SSL SECURITY CERTIFICATE SERVICE POLICIES

Policies in force as of November 7th, 2020.

1. DEFINITIONS.

The terms defined in this section may be used in these policies both singular and plural.

The terms referred to in capital letters and without definition in these policies will have the definition and meaning that has been granted to them in the Akky Domain Name Policies, unless these are defined otherwise or said definition or sense is limited.

All the headings used in these policies are used exclusively to facilitate their reading, but will not be considered when interpreting them.

1.1. *Administrative Contact*.

This primary contact will be the official applicant for the certificate and must be a full-time employee who is available to answer any questions regarding the validation process.

1.2. *Applicant*.

The User who has contracted the Service through the System.

1.3. *Certifying Authority*.

Company in charge of validating and issuing SSL Certificates. The Certifying Authority varies depending on the brand of the purchased certificate, for Domain Validation and Extended Validation certificate types, it is Sectigo® (Formerly Comodo) who performs the corresponding verification using the documents that determines as valid. For Organization Validation, it is Digicert® who performs the Verification through the documents that it determines as valid for this purpose.

1.4. *Common name*.

In the SSL Certificates industry, the Domain Name included in CSR is called this way.

1.5. *CSR (Certificate Signing Request)*.

It is a file with encrypted text that contains the information of the SSL certificate request, including the domain name, name of the organization, etc.

1.6. *Dedicated or Static IP*.

Address permanently assigned by an Internet service provider to a device.

1.7. *SANS (Secure Alternate Name)*.

Additional Domain names that can be added to a multi-domain certificate.

1.8. *Signature Algorithm*

It is a method to encrypt information through mathematical functions, the 'hash' algorithms transform a set of data into a single fixed-length value that, when calculated, is used to verify the integrity of the stored information.

1.9. *SSL Certificate (Secure Sockets Layer)*.

It is a digital title that authenticates the identity of a website and encrypts the information sent to the server with SSL technology.

1.10. ***SSL Certificate Types***.
There are 3 types of SSL Certificates, which can be issued:

a) Domain Validation. The Certifying Authority validates the ownership of the related Domain Name.
b) Organization validation. The Certifying Authority, validates the ownership of the related Domain Name, also verifies the name of the organization and telephone number.
c) Extended Validation. The Certifying Authority validates the ownership of the related Domain Name, also verifies the name of the organization, telephone number, physical address and good legal terms.

1.11. ***SSL Certificates Modality***.
SSL Certificates can be issued for a Common Name, for the different subdomains derived from the Common Name or for multiple Domain Names independent of each other.

1.12. ***Service***.
Refers to SSL Security Certificates.

1.13. ***Technical Contact***.
This contact will receive the certificate and is generally the one who will install the certificate on the web server.

1.14. ***Verification Mechanisms***.
They are used by the Certification Authority (CA) to prove that the user is the owner of the domain or has rights over it. For example: Email, HTTP File, HTTPS File, CNAME Record.

1.15. ***Website Trust indicator***.
It is an element that is used in the SSL Certificates to accompany the Website and the way it is presented may vary depending on the browser used. Examples: https, the padlock icon in the browser bar, a certification authority site seal, a green bar that wraps the URL in Extended Validation certificates.

2. GENERAL PROVISIONS.

The Registrant and Users of a Domain Name in Akky declare that they know and accept these policies, in relation to this Service, the Domain Name Service and the Certification Authority (Sectigo® and Digicert®) for the issuance, revocation and administration of an SSL Certificate; as well as Akky's attributions to eliminate and/or modify them at any time.

Any modification or update to the Policies published on the Akky Website will be made known through a notice of at least five (05) days immediately prior to the date of their entry into force, on the Akky Website, in order to That the Registrant and the Users express what is in their interests. Once the previous term has elapsed, the Registrant and the Users of the Domain Name will be bound by these new Policies, without it being necessary for Akky to make any other type of publication or notice.

Akky may assign, transfer, compromise, give over or dispose, in whole or in part, the rights and obligations derived from the provision of the Service contained in the terms and conditions of these Policies, without prior authorization. In case of carrying out any of the above assumptions, Akky will communicate the new person in charge of the adequate and timely execution of the activities related to the provision of the present Service, for which the Applicant, the Users and/or, where appropriate, the Registrant, will be subject to the terms and conditions established in the Policies of the new provider.

Akky simply manages the Domain Name space, and therefore, any consequence derived from the registration and/or use of the Service and/or the Domain Names that constitutes or could constitute violations of the applicable legislation, is the sole responsibility of the Registrant, even when the Domain Name with which this Service is configured is administrated with another Registrar.

Akky reserves the right to review, remove, edit or block any material or information that Users have published, received or sent in contravention of any law, at the express request of an Authority or in the event of abuse of the Service. Akky, at any time, may suspend, temporarily or permanently, and/or cancel access and/or use of the Service.

3. ABOUT THE SERVICE

3.1. *General Aspects*.

3.1.1. *Contracting*.

The Service can be contracted by Users through the System by selecting a Type of SSL Certificate and adding it to the shopping cart, the Applicant is responsible for obtaining authorization from the Registrant to relate this Service to a Domain Name, the which can be administered even with another Registrar.

3.1.2. *Coverage Period*.

The Applicant will choose the coverage period of the Service in accordance with the options determined by the System. The validity of the Service will begin on the date the SSL Certificate has been issued by the Certification Authority. It is necessary to process the configuration and validation so that the Certifying Authority issues the certificate, otherwise, it will expire without having been issued when the selected term ends.

3.1.3. *Renewal*.

For the SSL Certificate renewal, Akky may notify the Applicant 30 days before the certificate’s expiration. The sending of this notification is done to support the Applicant for the reissue of the certificate, for which is its responsibility to know the expiration date and carry out the reissue in a timely manner. Once the notice of next expiration is received and before the end of the validity period selected by the Applicant at the time of contracting the Service, it may be renewed for periods determined by the System. It is the user’s responsibility to renew the SSL Certificate before its expiration, since once the validity period concludes, the Service is considered as expired, so it is necessary that the Certification Authority validates and issues the SSL Certificate again as in hiring.

3.1.3.1. In the SSL Certificates industry, it is necessary to perform a reissue of an SSL Certificate in which coverage period is greater than one (1) year, considering the following:

3.1.3.1.1. The reissue must be made by the user from 30 days prior to the certificate’s expiration date

3.1.3.1.2. When a certificate is reissued, the Certifying Authority reserves the right to carry out the documentation verification again, in cases where the information contained in the CSR is updated.

3.1.3.1.3. When reissuing, the Common Name, contained in the CSR, must be kept.

3.1.3.1.4. The corresponding notice will be sent 30 days before the end of the effective period.

3.1.4. ***Assignment*.**

The Service will be assigned to the Domain Name indicated by the User, when configuring it through the System, therefore, in order to assign this service and its correct operation, the Applicant assumes the following responsibilities:

3.1.4.1. The selection of the certificate type and the validation method selected and its configuration.

3.1.4.2. Ensure that has the documentation and requirements established for the Certifying Authority to validate and issue the selected SSL Certificate, for the Organization Validation and Extended Validation types the applicant must ensure that the Administrative Contact provides the required documents and registers in the Information Directories specified by the Certifying Authority. Therefore, it exempts Akky from any type of responsibility in the event that this authority determines the impossibility of issuing the SSL Certificate due to non-compliance of these requirements.

3.1.4.3. Must ensure that the Domain Name related to this Service exists and has paid coverage with the corresponding Registrar.

3.1.4.4. Perform the configuration requested by the Certifying Authority depending on the verification mechanism selected.

3.1.4.5. Notify the contacts established in the certificate data as Administrative Contact and/or Technical Contact.

3.1.4.6. Ensure that the Certificate's Administrative Contact performs the validation of the Domain Name property for all types of SSL Certificates.

3.1.4.7. Akky reserves the right to modify or eliminate the Service assignment at request of the Domain Name's Registrant after carrying out the Ownership validation and the Registrant's authentication, by presenting the required or enough documentation for this purpose.

3.1.5. ***Cancellation*.**

3.1.5.1. The Applicant can carry out the Service cancellation, which can be done at any time through the System.

3.1.5.2. Akky reserves the right to delete the Service in accordance with point 3.1.4.6. of these policies.

3.1.5.3. The Certifying Authority could notify the user of some security inconsistency found on the Website related to a SSL Certificate, which must be resolved to continue the certificate's validity. If this communication is not attended, the Certification Authority may revoke the SSL Certificate. It is the Applicant and User's responsibility to attend the communication of the Certification Authority, in order to keep their SSL Certificate in force, thus exempting Akky from correcting its revocation.

3.1.5.4. In case of Service cancellation, the corresponding payment will be non-refundable or transferable.

3.1.6. ***Elimination*.**

The Service will be eliminated if payment is not received within the periods established by Akky, at the time of contracting the Service or on the date of its renewal.

3.1.7. ***Access*.**

To Access and configure the Service, the Applicant must use its User Account in Akky's System.

3.1.8. ***Fees, terms and forms of payment*.**

3.1.8.1. The fees and forms of payment will be shown before completing the payment for their purchase or renewal, in the cart summary.

3.1.8.2. The Applicant and Users must cover the fee corresponding to the Service indicated according to the coverage period.

3.1.8.3. The Applicant and Users acknowledge and accept that the payments made are not refundable or transferable to another Service. Additionally, if the Service cancellation is requested or the Certifying Authority determines the impossibility of issuing the SSL certificate in accordance to point 3.1.4.2., service payment will not be refundable or transferable.

3.1.8.4. Akky may send various notices regarding the Service collection before its expiration date, via email to the Applicant. The sending of these messages is carried out as a support to the Users for the Services payment, for which is their responsibility to know the Service's renewal date and process the corresponding payment on time.

3.1.8.5. As the date of contracting the Service, the User has the period of validity indicated in the Service Order to make the corresponding payment.

3.1.8.6. When generating a Service Order using a credit card or debit card, Akky will enable automatic renewal for the services included in that Service Order. If the user keeps the automatic renewal, a temporary charge will be generated to confirm that the card is valid, which will be returned once that validation is concluded. It is responsibility of the Main User and/or Users with Payment permissions as appropriate, to place correct information and ensure that through this payment method the renewal of those services can be completed. If necessary, Akky will notify the users that it was not possible to process the automatic renewal in order for the registered information is verified. If this modification is not made, the services will be placed in the corresponding status because it has not been possible to process their renewal.

3.1.8.7. Automatic renewal may be disabled at the time of the Service Order generation or through the Control Panel, by the Main User and/or the Users with payment permissions, however, it will be necessary to generate the corresponding Service Order for its renewal. In case of modifying the credit or debit card, a transitory charge will be generated to confirm that the card is valid, which will be returned once this validation is concluded.

3.1.8.8. In order to process the automatic renewal, Akky Will use the Openpay® services as the operator of these credit and debit card payments.

3.1.8.9. There is a period of up to 30 (thirty) calendar days after the Service Renewal date to make the corresponding payment.

3.1.8.10. The consideration for the Service will be proportional to the contracting validity.

3.2. ***Specifications***.

3.2.1. The Service consists of establishing a secure connection through the transfer of encrypted data between a browser and a web server. There are different Types and Modalities of SSL Certificates, each one with specific characteristics that are published through Akky's Website.

3.2.2. The information's validation necessary for the SSL Certificate issuance depending on its Type, is carried out by a Certifying Authority determined by the brand that issues the certificate, which will establish communication with the Administrative Contact via email and/or telephone. The Certifying Authority reserves the right to use the language of origin with which it will establish communication. Akky could support the Administrative Contact in understanding the validation by the Certifying Authority, in case it uses a language other than Spanish.

3.2.3. Akky reserves the right to provide the Service with its own resources or with support of suppliers.

3.2.4. Users accept that they are of legal age and are in full use and enjoy their ability to pursue, otherwise they must refrain from using and/or requesting the Service.

3.2.5. The Service is associated with one or more Domain Names depending on the Certificate Modality and that said Service will not be transferable to any other Domain Name.

3.2.6. The Service configuration is carried out as follows:

3.2.6.1. Entry and verification of the CSR. It is necessary that after logging into the Control Panel, the user places the corresponding CSR file in the Generate certificate section. Once you have validated the CRS, it is necessary for the information contained in it to be verified.

3.2.6.2. Configuration. In the event that the SSL Certificate is multidomain, it is necessary to list the Domain Names that will be covered by this certificate. It is the responsibility of the person who performs this configuration to place the Domain Names in this step, since, if not, SAN compatibility will be disabled and it would not be feasible to use this mode.

3.2.6.3. Server Type Selection. It is necessary to select the type of server platform configured for the SSL Certificate, in case whoever performs the configuration does not know this information and continues in the configuration process, the Certificate will be issued considering the standard format X 509 (PEM or Privacy Enhanced Mail) is an ITU-T (International Telecommunication Union) standard for public key infrastructures.

3.2.6.4. Verification Mechanism Selection. Depending on the Certificate's type and brand, the Verification Mechanism may vary. The Verification Mechanisms types are: E-mail, HTTP File, HTTPS File, CNAME Record.

3.2.6.5. Signature Algorithm Selection. Depending on the Certificate's Type and brand, the Signature Algorithm may vary. The options are: SHA-256, SHA-384, SHA-512.

3.2.6.6. Administrative, Technical Contact Information. It is necessary to enter contact information for the Certifying Authority to communicate with the Administrative Contact if necessary to carry out the validation of the information, and in the case of the Technical Contact, to send the file that contains the issued Certificate via email.

3.2.6.7. Company Data. It is necessary to enter the requested information from the Company related to the SSL Certificate, the Applicant is responsible for ensuring that the information provided matches the legal details of the company registered in the documentation. In case of being incorrect, the delay or the impossibility of issuing the SSL Certificate could occur.

3.2.7. When completing the configuration, it will be necessary to carry out the instructions sent by email from the Certifying Authority depending on the Type of Verification Mechanism selected.

3.2.8. It is necessary that the Applicant considers a static IP for the SSL Certificate installation.

3.2.9. In the event that the warranty related to the SSL Certificate is required, it is necessary for the Applicant to refer to the process established by the Certification Authority (Sectigo® and Digicert®).

3.3. *Intellectual property*.

The Registrant and the Users must ensure that they are not infringing any intellectual or industrial property rights when using the Service (such as: registered trademarks, licenses, reservations of rights), and/or any other third-party right, according to the national and international legal system applicable in the matter.

3.4. *Personal Data*.

The Registrant and the Users are the only ones responsible for the treatment they carry out of the personal data to which they have access by virtue of the use of the Service, as well as their protection and that their treatment is carried out with the secrecy and security that they deserve, of In accordance with the provisions of the Federal Law on Protection of Data Held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de Particulares), as well as the current legislation that is applicable in the matter.

Update publication date:	February 26th, 2021.
Effective as from:	March 02, 2021.

RAR-0321

*** The English version of this document has no legal value, it is provided solely as a means to facilitate the reading and understanding of the Spanish version, it is not a substitute to the legal validity of the Spanish version. In case of any discrepancy between the Spanish version and the English version, the Spanish version shall prevail.**