the information contained in the Certificate
  - The CA determines or is made aware that any of the information appearing in the certificate is inaccurate or misleading,
  - The legal representative of the entity to which the service, the server or the Subject belongs notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization,
  - The CA obtains proof that the validation of the authorization of the domain or of the control of one or more FQDNs in the certificate is not reliable.
  - The CA is made aware that the subject has violated one or more of its material obligations under these TCSU.
  - The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn).
- **Cessation of operation** (RFC 5280 CRLReason #5)
  - The final shutdown of the service or the server or the cessation of activity of the CM entity,
  - The departure of the Subject from the entity or the cessation of activity of the entity attached to the Subject,
  - The CM no longer controls, or is no longer authorized to use, all of the domain names in the certificate,
  - The CM will no longer be using the certificate because they are discontinuing their website,
  - 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 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).
- **Affiliation changed** (RFC 5280 CRLReason #3)
  - The information of the service, the server or the Subject 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,
  - Information in the Public Register has changed to substantially affect the validity of the PSD2 attributes in the certificate,
  - the authorization status granted by that NCA has changed (e.g., that PSP is no longer authorized or one of its roles has been revoked).
- **Superseded** (RFC 5280 CRLReason #4)
  - The CM or the Subject has requested a new certificate to replace an existing certificate,
  - The CA obtains reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name in the certificate should not be relied upon,
  - The CA is made aware that the certificate was not issued in accordance with this Certificate Policy or the Certification Practice Statement,
  - The CM, the subject, the entity, if any Certification Agent or DRA operator, has not fulfilled its obligations under this Certificate Policy or the Certification Practice Statement,
  - The certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the Certification Policy,

- **Other reason of revocation which results in no reasonCode extension being provided in the CRL**:
  - The CM or the Subject, the legal representative of the entity to which he/she belongs, requests in writing, without specifying a CRL reason, that the CA revoke the Certificate,
  - The CA obtains evidence that the private key corresponding to the public key in the certificate is suspected of being lost or stolen (or possibly the activation data associated with the private key),
  - The CM or the Subject, the legal representative of the entity to which he/she 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 CA's right to issue certificates under CA/Browsers Forum Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository,
  - Revocation is required by this Certification Policy and/or the Certification Practice Statement for a reason that is not otherwise required to be specified by this section,
  - The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate,
  - 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),
  - 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.

11. 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 encrypt 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.

12. ACCURACY AND LIMIT OF USE

The TSU ensures that its clock is synchronized with UTC within an accuracy of one second.

TIME-STAMPS can be verified at least 2 years after their generation.

TIME-STAMPS issued are not kept and archived by the TSA.

13. 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	
LCR	http://crl.certigna.fr/identca.crl http://crl.dhimyotis.com/identca.crl
OCSP	http://identca.ocsp.certigna.fr http://identca.ocsp.dhimyotis.com
CERTIGNA IDENTITY PLUS CA	
LCR	http://crl.certigna.fr/identityplusca.crl http://crl.dhimyotis.com/identityplusca.crl
OCSP	http://identityplusca.ocsp.certigna.fr http://identityplusca.ocsp.dhimyotis.com

CERTIGNA ENTITY CA	
LCR	http://crl.certigna.fr/entityca.crl
	http://crl.dhimyotis.com/entityca.crl
OCSP	http://entityca.ocsp.certigna.fr
	http://entityca.ocsp.dhimyotis.com
CERTIGNA ENTITY CODE SIGNING CA	
LCR	http://crl.certigna.fr/entitycsca.crl
	http://crl.dhimyotis.com/entitycsca.crl
OCSP	http://entitycsca.ocsp.certigna.fr
	http://entitycsca.ocsp.dhimyotis.com
FR03	
LCR	http://crl.certigna.fr/2ddoc.crl
	http://crl.dhimyotis.com/2ddoc.crl
OCSP	http://2ddoc.ocsp.certigna.fr
	http://2ddoc.ocsp.dhimyotis.com
CERTIGNA SERVICES CA	
LCR	http://crl.certigna.fr/servicesca.crl
	http://crl.dhimyotis.com/servicesca.crl
OCSP	http://servicesca.ocsp.certigna.fr
	http://servicesca.ocsp.dhimyotis.com
CERTIGNA WILD CA	
LCR	http://crl.certigna.fr/wildca.crl
	http://crl.dhimyotis.com/wildca.crl
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.

14. LIABILTY AND INSURANCE

3.1. Liability

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

CERTIGNA'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.

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

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

- Fault, negligence, omission or default of the SUBJECT, The CM or the APPLICANT, 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, The CM or the APPLICANT,
- Delay in providing the data to be processed due to the SUBJECT, The CM or the APPLICANT,
- 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.

CERTIGNA may not be held liable for any unauthorized or improper use of TIME-STAMPS issued by its time-stamping service.

CERTIGNA shall under no circumstances be held liable for any damage caused using the TIME-STAMPS issued by the TSA.

CERTIGNA cannot be implicated by delays or losses that the transmitted data on which a TIME-STAMP is requested by the application service.

CERTIGNA cannot be held liable 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 APPLICANT will be authorized to terminate the contract and there will be no prejudice.

The data transmitted in a TIME-STAMP request and the verification of their value in the associated response remain the responsibility of the APPLICANTS.

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.

15. CONTRACT AND MODIFICATIONS

The CONTRACT cancels any previous commitment.

The SUBSCRIBER, the SUBJECT, the CM or the APPLICANT agrees that during the term of the CONTRACT, CERTIGNA may modify these GCSU unilaterally and at any time. However, the conditions accepted and signed by the SUBSCRIBER, the SUBJECT, the CM or the APPLICANT remain valid throughout the duration of the CONTRACT unless the SUBSCRIBER, the SUBSCRIBER, the SUBJECT, the CM or the APPLICANT explicitly accepts the new conditions issued and published by the CA on the Website or on the DRA's website. The new version of the GCSU will apply to any new order of products on the Website.

16. 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.

17. PRIVACY POLICY

By accepting these GCSU the SUBSCRIBER, the SUBJECT, the CM or the APPLICANT acknowledges having read the CERTIGNA Personal Data Use Policy available on the Website.

The data provided by the SUBSCRIBER, the SUBJECT, the CM or the APPLICANT, when registering on the Website, when ordering and when REQUEST FOR CERTIFICATE are Personal Data, the collection and processing of which are governed by the Aforementioned Personal Data Policy.

18. ASSIGNMENT OF THE CONTRACT

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

19. 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.

20. CERTIGNA CONTACT INFORMATION

20.1. FAQs et customer support

Answers to frequently asked questions can be found in our FAQ section at https://www.certigna.com/faq/.

If you have any other questions, you can contact our Customer Service department as follows:

- Contact e-mail: contact@certigna.fr ;
- Telephone: 0 806 115 115 (Free service) available Monday to Friday from 09:00 to 18:00;
- Chat on the https://www.certigna.com website, available Monday to Friday from 09:00 to 18:00.

20.2. Requesting a révocation

As mentioned in chapter 3.4.2, the certificate revocation request by the CM or Subject, a legal representative of the entity, an DRA operator or, where applicable, a CA, can be made in one of the following ways:

- From the customer area of the CERTIGNA website https://www.certigna.com by selecting the certificate to be revoked;
- By post: by completing and signing the certificate revocation form available on the CERTIGNA website https://www.certigna.com. The applicant authenticates himself by attaching a photocopy of his identity document to the mail sent.

Information on the processing of your personal data is available in the Policy on the use of personal data, which can be accessed at the following address: https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

20.3. Reporting au malicious or dangerous certificate

For reporting a malicious or dangerous certificate (suspected Private Key compromise, certificate misuse, or other types of fraud, compromise, inappropriate conduct, etc.) or any other matter related to certificates, use the contact form available at https://www.certigna.com/contactez-nous/ by selecting "Certificate considered malicious or dangerous".

20.4. Making a complaint

To bring a complaint to CERTIGNA's attention, please use the contact form available at the following address https://www.certigna.com/contactez-nous/ and select the "Réclamation" reason.

You can also make a complaint to our customer service department using the following contact details:

- Contact e-mail: contact@certigna.fr ;
- Telephone: 0 806 115 115 (Free service) available Monday to Friday from 09:00 to 18:00;
- Chat on the https://www.certigna.com website, available Monday to Friday from 9am to 18:00;
- Mail addressed to

CERTIGNA
20 allée de la Râperie
Zone de la plaine
59650 Villeneuve d'Ascq, France

Information on the processing of your personal data is available in the Policy on the use of personal data, which can be accessed at the following address: https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

21. 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".

22. LOSS OF QUALIFICATION/CERTIFICATION OF THE SUPPORT

22.1 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.

22.2 The CRYPTOGRAPHIC DEVICE used if necessary, by CERTIGNA to store and use the private key and the CERTIFICATE of a TSU, 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 maintenance of the device, CERTIGNA will inform the APPLICANT and revoke its CERTIFICATE, without condition of reimbursement on the TIME-STAMP issued with this CERTIFICATE.

23. AVAILABILITY COMMITMENTS FOR CERTIFICATES

The certificate status information feature is available 24 hours a day, 7 days a week with a maximum downtime of the function defined in the following table:

RGS ***	
2 hours	per interruption (failure or maintenance)
8 hours	Per month

RGS **	
4 hours	per interruption (failure or maintenance)
16 hours	Per month

RGS *	
4 hours (workdays)	per interruption (failure or maintenance)
32 hours (workdays)	Per month

The revocation management function is available 24/7 for online revocations with a maximum downtime of the function defined in the following table:

RGS ***	
1 heure	per interruption (failure or maintenance)
4 hours	Per month

RGS **	
2 hours	per interruption (failure or maintenance)
8 hours	Per month

RGS *	
2 hours (workdays)	per interruption (failure or maintenance)
16 hours (workdays)	Per month

24. SERVICE COMMITMENTS FOR THE PREMIUM TIMESTAMP OPTION

Availability commitment:

Certigna is committed to an availability rate of 99.9%, it being specified that an unavailability will be the result of a critical incident defined as the complete interruption of the timestamping service.

The annual availability rate will be calculated on the basis of 365 days of 24 hours, and pro rata temporis for the month of commissioning and for the month of termination of the service.

Only critical incidents of Certigna responsibility are considered in the calculation of annual availability:

- Availability = MTBF / (MTD + MTBF)

Mean Time Between Failures = Sum of correct operation times / number of critical failure incidents

Mean Total Downtime = Total downtime / number of critical incidents

Associated penalty:

If the availability commitment is not reached, the following penalties will apply:

Lack of availability	**Penality** **Expressed as a % of the monthly average of annual invoicing (subscription + token consumption)**
Less than 0,01%	3%
From 0,01% to 0,02%	4%
Over 0,03%	5%

Services Center:

The declaration of an incident shall be made to the email address astreinte@certigna.com

APPENDIX 1: 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:

- **APPLICANT** - Legal or natural person who need to timestamp data by the TIME-STAMP AUTHORITY and who has accepted the present GCSU;
- **CERTIFICATION AUTHORITY (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;
- **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;
- **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.
- **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.
- **CONTRACT:**

  For CERTIFICATES, relations between:
  - CERTIGNA and the SUBSCRIBER who are governed by these GCSU expressly accepted by the SUBSCRIBER when ordering on the Website.
  - CERTIGNA and the SUBJECT or the CM which are framed by these GCSU expressly accepted by the SUBJECT or the CM during each CERTIFICATE REQUEST.

  For TIME-STAMPING TOKENS: relations between CERTIGNA and the APPLICANT framed by these T & Cs expressly accepted by the APPLICANT when ordering TIME- STAMPING TOKENS.

  All the documents to which these GCSU refer, in particular the Policy on the use of personal data available on the Certigna.com site, are also included in the CONTRACT.
- **COORDINATED UNIVERSAL TIME** (UTC) - Time scale based on the second as defined in Recommendation ITU-RTF.460-6.
- **CRL**: Certificate Revocation List;
- **CRYPTOGRAPHIC DEVICE**: USB key, smart card or cryptographic module;
- **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;
- **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.
- **OID** : Object Identifier.
- **PART(S):** Individually the SUBCRIBER, the SUBJECT, the CM or the APPLICANT or the CA, and collectively, the CA and the SUBSCRIBER, the CA and the SUBJECT, the CA and the CM, or the CA and the APPLICANT.
- **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, …
- **REGENERATION:** Operation consisting in issuing a new CERTIFICATE to replace an existing one, with exactly the same information but a different key pair (following the loss of the certificate or the password).
- **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;
- **SUBSCRIBER** :
  - for himself: in this case he is required to respect the obligations of the Subscriber (chapter 8.1) as well as of the SUBJECT or CM (chapter 8.2); or
  - in the name and on behalf of the SUBJECT. In this case he is bound to respect the obligations of the SUBSCRIBER only (chapter 8.1); the obligations of the SUBJECT remaining the responsibility of the latter;
- **TIME-STAMP** – Data in electronic form which binds other electronic data to a time establishing evidence that these data existed at that time.
- **TIME-STAMP POLICY** (TP) – Set of rules that indicates the applicability of a TIME-STAMP to a particular community and/or class of application with common security requirements.
- **TIME-STAMPING SERVICE** - Trust service for issuing TIME-STAMPS.
- **TIME-STAMPING UNIT** (TSU) - Set of hardware and software which is managed as a unit and has a single TIME-STAMP signing key active at a time. TIME STAMP UNITS use TIME STAMP CERTIFICATES issued by the CERTIFICATION AUTHORITY "Certigna Entity CA". These CERTIFICATES have a name with the following syntax "CERTIGNA - TSU <TSU number>".
- **UTC**(k) - Time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.
- **TIME-STAMP USER** – Entity (person or application) which relies on a TIME-STAMP issued under the TIME-STAMP POLICY.
- UNLOCK: Operation consisting of resetting the PIN code of a CRYPTOGRAPHIC DEVICE blocked following the entry of 3 incorrect PIN codes.

APPENDIX 2: CERTIFICATE LIST

The CERTIFICATES covered by these GCSU are as follows:

CERTIGNA ENTITY CA	**1.2.250.1.177.2.6.1**	**RGS**	**ETSI**	**Profil**
Seal for documents	1.2.250.1.177.2.6.1.1.1	RGS *	LCP	CM
Seal for documents	1.2.250.1.177.2.6.1.1.2	RGS *	LCP	CM
Seal for documents	1.2.250.1.177.2.6.1.4.1	RGS **	QCP-l-qscd	CM
Seal for documents	1.2.250.1.177.2.6.1.4.2	RGS **	QCP-l-qscd	CM
Seal for documents	1.2.250.1.177.2.6.1.42.1	RGS **	LCP	CM
Seal for documents	1.2.250.1.177.2.6.1.42.2	RGS **	LCP	CM
Seal for documents	1.2.250.1.177.2.6.1.41.1		QCP-l-qscd	CM
Seal for documents	1.2.250.1.177.2.6.1.41.2		QCP-l-qscd	CM
Seal for documents	1.2.250.1.177.2.6.1.7.1		QCP-l	CM
Seal for documents	1.2.250.1.177.2.6.1.7.2		QCP-l	CM
Seal for documents	1.2.250.1.177.2.6.1.8.1		QCP-l + PSD2	CM
Seal for documents	1.2.250.1.177.2.6.1.8.2		QCP-l + PSD2	CM
Seal for timestamping tokens	1.2.250.1.177.2.6.1.9.1		QCP-l	CM
Seal for timestamping tokens	1.2.250.1.177.2.6.1.9.2		QCP-l	CM
Seal for timestamping tokens	1.2.250.1.177.2.6.1.3.1	RGS *	LCP	CM
Seal for timestamping tokens	1.2.250.1.177.2.6.1.3.2	RGS *	LCP	CM
Seal for timestamping tokens	1.2.250.1.177.2.6.1.6.1	RGS **	QCP-l-qscd	CM
Seal for timestamping tokens	1.2.250.1.177.2.6.1.6.2	RGS **	QCP-l-qscd	CM
CERTIGNA ENTITY CODE SIGNING CA	**1.2.250.1.177.2.8.1**	**RGS**	**ETSI**	**Profil**
Seal for code signing	1.2.250.1.177.2.8.1.1.1	RGS *	LCP	CM
Seal for code signing	1.2.250.1.177.2.8.1.1.2	RGS *	LCP	CM
Seal for code signing	1.2.250.1.177.2.8.1.2.1	RGS **	QCP-l-qscd	CM
Seal for code signing	1.2.250.1.177.2.8.1.2.2	RGS **	QCP-l-qscd	CM
FR03	**1.2.250.1.177.2.2.1**	**RGS**	**ETSI**	**Profil**
Cachet de documents (2D-DOC)	1.2.250.1.177.2.2.1.1	RGS *	LCP	CM
CERTIGNA SERVICES CA	**1.2.250.1.177.2.5.1**	**RGS**	**ETSI**	**Profil**
Authentication for server	1.2.250.1.177.2.5.1.1.1	RGS *	OVCP	CM
Authentication for server	1.2.250.1.177.2.5.1.1.2	RGS *	OVCP	CM
Authentication for client	1.2.250.1.177.2.5.1.2.1	RGS *	OVCP	CM
Authentication for client	1.2.250.1.177.2.5.1.2.2	RGS *	OVCP	CM
Authentication for client/server	1.2.250.1.177.2.5.1.3.1		QEVCP-w	CM
Authentication for client/server	1.2.250.1.177.2.5.1.4.1		QEVCP-w	RC
Authentication for client/server	1.2.250.1.177.2.5.1.4.2		QEVCP-w	RC
Authentication for client/server	1.2.250.1.177.2.5.1.5.1		QNCP-w	CM
Authentication for client/server	1.2.250.1.177.2.5.1.5.2		QNCP-w	CM
CERTIGNA WILD CA	**1.2.250.1.177.2.7.1**	**RGS**	**ETSI**	**Profil**
Authentication for client/server	1.2.250.1.177.2.7.1.1.1		OVCP	CM
Authentication for client/server	1.2.250.1.177.2.7.1.1.2		OVCP	CM
Authentication for client/server wildcard	1.2.250.1.177.2.7.1.2.1		OVCP	CM
Authentication for client/server wildcard	1.2.250.1.177.2.7.1.2.2		OVCP	CM
CERTIGNA IDENTITY CA	**1.2.250.1.177.2.3.1.**	**RGS**	**ETSI**	**Profil**
Encipherment	1.2.250.1.177.2.3.1.1.1	RGS *	LCP	SUBJECT
Encipherment	1.2.250.1.177.2.3.1.1.2	RGS *	LCP	SUBJECT
Encipherment	1.2.250.1.177.2.3.1.3.1	RGS *	LCP	SUBJECT
Encipherment	1.2.250.1.177.2.3.1.3.2	RGS *	LCP	SUBJECT
Authentication & signature	1.2.250.1.177.2.3.1.2.1	RGS *	LCP	SUBJECT
Authentication & signature	1.2.250.1.177.2.3.1.2.2	RGS *	LCP	SUBJECT
Authentication & signature	1.2.250.1.177.2.3.1.4.1	RGS *	LCP	SUBJECT
Authentication & signature	1.2.250.1.177.2.3.1.4.2	RGS *	LCP	SUBJECT

CERTIGNA IDENTITY PLUS CA	**1.2.250.1.177.2.4.1.**	**RGS**	**ETSI**	**Profil**
Authentication & signature	1.2.250.1.177.2.4.1.1.1	RGS **	QCP-n-qscd	SUBJECT
Authentication & signature	1.2.250.1.177.2.4.1.1.2	RGS **	QCP-n-qscd	SUBJECT
Authentification	1.2.250.1.177.2.4.1.2.1	RGS ***	NCP+	SUBJECT
Authentication	1.2.250.1.177.2.4.1.2.2	RGS ***	NCP+	SUBJECT
Signature	1.2.250.1.177.2.4.1.3.1	RGS ***	QCP-n-qscd	SUBJECT
Signature	1.2.250.1.177.2.4.1.3.2	RGS ***	QCP-n-qscd	SUBJECT
Authentication & signature	1.2.250.1.177.2.4.1.4.1	RGS **	QCP-n-qscd	SUBJECT
Authentication & signature	1.2.250.1.177.2.4.1.4.2	RGS **	QCP-n-qscd	SUBJECT
Authentification	1.2.250.1.177.2.4.1.5.1	RGS ***	NCP+	SUBJECT
Authentication	1.2.250.1.177.2.4.1.5.2	RGS ***	NCP+	SUBJECT
Signature	1.2.250.1.177.2.4.1.6.1	RGS ***	QCP-n-qscd	SUBJECT
Signature	1.2.250.1.177.2.4.1.6.2		QCP-n	SUBJECT
Authentication & signature	1.2.250.1.177.2.4.1.7.1		QCP-n	SUBJECT
Authentication & signature	1.2.250.1.177.2.4.1.7.2		QCP-n	SUBJECT
Authentication & signature	1.2.250.1.177.2.4.1.8.1		QCP-n-qscd	SUBJECT
Authentication & signature	1.2.250.1.177.2.4.1.8.2		QCP-n-qscd	SUBJECT