GENERAL TERMS OF USE

The purpose of the present General terms is to clarify the content and provisions for the usage of the certification services proposed by CERTINOMIS, as well as the respective commitments and obligations of the various involved participants.

DEFINITIONS

AGENT: Person who, directly by law or by delegation, has the power to authorise a certificate request bearing the organisation's name. This person may also have other powers in the organisation's name, notably for revocation. In the absence of designation, the legal representative is the sole certification agent.

BENEFICIARY: Natural person identified by the Registration Authority, who is responsible for the CERTIFICATES delivered to him. The beneficiary can be the SUBJECT or the SCO, who makes a commitment regarding its usage conditions and obligations relative to the Certification Authority.

CA: Certification Authority, is in charge of enforcing at least one Certification Policy (CP) and is identified as such in the Certificates, as the issuer of the certificates issued under that certification policy.

CERTIFICATE: Electronic attestation issued by CERTINOMIS that links the data related to the encryption or verification of signatures, exchanges, messages and electronic documents to the BENEFICIARY, in order to ensure their confidentiality or authentication and integrity.

CONTRACT: contractual unit consisting of the present General terms, the Usage Terms for the ordered certificate, the application file as well as the related Certification Policy, found on the site: www.certinomis.fr and applicable on the signing date of the CONTRACT.

CP: Certification Policy; Document establishing the duties and responsibilities of CERTINOMIS, of its CUSTOMERS, AGENTS and BENEFICIARIES involved in the entire lifecycle of a CERTIFICATE (available for consultation at www.certinomis.fr under the "certification policies" heading).

CUSTOMER: Institution, legal or natural person that enters into a contract with CERTINOMIS in order to obtain CERTIFICATES.

MEDIUM: Physical medium (crypto-processor card or memory stick) that notably contains the BENEFICIARY's CERTIFICATE(s). The MEDIUM becomes the CUSTOMER's property upon being provided by CERTINOMIS.

RA: Registration Authority, is in charge of verifying the identifying information of the future subject of a Certificate, as well as possible other specific attributes, before transmitting the corresponding request to the function generating the CERTIFICATE.

SCO: Server Certificate Officer- the natural person responsible for the server Certificate, notably for the usage of this Certificate and of the corresponding key pair, on behalf of the entity to which the IT server identified in this Certificate is attached.

SUBJECT: The natural person identified in the certificate and who holds the private key corresponding with the public key that is in this certificate.

THIRD PARTY USER: Person using a BENEFICIARY's CERTIFICATE in order to verify his identity or to encrypt messages for his attention.

1 Contact info

Information request:

For any question related to purchase of a Certificate or delivery of an ordered Certificate, Customer may contact his sales representative.

For any question related to understanding of the present GTU or of the Certification Policy, Beneficiaries, Agents, and Third Party Users may write to ld-politiquecertification@certinomis.fr

Revocation request:

The revocation can be requested:

○ By the BENEFICIARY, electronically via the Internet site www.certinomis.fr heading "revoking your CERTIFICATE". Identification is performed by means of a revocation code supplied by CERTINOMIS.

○ By letter signed by the applicant. The BENEFICIARY undertakes to sign the revocation request and to provide elements that will allow for sufficiently reliable identification, notably copies of identity documents and powers and/or K-bis excerpt.

○ BY CERTINOMIS in the event of non-compliance with this Agreement by the BENEFICIARY or in case of fraudulent use.

2 Certificate type and usage:

Authentication / Signature / Confidentiality

3 Reliance limits

The beneficiaries must strictly comply with the authorised uses of the key pairs and certificates. In the opposite case, they could be held liable. The authorised use of the key pair and of the associated certificate is also described in the certificate itself, via the extensions relating to the uses of keys. The usage of the private key of the CERTIFICATE attributed to a BENEFICIAIRY is strictly limited to the service defined by the OID of its policy.

The THIRD PARTY USERS must strictly comply with the authorised uses of the certificates. In the opposite case, they could be held liable.

The BENFICIARY acknowledges to know that a fraudulent use or simply non-compliant to present Agreement is a legitimate justification of revocation by the CA.

4 Obligations of subscribers

The BENEFICIARY are required to take all necessary measures in order to ensure the safety of the IT workstations in which the MEDIA are used. When CERTINOMIS provides the MEDIUM, it is compliant with the security requirements contained in Chapters 6 and 12 of the CP.

The BENEFICIARY undertake to carry out the measures needed to ensure the CERTIFICATE's backup. This backup must be retained securely only by the BENEFICIARY.

Should the BENEFICIARY or CERTINOMIS learn of the established or suspected compromise of the confidential data, of any non-compliance with the present Agreement, of the death of the BENEFICIARY, of the cessation of activities of the CUSTOMER or of any modification of the data contained in the CERTIFICATE, they are required to immediately request the revocation of the associated CERTIFICATE and, without delay, to verify the said revocation.

The BENEFICIARY undertake to no longer use a CERTIFICATE after its expiry, after a revocation request or after notification of the CERTIFICATE's revocation, for any reason whatsoever.

In case of a revocation request by the BENEFICIARY, CERTINOMIS revokes the CERTIFICATE within less than twenty-four (24) hours of its verification of the request.

Regardless of the cause behind the revocation, CERTINOMIS notifies the BENEFICIARY of this revocation.

The BENEFICIARY agrees to cease using the private key associated with the CERTIFICATE in the event of a compromise of the CA.
The BENEFICIARY of the certificate agrees to comply with the Certification Policy (CP) and to provide complete and accurate information to the RA, both in the certificate request and for any other request or response addressed to the RA or the CA

Once the certificate delivered, the beneficiary must verify the contents of the certificate. The first use of the certificate shall constitute tacit acceptance of the certificate. Otherwise, the certificate shall be tacitly accepted 15 days after the certificate has been issued.

By accepting a certificate, the recipient expressly acknowledges its consent to the contractual terms and conditions of use and, more generally, to all information published in Certification Policy identified in the Certificate.

The BENEFICIARY agrees to maintain exclusive control of the private key associated with the CERTIFICATE

THE BENEFICIARY UNDERTAKES TO PROVIDE ALL RELEVANT, ACCURATE AND COMPLETE INFORMATION WHEN APPLYING FOR THE CERTIFICATES

5 Obligations of relying parties

The THIRD PARTY USER makes a commitment to verify the usage of the CERTIFICATE in the field «KeyUsage ». This usage can be by instance; signature, authentication, confidentiality.

The THIRD PARTY USER makes a commitment to verify the revocation status of the CERTIFICATE by checking le certificate revocation list indicated by the distribution point of the certificate. In case the CERTIFICATE would come to be revoked, it falls to the THIRD PARTY USER to determine if it is reasonable to grant his trust to the CERTIFICATE. The responsibility of CERTINOMIS shall under no circumstances ne held liable in case of use of a revoked CERTIFICATE.

The THIRD PARTY USER makes a commitment to have a computing equipment being capable of validating the CERTIFICATES and certificates revocation lists.

The THIRD PARTY USER makes a commitment to check that the CERTIFICATE issued by CERTINOMIS is referenced at the level of security and for the trust services required by the application.

The THIRD PARTY USER recognizes that the CERTIFICATES issued by CERTINOMIS are worth proof of the authenticity of the identified entities.

6 Agreement on evidence

By agreeing to these Terms, you expressly agree that any notification or communication between you and Certinomis may be effected by any electronic and paperless means.

As such, and in accordance with Article 1366 of the Civil Code, the Parties acknowledge that the computerized files, data, messages and registers kept in the computer systems of each Party, in particular the recordings and backups made on the site will be admitted as proof of the communications and exchanges between the parties, to the extent that the Party from which they originate can be identified and established and maintained under conditions that guarantee their integrity.

7 Limitations of warranty and liability

Certinomis is subject to a general obligation of means.

CERTINOMIS assumes no commitment and no responsibility as for the shape, the smugness, the accuracy, the authenticity, the forgery or the legal effect of documents provided with CERTIFICATE request by the CUSTOMER.

Under no circumstances will CERTINOMIS in any way intervene in the contractual relations that may be established between the BENEFICIARIES and the THIRD PARTY USERS of the said CERTIFICATES.

CERTINOMIS assumes no commitment neither responsibility as for the consequences of the delays nor the losses that any electronic messages, letters, documents could undergo in their transmission, neither any changes nor other errors which can occur in the transmission of any electronic communication.

CERTINOMIS cannot be held liable in the event of the compromise of the private key belonging to the BENEFICIARY. CERTINOMIS is not entrusted with the safekeeping and/or protection of the BENEFICIARY's private key, for which the latter is personally responsible.

The parties formally agree that under no circumstances can CERTINOMIS be held liable if the BENEFICIARY has not carried out the certificate revocation request in compliance with the provisions contained herein.

The parties formally agree that under no circumstances can CERTINOMIS be held liable if the AGENT or BENEFICIARY has not carried out the certificate revocation request in compliance with the provisions contained herein.

Certinomis shall not be liable in the following cases:

- in the case of use of the CLE PRIVEE or a CERTIFICATE for purposes other than those provided for in the TOU or the CP relating thereto;
- for failure to perform the services due to the unforeseeable and insurmountable fact of a third party;
- in case of force majeure, as defined by law and French jurisprudence;

Barring mandatory provisions to the contrary, Certinomis may in no case be liable, when acting in the course of their professional activity, vis-à-vis the CUSTOMER, an AGENT, a BENEFICIARY or a THIRD PARTY USER using a CERTIFICATE or relying on a CERTIFICATE issued by Certinomis for (i) any type of damage, loss, cost or expense of a special, incidental, indirect, consequential, punitive or penal nature, or for (ii) the losses of profits, business losses, contract losses, loss of enjoyment, loss of reputation or loss, or damage to, the data, even though b has or should have known of the possibility of such damage.

8 Applicable CP

The OIDs of the CPs applicable for the present GTU are:

Elementary Level

1.2.250.1.86.2.3.4.1.1 ; 1.2.250.1.86.2.3.4.2.1 ; 1.2.250.1.86.2.3.4.3.1 ; 1.2.250.1.86.2.3.4.10.1
1.2.250.1.86.2.3.5.30.1

RGS 2 stars and qualified eIDAS Level

1.2.250.1.86.2.3.6.1.1 ; 1.2.250.1.86.2.3.6.2.1 ; 1.2.250.1.86.2.3.6.10.1 ; 1.2.250.1.86.2.3.6.30.1
1.2.250.1.86.2.6.6.1.1 ; 1.2.250.1.86.2.6.6.2.1 ; 1.2.250.1.86.2.6.6.10.1 ; 1.2.250.1.86.2.6.6.30.1 ; 1.2.250.1.86.2.6.6.40.1

9 Privacy policy

As part of its activity of Trust Service Provider Certinomis collects and processes pieces of information related to natural persons who are BENEFICIARY of a CERTIFICATE.

The measures taken by Certinomis to guarantee the respect of your rights and the safety of your personal data in accordance with the provisions of the French law n°78-17 of 6 January 1978 and of the European Regulation UE 2016/679 of 27 April 2016 are detailed on this page https://www.certinomis.fr/en-legal-mentions

The personal data relative to the BENEFICIARY that are submitted and held by CERTINOMIS as part of the CONTRACT are compliant with the applicable substantive law in terms of personal data and cannot be disclosed without having obtained the prior consent of the BENEFICIARY

The BENEFICIARY can access, rectify, update or delete their personal data through the electronic address indicated within the framework of the procedures available on the website www.certinomis.fr in the event that they are inaccurate, incomplete or outdated.

The BENEFICIARY is informed and gives its explicit consent by signing the present Agreement that Certinomis will keep the personal data he communicated for obtaining his CERTIFICATE for a minimum time period of seven (7) years and maximum time period of ten (10) years after the issuance date of his CERTIFICATE.

Particularly, the BENFICIARY is informed and accepts that logs and event logs of the CA will be kept for a minimum period of time of ten (10) years.

Under no circumstances will CERTINOMIS in any way intervene in the contractual relations that may be established between the BENEFICIARIES and the THIRD PARTY USERS of the said CERTIFICATES.

10 Refund policy

The commercial policies of CERTINOMIS are defined by the terms of sale annexed with the CERTIFICATE request or to the applicable contract.

11 Applicable law, dispute resolution

The parties undertake to seek an amicable agreement in the event of a dispute: at the initiative of the requesting party, a meeting shall be held within eight (8) days in Certinomis' premises or in virtual form. Any dispute settlement agreement shall be recorded by writing on a document signed by a duly accredited representative of both party.

In case of dispute related to the interpretation, formation or performance of the present policy, and in the absence of an amicable agreement or settlement, the parties confirm the formal and exclusive competence of the Paris courts, notwithstanding multiple defendants, summary order and activation of guarantees or protective measures.

In case of dispute related to the interpretation, formation or performance of the present policy, the parties confirm the formal and exclusive competence of the French law.

12 Repository licenses and audit

Licenses and audits granted to CERTINOMIS are published on LSTI web site: https://www.lsti-certification.fr/index.php/en/ and also on the ANSSI web site: https://cyber.gouv.fr/la-liste-nationale-de-confiance

SIGNATURES, APPROVALS

I THE UNDERSIGNED CONFIRM HAVING REVIEWED AND ACCEPTED THE PRESENT GENERAL USAGE TERMS.

ON:...../...../..... IN: .....

SIGNATURE OF THE CERTIFICATE BENEFICIARY