GENERAL TERMS OF USE

These General Terms are intended to specify the content and terms of use of the certification services offered by CERTINOMIS as well as the respective commitments and obligations of the various stakeholders involved.

DEFINITIONS

CA: Certification Authority, responsible for the application of at least one certification policy (CP) and identified as such, as the issuer in the certificates issued under this certification policy.

RA: Registration Authority, responsible for verifying the identification information of the future subject of a certificate, as well as possibly other specific attributes, before transmitting the corresponding request to the function generating the electronic certificates.

CP: Certification Policy; Document establishing the duties and responsibilities of CERTINOMIS, its CLIENTS, MANDATARIES, and BENEFICIARIES involved in the entire lifecycle of a CERTIFICATE (available at www.certinomis.com under "certification policies").

CERTIFICATE: Electronic attestation issued by CERTINOMIS linking the data related to the encryption or signature verification of exchanges, messages, and electronic documents to the BENEFICIARY, to ensure confidentiality, authentication, and integrity.

BENEFICIARY: Natural person identified by the RA, who is responsible for the CERTIFICATES issued to them. The beneficiary commits to the terms of use and obligations towards the CA.

HOLDER: The natural person identified in the certificate and who is the holder of the private key corresponding to the public key in this certificate.

SC: Server Certificate Manager - The natural person responsible for the server certificate, including the use of this certificate and the corresponding key pair, on behalf of the entity to which the identified server in the certificate belongs.

CLIENT: Organization, legal or natural person who contracts with CERTINOMIS to obtain CERTIFICATES.

CONTRACT: Contractual set consisting of these General Terms, the Terms of Use of the ordered certificate, the application file, and the relevant Certification Policy available on the website: www.certinomis.com applicable at the date of conclusion of the CONTRACT.

MANDATORY: Person having, directly by law or by delegation, the power to authorize a certificate request bearing the name of the organization. They may also have other powers on behalf of the organization, such as revocation. In the absence of designation, the legal representative is the sole certification mandatory.

THIRD-PARTY USER: Person using the CERTIFICATE of a BENEFICIARY to verify their identity or to encrypt messages intended for them.

1 Contact

INFORMATION REQUEST:

For any request related to the purchase of a certificate or the issuance of an ordered certificate, the Client can contact their commercial representative.

For any request related to the understanding of these Terms of Use or the Certification Policy, agents, beneficiaries, or third-party users can write to ld-politiquecertification@certinomis.fr.

Revocation request:

Revocation can be requested:

□ By the BENEFICIARY, if the requester does not wish to specify a reason for revocation, electronically from the website www.certinomis.fr under the "revoke your CERTIFICATE" section. Identification is done using a revocation code provided by CERTINOMIS;

□ By a duly completed and signed paper form by the requester. The CLIENT, the AGENT, or the BENEFICIARY commit to signing the revocation request and providing elements that allow sufficiently reliable identification, including copies of identity documents and powers and/or K-bis extract. The form is available at https://www.certinomis.fr/revoquer-votre-certificat;

□ By Certinomis in case of non-compliance with these terms by the Beneficiary or in case of fraudulent use.

Possible reasons for revocation:

When making a revocation request, the requester has the option to specify the reason for the revocation request. The different possibilities are:

- keyCompromise (RFC 5280 CRLReason #1): indicates that it is known or suspected that the requester's private key has been compromised;

- affiliationChange (RFC 5280 CRLReason #3): indicates that the requester's name or other identity information of the BENEFICIARY in the CERTIFICATE has changed, but there is no reason to suspect that the private key has been compromised;
- superseded (RFC 5280 CRLReason #4): indicates that the certificate is replaced because: the requester has requested a new certificate, or the certificate must be revoked as it no longer complies with the requirements of the CP or the certification practice statement;
- cessationOfOperation (RFC 5280 CRLReason #5): indicates that the website using the CERTIFICATE is closed before the CERTIFICATE expires, or the RC no longer owns or controls the domain name present in the CERTIFICATE before the CERTIFICATE expires;

2 Types of Certificates and Uses:

Server Authentication Certificate

3 Usage Limitations

The BENEFICIARIES must strictly adhere to the authorized uses of the key pairs and certificates. In the case of fraudulent use, their responsibility could be engaged. The authorized use of the key pair and the associated certificate are also indicated in the certificate itself, through the extensions concerning key usages. The use of the HOLDER's private key and the associated certificate is strictly limited to the service defined by the identifier of their PC.

THIRD-PARTY USERS of certificates must strictly adhere to the authorized uses of the certificates. In the case of fraudulent use, their responsibility could be engaged.

The Beneficiary acknowledges being informed that fraudulent use or even simply non-compliance with these T&Cs is a legitimate reason for revocation by the CA.

4 Obligations

The CLIENT is obligated to take all necessary measures to ensure the security of the computer systems of the BENEFICIARIES and the MANDATARIES on which the MEDIA are used.

The MANDATARY and the BENEFICIARY commit to taking the necessary measures related to the backup of the CERTIFICATE. This backup must be securely kept by the BENEFICIARY alone.

Knowledge of the confirmed or suspected compromise of confidential data, non-compliance with these general conditions, cessation of the CLIENT's activity, or modification of the data contained in the CERTIFICATE by the CLIENT, the MANDATARY, the BENEFICIARY, or CERTINOMIS, entails the obligation, on their part, to immediately request the revocation of the associated CERTIFICATE and to proceed, without delay, to verify said revocation.

The MANDATARY and the BENEFICIARY commit to no longer using a CERTIFICATE following its expiration, a revocation request, or notification of the CERTIFICATE's revocation, regardless of the cause.

In the event of a revocation request by the CLIENT, the MANDATARY, or the BENEFICIARY, CERTINOMIS revokes the CERTIFICATE within a period of less than twenty-four (24) hours from the verification of the request.

Regardless of the cause leading to the revocation, CERTINOMIS notifies the MANDATARY and/or 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 commits to comply with the Certification Policy (CP) and to provide complete and accurate information to the AE, both in the certificate request and for any other request from the AE or the CA.

The BENEFICIARY must verify the content of the CERTIFICATE. The BENEFICIARY has a period of 15 days following the issuance date of the CERTIFICATE to express their non-consent to the CA (by phone, email, or simple mail).

The BENEFICIARY agrees to install the CERTIFICATE only on the servers concerned by the "Subject Alternative Name" (SAN) field of the CERTIFICATE.

The BENEFICIARY acknowledges that the first use of the CERTIFICATE constitutes acceptance.

The RC commits, according to the chosen option, to using MEDIA that comply with the security requirements listed in Chapters 6 and 12 of the PC.

The RC commits to taking reasonable measures to protect the private key corresponding to the public key of the CERTIFICATE.

The MANDATARY commits, during the validity period of the certificates, to declare to CERTINOMIS all departures or changes of RC.

5 Obligations of Third-Party Users

The THIRD-PARTY USER commits to verifying the usage indicated in the CERTIFICATE. This usage can be, for example, signature, authentication, or encryption.

The THIRD-PARTY USER commits to verifying the revoked or non-revoked status of a CERTIFICATE by checking the list of revoked certificates indicated by the distribution point present in the certificate. In the event that the CERTIFICATE is revoked, it is the responsibility of the THIRD-PARTY USER to determine whether it is reasonable to trust the CERTIFICATE. CERTINOMIS cannot be held liable in any case of certificate revocation.

The THIRD-PARTY USER commits to having sufficient computer equipment to perform the verification of CERTIFICATES and the lists of revoked certificates.

The THIRD-PARTY USER commits to ensuring that the CERTIFICATE issued by CERTINOMIS is referenced at the required security level and for the trust service required by the application. For QNCP-w and QEVCP-w level CERTIFICATES, the THIRD PARTY USER undertakes to use the list of trusted services (EUTL) published by the European Commission to verify the CERTIFICATE: https://webgate.ec.europa.eu/tl-browser/.

The THIRD-PARTY USER acknowledges that the CERTIFICATES issued by CERTINOMIS serve as proof of the authentication of the IDENTIFIED ENTITIES.

6 Warranty and Liability Limitations

Under no circumstances does CERTINOMIS intervene, in any way whatsoever, in the contractual relationships that may be established between the CLIENTS, MANDATARIES, or BENEFICIARIES and the THIRD-PARTY USERS of the said CERTIFICATES.

CERTINOMIS assumes no commitment or responsibility regarding the form, sufficiency, accuracy, authenticity, forgery, or legal effect of the documents submitted during the CERTIFICATE request by the CLIENT.

CERTINOMIS assumes no commitment or responsibility for the consequences of delays or losses that may occur in the transmission of any electronic messages, letters, documents, nor for delays, alterations, or other errors that may occur in the transmission of any electronic communication.

CERTINOMIS's liability cannot be engaged in the event of the compromise of the private key of the MANDATARY or the BENEFICIARY. CERTINOMIS is not entrusted with the storage and/or protection of the BENEFICIARY's private key, which is their personal responsibility.

The parties expressly agree that, in no way, can CERTINOMIS's liability be engaged as long as the MANDATARY or the BENEFICIARY has not made a certificate revocation request in accordance with the stipulations herein.

7 Certification Policies

The identifiers of the applicable CPs for these T&Cs are:

1.2.250.1.86.2.6.8.63.1: client and server authentication, based on CP EN 319 411-2 QEVCP-w (0.4.0.194112.1.4)
1.2.250.1.86.2.6.8.62.1: client and server authentication, based on CP EN 319 411-2 QNCP-w (0.4.0.194112.1.5)
1.2.250.1.86.2.6.7.20.1: server authentication, based on CP EN 319 411-1 OVCP (0.4.0.2042.1.7) and RGS 1 star
1.2.250.1.86.2.6.7.61.1: client and server authentication, based on CP EN 319 411-1 OVCP (0.4.0.2042.1.7)
1.2.250.1.86.2.6.7.60.1: client and server authentication, based on CP EN 319 411-1 DVCP (0.4.0.2042.1.6)

The correspondance beween commercial products and OID of CPS is as follows :
s-ULTRA: 1.2.250.1.86.2.6.8.63.1 (QEVCP-w)
s-SECURE: 1.2.250.1.86.2.6.8.62.1 (QNCP-w)
s-RGS: 1.2.250.1.86.2.6.7.20.1 (RGS 1 étoile)
s-ORGA: 1.2.250.1.86.2.6.7.61.1 (OVCP)
s-WEB: 1.2.250.1.86.2.6.7.60.1 (DVCP)

8 Privacy Policy

As part of its activity as an Electronic Certification Service Provider, Certinomis collects and processes information relating to natural persons who are beneficiaries of an electronic certificate or identified as legal representatives, certification agents, or billing contacts of a client organization.

The measures taken by Certinomis to ensure the respect of your rights and the security of your personal data in accordance with the provisions of Law No. 78-17 of January 6, 1978, and the European Regulation EU 2016/679 of April 27, 2016, are detailed on this page: https://www.certinomis.fr/mentions-legales.

The personal data relating to the MANDATARY and the BENEFICIARY transmitted and held by CERTINOMIS within the framework of the CONTRACT are in compliance with the current positive law regarding personal data and cannot be disclosed. The MANDATARY and the BENEFICIARY can obtain communication of their personal data, have them corrected, updated, or deleted at the email address mentioned in the procedures available on the website www.certinomis.com when they are inaccurate, incomplete, or outdated.

The BENEFICIARY is informed and explicitly consents by signing these presents that Certinomis retains the personal data they have communicated for the purpose of obtaining their certificate for a minimum period of seven (7) years and a maximum of ten (10) years from the date of issuance of their certificate.

The BENEFICIARY is notably informed and accepts that the logs and event journals of the Certification Authority are kept for ten (10) years.

Under no circumstances does CERTINOMIS intervene, in any way whatsoever, in the contractual relationships that may be established between the CLIENTS, MANDATARIES, or BENEFICIARIES and the THIRD-PARTY USERS of the said CERTIFICATES.

9 Refund Policy

CERTINOMIS’s commercial policies are defined by the sales conditions attached to the order or the applicable contract.

10 Applicable Law, Dispute Resolution

The parties commit to seeking an amicable agreement in case of a dispute: at the initiative of the requesting party, a meeting will be organized within eight days at Certinomis’s premises or in a virtual form. Any agreement to settle the dispute must be recorded in writing on a document signed by an accredited representative of both parties.

In case of a dispute related to the interpretation, formation, or execution of the CONTRACT and failing to reach an amicable agreement, the parties expressly and exclusively grant jurisdiction to the competent courts of Paris, notwithstanding multiple defendants or summary proceedings or third-party claims or protective measures.

In case of a dispute related to the interpretation, formation, validity, or execution of the CONTRACT, the parties expressly and exclusively grant jurisdiction to French law.

11 References and Audits

The CERTIFICATE is issued in compliance with the applicable standards according to the targeted security level. A compliance audit is conducted at least once a year according to the applicable standards defined for each type of CERTIFICATE (see chapter 7 of these T&Cs).

The audits and references obtained by CERTINOMIS are published on the LSTI website: http://www.lsti-certification.fr as well as on the ANSSI website: https://cyber.gouv.fr/produits-services-qualifies

SIGNATURES, APPROVALS

I, THE UNDERSIGNED, CERTIFY THAT I HAVE READ AND ACCEPTED THESE TERMS AND CONDITIONS OF USE.

ON : ……/…/…AT : ……………………………

SIGNATURE OF THE CERTIFICATE BENEFICIARY