SPECIAL TERMS AND CONDITIONS OF SALE
SSL/TLS CERTIFICATES

CONTENTS

1. PURPOSE 2
2. DEFINITIONS 2
3. TERMS FOR PROVISION OF THE SERVICE 2
4. MANAGEMENT INTERFACE 3
5. CUSTOMER'S OBLIGATIONS AND RESPONSIBILITIES 3
5.1. Mandate Granted to Ikoula 3
5.2. Validation Process 3
5.3. Accuracy of Information Provided 3
5.4. Hosting, Authorizations and Private Key 4
5.5. Use of the SSL/TLS Certificate 4
6. IKOULA'S OBLIGATIONS AND RESPONSIBILITIES 4
6.1. Obligation of Means and Role as Intermediary 4
6.2. Liability 4
7. SERVICE TERM 4
7.1. Contractual Term 4
7.2. SSL/TLS Certificate Validity and Reissuance 5
7.3. Reissuance Procedure and the Customer's Role 5
7.4. Renewal of the Service 6
7.5. Termination and End of the Service 6
7.6. Revocation of the SSL/TLS Certificate 6

© 1998 - 2026 **IKOULA**, all rights reserved.

1. Purpose

These special terms and conditions (hereinafter the "**Special Terms**") define the terms under which Ikoula provides the Customer with the SSL/TLS Certificate Service where the Customer has a Domain Name (hereinafter the "**Service**").

2. Definitions

- **Certification Authority:** trusted entity responsible for issuing SSL/TLS Certificates.
- **SSL/TLS Certificate (also referred to as a "Certificate" or "Electronic Certificate"):** SSL is the acronym for "Secure Socket Layer". TLS is the acronym for "Transport Layer Security". These acronyms refer to standard protocols for securing the transmission of data over the Internet. TLS is the modern and secure successor to SSL. In these Special Terms, the terms "SSL/TLS Certificate", "Certificate" and "Electronic Certificate" are used interchangeably to refer to an SSL/TLS certificate, regardless of the Certification Authority that issued it. An SSL/TLS Certificate is a digital certificate consisting of a set of data cryptographically linking a holder identified by its Private Key to a Public Key. An SSL/TLS Certificate may be assigned to an individual, a private or governmental organization, an educational institution, or to a computer network component such as a firewall, router, or any other security hardware device.
- **Digital Signature:** encrypted electronic data file attached or logically linked to other electronic data, which identifies and is uniquely linked to the signature of the electronic data, which is created using the signer's Private Key and is linked in such a way that any subsequent changes to the electronic data can be detected.
- **Private Key:** encrypted and confidential electronic data file designed to be associated with a Public Key using the same encryption algorithm and which may be used to create digital signatures, to decrypt files or messages that have been encrypted with a Public Key. The Private Key belongs to the Customer and Ikoula does not provide Private Keys unless Ikoula has generated the CSR (Certificate Signing Request) at the same time as the Private Key.
- **Public Key:** means an encrypted and freely available electronic data file designed to be associated with a Private Key using the same encryption algorithm and which may be used to verify Digital Signatures and to encrypt files or messages.
- **DNS (Domain Name System):** a distributed computer service that associates Domain Names with their IP addresses or other types of records. For the purposes of the Service, "DNS" validation requires the Customer to add a record provided by the Certification Authority to the DNS zone of its Domain Name in order to demonstrate control over that Domain Name.
- **Domain Name(s):** the literal address of a website. A second-level Domain Name consists of a stem (for example: "ikoula") and an extension or TLD (for example ".com"), this extension being considered a top-level domain name. It should be noted that a domain name may include one or more prefixes (for example: "www").
- **Server:** means the Customer's server operating with the IP address identified by a Domain Name by the Customer to Ikoula and which is encryptedly linked to the Public Key presented in the SSL/TLS Certificate.

3. Terms for Provision of the Service

The Customer acknowledges that the SSL/TLS Certificate is linked to the Domain Name chosen by the Customer. Accordingly, it may not be transferred from one Domain Name to another, whether subscribed through Ikoula or through a third-party registrar, during or at the end of the Customer's contractual commitment.

IKOULA Net - SASU, capital of 181 260 euros - SIREN 417 680 618
2 Cité Paradis, 75010 Paris- France
Fax : +33 (0)1 78 76 35 46
www.ikoula.com

Regarding the provision of the Domain Name, where the latter is provided by Ikoula, the Customer undertakes to read the applicable special terms and conditions.

4. Management Interface

Ikoula provides the Customer with a management interface (hereinafter the "**Interface**") allowing the Customer to manage the actions to be performed in relation to its SSL/TLS Certificate.

The Customer is assigned a confidential Access Code to access the Interface. The Customer undertakes to maintain the confidentiality of this Access Code and not to disclose it to unauthorized third parties. The Customer is solely responsible for its Access Code and for any activity carried out with it on the Interface, including any consequences arising therefrom. Accordingly, any action performed using the Customer's identifiers shall be deemed to have been performed by the Customer.

The Customer shall immediately notify Ikoula in the event of loss, theft or unauthorized use of its Access Code. In such case, Ikoula reserves the right to block access and provide new identifiers.

The Customer is responsible for securing access to its account on the Interface and undertakes to take all reasonable measures to prevent any unauthorized access to its Access Code or account.

The Customer's use of any other identifier and password that may be provided by Ikoula shall be subject to the same rules, terms and obligations as those set out for the Access Code.

5. Customer's Obligations and Responsibilities

5.1. Mandate Granted to Ikoula

The Customer appoints Ikoula to act as intermediary with the Certification Authority, in particular to accept, in the name and on behalf of the Customer, subscription agreements with the Certification Authority and to confirm its order with the Certification Authority. The Customer expressly authorizes Ikoula to transmit to the Certification Authority any information requested from it strictly for the provision of the Service.

5.2. Validation Process

The Certification Authority shall carry out the validation process for the SSL/TLS Certificate requested by the Customer. The Customer shall be contacted directly by the Certification Authority.

If the Customer chooses DNS validation and the DNS is not managed by Ikoula, the Customer must contact Ikoula technical support in order to enter the fields required for validation.

5.3. Accuracy of Information Provided

The Customer undertakes to provide Ikoula with, and enter on the Interface, accurate, complete and regularly updated contact details and contact information.

In the event of incorrect, incomplete or outdated contact details or information, Ikoula cannot guarantee that the Customer will be able to carry out operations relating to the SSL/TLS Certificate, and issuance of the SSL/TLS Certificate may be refused or the SSL/TLS Certificate may be revoked by Ikoula or the Certification Authority. The Customer releases Ikoula from any liability in this respect.

IKOULA Net - SASU, capital of 181 260 euros - SIREN 417 680 618
2 Cité Paradis, 75010 Paris- France
Fax : +33 (0)1 78 76 35 46
www.ikoula.com

5.4. Hosting, Authorizations and Private Key

The Customer undertakes to be solely responsible for the hosting space of the website on which the Electronic Certificate is installed and to have the access rights required to manage it.

The Customer undertakes to obtain any authorization, permission or license that may be required to use the SSL/TLS Certificate and keep it in force.

The Customer shall take all appropriate precautions to prevent any breach, loss of control or unauthorized disclosure of confidential information from the time its Private Key is delivered.

5.5. Use of the SSL/TLS Certificate

The Customer shall not use the subscribed SSL/TLS Certificate to transmit (whether by sending emails or by downloading using any form of communication protocol), receive (whether by requesting an email or by downloading using any form of communication protocol), disclose, display or otherwise use information that is illegal, offensive, abusive, contrary to public morality, indecent, defamatory, obscene or threatening, or that would breach any confidence, copyright or other intellectual property right of a third party, or that would cause distress, embarrassment, denial of service, disruption or nuisance. The Customer shall not send or offer advertising or promotional materials or any other form of unsolicited correspondence.

The Customer undertakes to use the SSL/TLS Certificate reasonably, within the meaning of the provisions of the Civil Code and current case law.

6. Ikoula's Obligations and Responsibilities

6.1. Obligation of Means and Role as Intermediary

Ikoula undertakes to apply all necessary care and diligence to provide a quality service in accordance with industry practice and the state of the art, under an obligation of means.

Ikoula's obligations under these Special Terms are limited to acting as intermediary between the Customer and the provider supplying the SSL/TLS Certificate, namely the Certification Authority.

6.2. Liability

THE CUSTOMER ALSO ACCEPTS THAT UNDER NO CIRCUMSTANCES SHALL IKOULA BE LIABLE TO THE CUSTOMER FOR ANY LOSS INCURRED BY THE CUSTOMER AS A RESULT OF THE USE OF THE SSL/TLS CERTIFICATE OUTSIDE THE SCOPE OF USE AS SPECIFIED IN THESE SPECIAL TERMS.

THE CUSTOMER ALSO ACKNOWLEDGES THAT IKOULA SHALL NOT BE LIABLE TO THE CUSTOMER FOR ANY LOSS, INCLUDING ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, INCURRED BY EITHER PARTY AS A RESULT OF ANY LOSS, THEFT, UNAUTHORISED DISCLOSURE, UNAUTHORISED HANDLING, ALTERATION, DEPRIVATION OF USE OR ANY OTHER COMPROMISE OF ANY PRIVATE KEY USED BY THE CUSTOMER.

7. Service Term

7.1. Contractual Term

The Service is subscribed to by the Customer for a period of one (1) to five (5) years from the date of issue of the SSL/TLS Certificate (hereinafter the "Contractual Term").

IKOULA Net - SASU, capital of 181 260 euros - SIREN 417 680 618
2 Cité Paradis, 75010 Paris- France
Fax : +33 (0)1 78 76 35 46
www.ikoula.com

The Contractual Term is independent of the technical validity period of the SSL/TLS Certificate actually issued (hereinafter the "SSL/TLS Certificate Validity Period").

7.2. SSL/TLS Certificate Validity and Reissuance

Under the rules established by the CA/Browser Forum and the Certification Authorities, the SSL/TLS Certificate Validity Period may be shorter than the Contractual Term and may be progressively reduced. Several successive SSL/TLS Certificates may therefore be issued during the Contractual Term, without entitling the Customer to any refund or compensation.

During the Contractual Term, Ikoula may carry out, or require the Customer to carry out, any new issuance, reissuance or validation operation required by the rules applicable to SSL/TLS Certificates or by the Certification Authority. These operations do not extend the Contractual Term and, like the successive reissuances of the SSL/TLS Certificate required to cover the Contractual Term, are included in the subscription price and do not give rise to any additional charges, unless the Customer has expressly ordered a separate service.

Reissuance of an SSL/TLS Certificate during the Contractual Term does not extend that term, as reissuance of the SSL/TLS Certificate and contractual renewal of the Service are two separate operations.

Each SSL/TLS Certificate issued or reissued has an SSL/TLS Certificate Validity Period determined by the Certification Authority. This period may not exceed the maximum validity period permitted by the rules applicable to SSL/TLS Certificates, even where the remaining Contractual Term is longer. Several reissuances are therefore necessary to cover the entire Contractual Term. The SSL/TLS Certificate Validity Period has no effect on the end date of the Contractual Term.

Where reissuance takes place towards the end of the Contractual Term, the SSL/TLS Certificate Validity Period of the reissued certificate is limited to the time remaining until the end of that term.

7.3. Reissuance Procedure and the Customer's Role

Reissuance of an SSL/TLS Certificate during the Contractual Term is separate from renewal of the Service and does not require a new order. Ikoula informs the Customer, by emails sent sixty (60) days, thirty (30) days and fifteen (15) days before the expiry of the current SSL/TLS Certificate Validity Period, that the reissuance procedure is due to begin shortly. Service notifications are sent to the contact details entered by the Customer in its customer account on the Interface. The Customer is responsible for keeping these details up to date, in accordance with Article 5.3 of these Special Terms.

Reissuance of the Certificate requires the Customer's active participation. The Customer undertakes to carry out, within the deadlines indicated to it, the operations necessary for issuance or reissuance of its SSL/TLS Certificate, including domain or organization validation and, where required, provision of the necessary information or technical elements. The Customer is also responsible for retrieving the reissued SSL/TLS Certificate and installing or reinstalling it on its Server before the current SSL/TLS Certificate expires. Unless the Customer has subscribed to a specific managed services offering, Ikoula does not provide assistance in this respect.

If the Customer fails to respond or to carry out the operations for which it is responsible within the required deadlines, the SSL/TLS Certificate may expire or may be unable to be issued or reissued, resulting in an interruption of HTTPS protection. The absence of a valid SSL/TLS Certificate resulting from this failure does not constitute unavailability attributable to Ikoula, the Contractual Term continues to run, and the Customer is not entitled to any refund or compensation.

IKOULA Net - SASU, capital of 181 260 euros - SIREN 417 680 618
2 Cité Paradis, 75010 Paris- France
Fax : +33 (0)1 78 76 35 46
www.ikoula.com

7.4. Renewal of the Service

Renewal of the Service at the end of the Contractual Term requires a new order, which gives rise to new billing and a new validation process. A new Contractual Term begins on the date of issue of the first SSL/TLS Certificate under that new order.

Advance payment for renewal of the Service, where applicable, does not in itself affect the current SSL/TLS Certificate Validity Period. The new validity period of the SSL/TLS Certificate begins when the Certificate reissuance procedure is actually initiated. Accordingly, where the Customer initiates this procedure before the expiry of the current SSL/TLS Certificate Validity Period, any remaining days of validity are neither carried over nor added to the SSL/TLS Certificate Validity Period of the renewed certificate.

7.5. Termination and End of the Service

The Service may be terminated immediately or on the date specified in the notice:

- by either party if the other party commits a material breach of any provision of these Special Terms and such breach (where capable of remedy) is not remedied within fifteen (15) days following a written request from the other party requesting resolution of the dispute,
- or by either party if the other party becomes insolvent or ceases to carry on business.

In addition to the provisions of the General Terms and Conditions of Sale or the Framework Agreement, the Customer acknowledges and accepts that, if the Certification Authority or any other third-party supplier terminates the agreements authorizing Ikoula to market or resell SSL/TLS Certificates, or if the Certification Authority ceases operations or no longer has the right to issue SSL/TLS Certificates, Ikoula undertakes to inform the Customer as soon as possible and to implement, within thirty (30) days of that notification, any alternative solution ensuring continuity of the Service under equivalent conditions.

If no alternative solution is available at the end of that period, Ikoula may terminate the Service by giving the Customer fifteen (15) days' written notice. In such case, no compensation shall be payable to the Customer in respect of that termination.

Likewise, if the proposed alternative solution is not satisfactory to the Customer, the Customer may terminate the Service by giving thirty (30) days' notice.

Ikoula may also terminate the Service with immediate effect on legitimate grounds, including in the event of a serious breach by the Customer or a violation by the Customer of applicable regulations or ethical rules.

The end of the Service, for any reason, brings to an end all obligations of Ikoula under the Service, including any issuance, reissuance, validation, renewal, assistance or notification operation relating to the SSL/TLS Certificate.

7.6. Revocation of the SSL/TLS Certificate

Revocation of the Certificate is separate from termination of the Service: it is the permanent invalidation of an SSL/TLS Certificate before its expiry date, carried out by the Certification Authority.

The Customer may request revocation of its SSL/TLS Certificate at any time.

The Customer must request revocation without delay and, in any event, within twenty-four (24) hours of any compromise of its Private Key or of the information contained in the SSL/TLS Certificate becoming inaccurate.

IKOULA Net - SASU, capital of 181 260 euros - SIREN 417 680 618
2 Cité Paradis, 75010 Paris- France
Fax : +33 (0)1 78 76 35 46
www.ikoula.com

The Certification Authority may also revoke an SSL/TLS Certificate in the circumstances provided for in its rules, including compromise of the Private Key, inaccurate information, a breach by the Customer, unlawful use or loss of the right to use the Domain Name.

A revoked SSL/TLS Certificate cannot be reactivated. Its reissuance or replacement is at the sole discretion of the Certification Authority. Ikoula does not guarantee the reissuance or replacement of a revoked SSL/TLS Certificate and shall not be held liable for any refusal by the Certification Authority.

Upon revocation, the Customer must immediately cease all use of the revoked SSL/TLS Certificate and the associated Private Key.

Revocation does not entitle the Customer to any refund, subject to applicable mandatory provisions.

As the Certification Authority may revoke an SSL/TLS Certificate under its own rules, including without cause, Ikoula shall not be held liable for revocation decided by the Certification Authority or for the time taken by the Certification Authority to process a revocation request.

IKOULA Net - SASU, capital of 181 260 euros - SIREN 417 680 618
2 Cité Paradis, 75010 Paris- France
Fax : +33 (0)1 78 76 35 46
www.ikoula.com