

LAST REVISED 15 August 2026
VERSION 1.0

Avenida de Manolete 3a
29660 Marbella, Malaga (ES)
CIF: ESB72758436
legal@pladinum.com · +34 697 9898 40

Introduction

This SSL Subscriber Agreement governs the issuance, installation, management, renewal, and revocation of SSL/TLS certificates obtained through Pladinum Group SL ("Pladinum", "we", "us", "our") by the person or entity to whom the certificate is issued (the "Subscriber", "you", "your").

It supplements the General Terms and Conditions and prevails over them in respect of SSL/TLS certificates.

Acceptance of this Agreement is a condition of issuance. A certificate will not be issued until it has been accepted.

1. The Certificate Authority

1.1 Certificates are issued by a publicly trusted Certificate Authority. Pladinum acts as an intermediary between the Subscriber and the Certificate Authority and does not itself issue certificates.

1.2 The Certificate Authority operates under the CA/Browser Forum Baseline Requirements and its own Certification Practice Statement. Those documents govern issuance and revocation and prevail over this Agreement in respect of the matters they cover.

1.3 The Certificate Authority may impose additional terms, require the completion of an application form, or contact the Subscriber directly for verification. The Subscriber agrees to cooperate with such requests.

2. Types of Certificate

2.1 Domain Validated (DV). Confirms control of the domain name only. It does not authenticate the identity of the organisation behind it.

2.2 Organisation Validated (OV). Adds verification of the organisation's identity, including name, type, status, and registered address. The Subscriber must be a legal entity.

2.3 Extended Validation (EV). Adds further verification points, including registration number, incorporation date, telephone verification, and screening against sanction and fraud lists. The Subscriber must be a legal entity.

2.4 Warranty terms and limits, where any apply, are set by the Certificate Authority and are shown before purchase.

3. Validation

3.1 Issuance is subject to successful validation of control over the domain name, by DNS record, by email to an address at the domain, or by placing a file on the web server, depending on the certificate type and the method selected.

3.2 Wildcard certificates cannot be validated by file. Email or DNS validation must be used.

3.3 Multi-domain certificates require validation for each name individually. File validation fails where a redirect is in place on any of those names.

3.4 For OV and EV certificates, the Subscriber must supply supporting documentation within the period stated at the time of order. Failure to do so renders the order void.

3.5 Where the information associated with the domain name does not match the documentation supplied, the request will not be validated. A new request may be made once the discrepancy is resolved.

4. Subscriber Obligations

4.1 Accurate information. The Subscriber warrants that all information supplied in connection with a certificate request is accurate and complete, and undertakes to notify Pladinum of any change that affects the validity of an issued certificate.

4.2 Control of the domain name. The Subscriber warrants that it owns or controls the domain name or names to be covered by the certificate, and that the choice and use of those names does not infringe the rights of any third party.

4.3 Private key. The Subscriber is the sole holder of the private key corresponding to the certificate. The Subscriber must generate it securely, keep it confidential, and protect it from loss, theft, disclosure, and unauthorised use. Any use of the private key is deemed to have been made by the Subscriber or with the Subscriber's consent.

4.4 Installation. Installation of the certificate on the Subscriber's server is the Subscriber's responsibility, as is the physical and logical security of that server.

4.5 Verification of contents. The Subscriber must check the contents of the certificate, including the correspondence between the public and private keys, promptly after issuance, and must notify Pladinum of any inaccuracy or defect. This obligation continues throughout the life of the certificate.

4.6 Lawful use. Certificates may be used only for authentication and encryption, in accordance with applicable law. They must not be used in safety-critical or specially regulated environments, including aviation safety and nuclear industry applications.

4.7 Revocation requests. The Subscriber must request revocation without delay where the private key is lost, stolen, disclosed, or otherwise compromised, or where information contained in the certificate becomes false or outdated.

5. Issuance and Reissuance

5.1 Domain Validated certificates are normally issued within fifteen (15) minutes of successful validation.

5.2 Organisation Validated and Extended Validation certificates are issued by the Certificate Authority on its own timeline, following receipt of complete documentation.

5.3 Certificates are issued for a maximum period set by the CA/Browser Forum and are reissued for the remainder of the purchased term. Reissuance is initiated automatically before expiry.

5.4 Installation of a reissued certificate is not automatic. The Subscriber must install each reissued certificate on their server. Failure to do so will cause the certificate to expire and browsers to display security warnings.

6. Term, Renewal and Expiry

6.1 The term begins on the date the certificate is issued, whether or not it has been installed, and runs for the period purchased.

6.2 A reminder is sent by email before expiry to the address held on the account.

6.3 Renewal is subject to full payment and, where applicable, to supplying current supporting documentation. A revoked or expired certificate cannot be renewed; a new certificate must be requested.

6.4 Where the certificate is associated with a domain name registered through Pladinum, expiry or deletion of that domain name does not automatically revoke the certificate, but validation for renewal will not be possible.

7. Revocation

7.1 Pladinum or the Certificate Authority will revoke a certificate immediately and without prior notice where:

- (i) the private key is lost, stolen, modified, disclosed, or otherwise compromised;
- (ii) information contained in the certificate has changed, is false, or is outdated;
- (iii) the certificate is used in breach of this Agreement or of the Certificate Authority's requirements;
- (iv) continued trust in the certificate would be inappropriate; or
- (v) revocation is required by the CA/Browser Forum, by the Certificate Authority, or by applicable law.

7.2 Where the Subscriber breaches an obligation under this Agreement and does not remedy it within fifteen (15) calendar days of notice, the certificate may be revoked.

7.3 Revocation is final. A revoked certificate cannot be restored and no refund is due. Revoked certificates are published in a publicly accessible revocation list, and the Subscriber must cease all use of a revoked certificate immediately.

8. Refunds

8.1 A certificate may be refunded within thirty (30) days of issuance provided it has not been installed on a server, in accordance with the Refund Policy.

8.2 After that period, or where the certificate has been installed, no refund is due.

8.3 No refund is due on revocation.

9. Availability Constraints

9.1 Certificates cannot be issued for certain top-level domains where the Certificate Authority has suspended issuance. Current restrictions are stated on the relevant product page.

9.2 Extended Validation wildcard certificates do not exist and cannot be issued.

10. Liability

10.1 Pladinum is not liable for: negligence, theft, or disclosure of the private key; the consequences of using a revoked certificate; the Subscriber's activities conducted under a certificate; the expiry or non-renewal of a certificate; failure to install a reissued certificate; or refusal by the Certificate Authority to approve a request.

10.2 A certificate encrypts data in transit. It does not secure the Subscriber's website or server. Pladinum is not liable for intrusion into or compromise of the Subscriber's systems.

10.3 Aggregate liability in respect of a certificate shall not exceed the amount paid for that certificate.

10.4 Nothing in this Section excludes or limits liability that cannot lawfully be excluded or limited.

11. Contact

Pladinum Group SL
Avenida de Manolete 3a
29660 Marbella, Malaga (ES)
SSL: support@pladinum.com

Customer Portal: my.pladinum.com

Website: www.pladinum.com