



1. Purpose

The aim of these General Terms and Conditions of Use (GTCU) is to set out the legal, technical and financial conditions for the Customer to obtain SSL Certificates from Keynectis, as well as the terms of use and the Parties' respective obligations.

The Customer's request for an SSL Certificate on the Keynectis website (hereinafter: the "Order") will be regarded as the Customer's unconditional and irrevocable agreement to comply with these GTCU, and as a waiver of its own general terms of purchase. No Order may be cancelled or amended by the Customer without the prior written consent of Keynectis.

2. Definitions

Certificate Authority (or CA): means one of the components of the Public Key Infrastructure (PKI) that generates and revokes SSL Certificates in accordance with the rules and practices it has set forth in its Certificate Policy (CP).

Within the framework hereof, the Certificate Authority that issues Domain Validated (DV) and Organization Validated (OV) SSL Certificates is the CA of the company Keynectis, called "Class 2 KEYNECTIS CA".

The Certificate Authority that issues Extended Validation (EV) SSL Certificates is called "KEYNECTIS Extended Validation CA".

These two CAs are technically and hierarchically linked to the Root CA of Keynectis ("Certplus Primary CA Class 2").

Registration Authority (or RA): means one of the components of the PKI, recognized by the CA, to authenticate and validate the identity of SSL certificate requesters, in accordance with the procedures defined by the Certificate Authority in its Certificate Policy. Within the framework hereof, the RA means the KEYNECTIS customer service.

SSL Certificate or Certificate: means an electronic certificate whose purpose it to enable a "Secure Socket Layer" (SSL) connection to be established between a website server on which an SSL Certificate has been installed and the website to which the certificate User connects using a certified domain name.

Customer: means any person, company or entity that submits a request to Keynectis for an SSL Certificate to enhance the security of its website, as part of its professional activity, and that enters into a contract with Keynectis.

Contract: means the contractual whole made up of the following, in decreasing order of priority: (i) these General Terms and Conditions of Use; (ii) the Certificate request form; (iii) the applicable procedures accessible on the Keynectis website, including the Certificate Policy; (iv) the Customer Order.

Certificate Revocation List (or CRL): means the list of invalid Certificates revoked before their expiration date. This list is issued periodically and is digitally signed by the CA that issued the Certificates contained in the list.

Domain Name: means the identifier of the website to be secured as indicated in the Customer's Order. It comprises several components: (i) the root, which in principle is the name of the company or activity; (ii) an extension or suffix separated from the root by a period. These two components are placed side by side to form the domain name.

Certificate Policy: means the set of rules identified by an OID and published by the CA describing the general characteristics of the Certificates it issues. The Certificate Policy also describes the obligations and responsibilities of the CA, the RA, the Customer and all of the PKI components involved throughout the lifecycle of a Certificate. Within the framework hereof, the Customer must comply with the rules set out in the applicable Certificate Policy (CP) which can be viewed at the following Internet address: <http://www.keynectis.com/CP>.

Certificate User: means a person or machine that trusts SSL Certificates and the CA certification path, in order to identify and authenticate a domain name and the entity whose domain name is included in the SSL Certificate.

3. Description of the SSL certification service

The terms of use of the KEYNECTIS electronic certification service are set out in and regulated by the Certificate Policy of the KEYNECTIS Certificate Authority, which forms an integral part hereof.

The Certificate Policy and all subsequent versions are published on the KEYNECTIS website at the following address: <http://www.keynectis.com/PC>. By accepting these general conditions, the Customer acknowledges that it has read and is bound by the terms of the Certificate Policy applicable on the Order date and its subsequent updated versions.

4. Processing requests to issue SSL Certificates

On receipt of an online request for an SSL Certificate submitted by a Customer, the RA verifies all the information and documentation provided by the Customer.

In addition, the RA verifies receipt of the Order and its payment in full.

On making its request, the Customer undertakes to provide all the useful, accurate and complete information required for the creation or renewal of a Certificate.

The Customer must notify KEYNECTIS in writing of any modification of information designated as mandatory, and provide the required supporting documentation.

In any event, the Customer will be notified by KEYNECTIS if its request dossier is incomplete or if any of the required information has not been provided to Keynectis. In this case, the SSL Certificate request will be put on hold by KEYNECTIS until the dossier is complete.

In any event, the SSL Certificate will only be delivered to the Customer upon receipt of full payment for the Order.



Once it has retrieved and installed its Certificate, the Customer must inspect its content and inform KEYNECTIS if any errors are found. In this case, KEYNECTIS shall revoke said Certificate and issue a new, rectified Certificate.

5. SSL Certificate lifespan

The SSL Certificate has a validity period of one (1), two (2) or three (3) year(s) depending on the option chosen by the Customer. This period begins as from its date of issuance by the Certificate Authority.

6. SSL Certificate renewal

SSL Certificate renewal implies the generation of a new Certificate and is carried out according to the same procedure as an initial Certificate request.

7. SSL Certificate revocation

The SSL Certificate may be revoked when the link connecting it to the associated public key is no longer valid.

The Customer must immediately inform KEYNECTIS thereof and submit an online request to revoke the Certificate in the following cases:

- Actual or suspected compromise of the security of its private key;
- Detection of erroneous information contained in the certificate;
- Modification of a piece of information contained in the certificate;
- Modification of the domain name or of the name of the enrolled organization.

The Customer's revocation request is processed according to the same procedure as that which is used to issue an SSL Certificate.

Keynectis reserves the right to revoke the Certificate with immediate effect and without notice if it discovers that the information contained in the Certificate is no longer valid.

The revoked Certificate will be added to the CRL within twenty-four (24) hours at most following its revocation.

8. Term of the Contract

This Contract takes effect on the date of order of the SSL Certificate by the Customer and ends on the validity end date of the certificate ordered and issued.

In the event of failure by one of the Parties to fulfill one of its contractual obligations, not remedied within 30 clear days of receipt of a letter sent by registered mail with acknowledgement of receipt precisely identifying the failure in question and requesting that it be remedied, termination will be effective as of right. This termination shall be performed without prejudice to any claim for damages to which the non-defaulting party may be entitled. In the event of termination for failure by the Customer consisting in a security defect attributable to the Customer, KEYNECTIS reserves the right to immediately revoke its SSL certificate.

9. Financial conditions

The applicable price of the SSL Certificate is the one indicated in the KEYNECTIS online offer on the date of the subscription or renewal of said SSL Certificate. SSL Certificate tariff conditions depend on their validity period and on the type of Certificate chosen by the Customer.

Following receipt by Keynectis of the Customer's Certificate request, an invoice will be sent by email to the Customer. The invoice is payable online by bank card, bank transfer or check. On receipt of the Customer's payment, KEYNECTIS shall proceed with Certificate issuance.

In the event of an incomplete request dossier rendering issuance of the ordered Certificate impossible, KEYNECTIS reserves the right to retain the amount paid by the Customer when the order was placed. If an Order cancellation request is sent to Keynectis by registered mail with acknowledgement of receipt within one month as from the order date, the amount paid will be retained in full by Keynectis as a penalty payment.

10. Restrictions on usage

The Customer undertakes to use the Certificates it has been issued only on its own behalf.

The Customer therefore undertakes not to use its Certificate on behalf of another organization or to use its private or public key in operations with any domain name or organization name other than the one stated in its certificate request.

The Customer undertakes not to download the Certificate onto more than one workstation.

The Customer undertakes not to use the Certificate and its associated private key on a number of servers or physical devices greater than the number of licenses purchased.

Furthermore, the Customer is informed that the use without a license of an SSL Certificate on a server or device hosted by a server is an act of piracy, and the offenders will be prosecuted within the limits authorized by the law.

11. Undertakings of the Customer

The Customer undertakes to follow the online Certificate request steps on the Keynectis website and to submit to Keynectis all information needed to process the Order and issue the Certificate.

The Customer undertakes to ensure that the information submitted for issuing the Certificate (i) is accurate; (ii) does not constitute a violation of the intellectual property rights of a third party; (iii) have not been and will not be used for illegal purposes.

The Customer undertakes to use the SSL Certificate and all the other issuance, renewal and revocation services provided by the Certificate Authority in accordance herewith and with the provisions of the Certificate Policy.



The Customer undertakes to take all appropriate measures to ensure the security of the server on which the Certificate is installed and to make all arrangements needed to securely safeguard the Certificate.

In addition, the Customer undertakes to maintain and protect the confidentiality and integrity of its private key and to not disclose it any way whatsoever. It guarantees that it is the only person in possession of its private key, password, personal identifier and any software or hardware device used to protect its private key, and that no unauthorized individuals have been or will be granted access to these elements.

In this regard, it alone will bear any damaging consequences that could result from the use of its private key and Certificate by a third party that gained access thereto by any means whatsoever.

If a change were to affect the Customer's organization or the domain name recorded in the Certificate, the Customer must immediately submit an online Certificate revocation request. In this context, the Customer undertakes to cease using the Certificate in question.

Following expiry or notification of revocation of the Certificate, the Customer undertakes to permanently remove the Certificate from the server on which it is installed and must cease using the Certificate for any reason whatsoever.

12. Undertakings of Keynectis

Keynectis is bound by a best endeavors obligation for all obligations relative to the management of the lifecycle of the SSL certificates it issues

It shall make available to the Customer a request enrollment Web interface.

It reserves the right to suspend access to the site whenever it deems necessary due to an event that is likely to affect the site's operation or integrity, for as long as required by the corrective action.

Keynectis undertakes to make available to the Customer a customer service which, in its capacity as RA, shall handle questions relating to requests to issue, renew or revoke an SSL Certificate. The opening times of the Keynectis customer service are Monday to Friday, 9 a.m. to 6 p.m., French time, excluding public holidays. The Keynectis customer service can be contacted by email or phone.

13. Liability

13.1 Liability of the Customer

The Customer acknowledges that it has read and accepts the exclusions and disclaimers contained herein and in the Certificate Policy.

The Customer is solely responsible for generating, maintaining and protecting its private key.

Furthermore, the Customer undertakes to protect Keynectis against all claims or legal action by a third party invoking:

- Failure to fulfill one of its contractual obligations, in particular those specified in Article 11 hereinabove;
- Any misleading declaration or false information provided in its Certificate request;
- Any violation of intellectual property rights by any third-party private individual or legal entity involving information or content it provided to KEYNECTIS;
- The impossibility of publishing certain elements of its certificate request due to the presence of false information or omissions resulting from negligence or the intention to harm a third party;
- Its inability to protect its private key or take the necessary security measures to prevent the compromise, loss, alteration or unauthorized use of its private key.

In this respect, the Customer shall cover all financial consequences resulting from such action, in particular damages and expenses.

13.2 Liability of KEYNECTIS

KEYNECTIS shall not be held liable for the form, adequacy, accuracy, authenticity, falsification or legal effect of the documents and information provided for requests to issue, renew or revoke a Certificate.

KEYNECTIS shall guarantee neither the accuracy of the information provided by the Customer to the Certificate User, nor the consequences of negligence or lack of precaution or security attributable to the Customer.

In addition, the Customer shall remain liable with respect to KEYNECTIS for any unauthorized use of the SSL Certificate and for any compromise, disclosure, loss, theft, modification or unauthorized use of its private key.

KEYNECTIS assumes no obligation or liability for the consequences of any delays; loss; alteration; destruction; fraudulent use of data; or accidental transmission of a virus or any other harmful element via any telecommunication means such as the Internet. Furthermore, KEYNECTIS shall not be held liable for the quality of the Customer's Internet connection.

If the liability of KEYNECTIS is invoked by virtue of these General Terms and Conditions of Use, it is expressly agreed that KEYNECTIS would be obliged to redress certain direct and immediate losses, upon presentation by the Customer of supporting evidence, within the following maximum limits:

- For the Order of a Domain Validated Certificate, within a limit that may not exceed 10,000 euros;
- For the Order of an Organization Validated K.SSL Certificate, within a limit that may not exceed 50,000 euros;
- For the Order of an Extended Validation SSL Certificate, within a limit that may not exceed 100,000 euros.

KEYNECTIS shall assume no liability arising out of the failure by the Customer to comply with the obligations defined herein and in the Certificate Policy.



KEYNECTIS shall not be held liable for any indirect or unforeseen damage suffered by the Customer, including loss of profits, sales, contracts, revenue, anticipated revenues or savings; loss of clientele, operating loss, damage to its brand image, loss or use of data, inaccuracy or corruption of files in relation to or resulting from the non-execution or faulty execution of these General Terms and Conditions or inherent to the use of Certificates issued by KEYNECTIS.

Any damage caused by force majeure as defined in Article 14 hereinafter is also excluded from any claim for compensation.

14. Force majeure

The Customer is informed that should a case of force majeure occur, the performance of the obligations of KEYNECTIS as defined herein shall be suspended without KEYNECTIS being held liable. Force majeure refers to any event external to one of the Parties, as defined in the case law of French courts and by Article 1148 of the French Civil Code, including total or partial strikes, within or outside the company; bad weather; epidemics; blockage of means of transportation or supply, for whatever reason; earthquake; fire; storm; flood; water damage; governmental or legal restrictions; viruses; computer breakdowns; blockage of telecommunications, including the switched network; any incident arising on the network of a third-party operator; labor disputes other than those directly involving one of the Parties; power outages, failure of the Parties' or a third-party's IT system, of the network or of telecommunications installations or networks.

15. Intellectual property

KEYNECTIS shall retain all intellectual property rights concerning its products, software, services, concepts, techniques, inventions, processes, know-how and work it developed, integrated or used as part of the SSL Service that it provides under these General Terms and Conditions, in particular all derived works, modifications, enhancements, configurations, translations, upgrades and interfaces.

Consequently, no property or license rights are transferred to the Customer with regard to these elements.

16. Personal data protection

Each of the Parties shall take all appropriate measures to protect personal data and comply, for the performance hereof, with the obligations arising under national, European and, if applicable, international legislation pertaining to personal data protection. Each of the Parties shall ensure that it complies with the statutory provisions in force regarding personal data protection and, in particular, with the French Data Protection Act of 6 January 1978, amended by the Law of 6 August 2004, and shall carry out the necessary formalities or ensure that they are carried out.

In addition, the Customer contact person authorized to carry out any act necessary for the performance hereof (in particular certificate requests) on behalf of the Customer has the right to access, rectify and delete said Customer's personal data. This right can be exercised by contacting the KEYNECTIS Data Protection Correspondent at the following address: sandrine.barilli@keynectis.com

17. Confidentiality

Each Party undertakes to maintain the confidentiality of all information identified as confidential provided within the framework hereof by the other Party, and not to disclose it to any third party throughout the term hereof and for a period of five (5) years following the expiry or termination hereof.

18. Miscellaneous

18.1 Communication

The Customer authorizes KEYNECTIS to cite its name, logo or brand as a commercial reference in any marketing or commercial documentation, including on its website.

18.2 Transfer of the Contract

The Parties agree not to transfer the Contract and the rights and obligations taken separately without the other Party's express prior agreement.

18.3 Insurance

Keynectis certifies that it has taken out Professional Liability Insurance concerning the services related hereto.

18.4 Agreement on evidence

With regard to the exchange of messages between the parties, the date of receipt of a message by the recipient and the signature of this message serve as evidence to the parties and establish that said message is attributable to the party having issued it.

18.5 Invalidity of any clause – Nullity

If one or more provisions herein are deemed to be invalid or declared as such under any law or regulation or following a final decision of any competent court, the other provisions will remain fully valid unless they are not dissociable from the invalid provision.

The nullity of any clause herein does not affect the validity of the other clauses; the Contract is continued in the absence of the cancelled clause unless the cancelled clause renders its continuation impossible or unbalanced in relation to the initial agreements.

18.6 Notifications

Any notification sent hereunder shall be sent by registered mail with acknowledgement of receipt to the Parties' head offices. Any claim from the Customer must, on pain of debarment, be sent by registered mail with acknowledgement of receipt to the Contract signatory within one (1) month of the occurrence of the event giving rise to said claim.

**19. Assignment of jurisdiction – Applicable law**

THE LAW APPLICABLE HERETO IS FRENCH LAW. IN THE EVENT OF DISPUTE REGARDING THE INTERPRETATION OR PERFORMANCE HEREOF, SHOULD THE PARTIES BE UNABLE TO REACH AN AMICABLE AGREEMENT WITHIN A PERIOD OF 30 DAYS UNLESS THIS PERIOD IS EXPRESSLY EXTENDED BY THE PARTIES, EXPRESS AND EXCLUSIVE COMPETENCE IS ASSIGNED TO THE COMMERCIAL COURT OF PARIS, WHICH SHALL HAVE SOLE COMPETENCE TO PRESIDE, NOTWITHSTANDING MULTIPLE DEFENDANTS OR THE INTRODUCTION OF THIRD PARTIES, EVEN IN THE CASE OF URGENT PROCEEDINGS OR CONSERVATORY PROCEDURES BY WAY OF INTERLOCUTORY PROCEDURE OR PETITION OR OPPOSITIONS ON INJUNCTION TO PAY.

