SSL AGREEMENT

1. PURPOSE AND SCOPE

This Agreement covers the purchase, validation, installation, use, and revocation of all SSL/TLS certificates provided through Atak Domain, including:

- DV SSL Certificates (Domain Validation)
- OV SSL Certificates (Organization Validation)
- EV SSL Certificates (Extended Validation)
- Wildcard SSL Certificates
- Multi-Domain / SAN SSL Certificates
- Code Signing Certificates
- e-Mail (S/MIME) Certificates
- UCC / Multi-Domain EV/OV Certificates

Atak Domain provides all SSL certificates through authorized global Certificate Authorities (CAs) (e.g., Sectigo, DigiCert, GlobalSign, GeoTrust, RapidSSL, etc.). This agreement is applied together with the CA/Browser Forum Baseline Requirements, relevant CA Rules, and Atak Domain's general terms and conditions.

2. DEFINITIONS

Subscriber: The person/entity requesting and validating the SSL certificate.
Relying Party: End-users who rely on the certificate to perform transactions.
CA (Certificate Authority): The global certificate authority that issues the certificate.
CSR: Certificate Signing Request.
DCV: Domain Control Validation.
OV/EV Validation: Corporate validation, phone verification, and commercial document verification.
Revocation: Cancellation of the certificate by the Certificate Authority.

3. SCOPE OF SERVICE

Atak Domain provides the Customer with the following services:

- Certificate application (technical guidance to create CSR)
- Domain validation methods (Email DCV, HTTP/HTTPS File Upload, DNS CNAME)
- Document collection for OV/EV and submission to the CA
- Certificate issuance by the CA
- Support for installing certificates on cPanel, Plesk, Nginx, Apache, etc.
- Renewal reminders
- Processing revocation (cancellation) requests and forwarding them to the CA

Atak Domain can only provide the certificate as approved by the CA; the validation process is solely under CA authority.

4. CUSTOMER OBLIGATIONS

4.1. Obligation to Provide Accurate Information

The Customer declares and guarantees that during certificate application:

- They have the usage rights for the domain name,
- Commercial information provided for OV/EV certificates is accurate,
- Phone number, address, and company registration information match official records.

If incorrect information is provided, the CA may revoke the certificate.

4.2. Maintaining Domain Control

Email addresses, web root directories, or DNS records used in DV/OV/EV validations must be correctly prepared by the Customer.

4.3. Secure Use of the Certificate

The Customer must:

- Not share their private key with third parties,
- Keep their server secure,
- Track the certificate expiration date.

Loss of the private key constitutes a security breach and the certificate will be revoked by the CA.

5. SERVICE PROVIDER OBLIGATIONS

Atak Domain is responsible for:

- Accurately submitting the certificate request to the CA,
- Providing technical guidance to the Customer,
- Forwarding validation requests from the CA.

Atak Domain cannot perform validation; all validation is carried out exclusively by the CA.

6. VALIDATION PROCESSES (DV / OV / EV)

6.1. DV SSL – Domain Control Validation

Only domain control is verified via:

- Email validation
- DNS CNAME
- HTTP/HTTPS validation

The CA confirms that domain control is held by the customer.

6.2. OV SSL – Organization Validation

The CA may request the following documents:

- Trade registry record
- Tax number

- Phone verification
- Corporate address validation
- Company verification via public records

The CA confirms that the customer is a legitimate organization.

6.3. EV SSL – Extended Validation

In EV validation, the CA thoroughly examines:

- Legal existence of the organization
- Physical address
- Trade registry records
- Authorized person verification
- Phone verification
- Operational existence check

CA/B Forum EV guidelines are applied fully.

7. TERMS OF USE

The Customer may use the SSL certificate:

- Only for the validated domain(s),
- Only on permitted servers,
- For lawful purposes.

The certificate may be revoked by the CA in cases such as:

- Fraudulent or malicious websites
- Phishing, malware distribution
- Trademark infringement
- Forgery of official documents
- Unauthorized private key sharing
- Fraud, spam, or illegal activities

8. VALIDITY PERIOD AND RENEWAL

Certificate validity periods:

- DV / OV / EV: 1 year
- Code Signing: 1–3 years

Due to CA/Browser Forum rules, SSL certificates longer than 1 year require automatic renewal.
Atak Domain sends renewal reminders, but renewal responsibility belongs to the Customer.

9. REVOCATION POLICY

The CA must immediately revoke the certificate under the following conditions:

- Private key theft
- Incorrect/misleading information
- Illegal activity
- Invalidated CA-verified information
- Loss of domain control
- Government/court requests
- Detection of a security breach

No refunds are provided for revoked certificates (in accordance with global CA policies).

10. PRICING AND REFUNDS

10.1. Pricing

All prices are published on the Atak Domain website and may be updated based on CA costs.

10.2. Refund Policy

According to global CA rules:

- No refunds can be issued after the certificate is issued.
- If validation fails, a full refund is provided.
- For OV/EV document rejection, the CA's refund policies apply.

11. LIMITATION OF LIABILITY

Atak Domain cannot be held liable for:

- Use of the SSL certificate,
- Loss of the private key,
- Website hacking,
- Server configuration errors,
- Damages caused by third parties,
- Losses suffered by Relying Parties.

Atak Domain's total liability is limited to the amount paid by the customer for the certificate.

12. WARRANTY (PROVIDED BY THE CA)

Some CAs (e.g., Sectigo, DigiCert) provide "Warranty" coverage for SSL certificates.

This warranty:

- Covers damages incurred by third parties due to incorrect identity validation,
- Is provided only by the CA,
- Atak Domain is not a party to this warranty.

Atak Domain only acts as an intermediary in the warranty process.

13. CONFIDENTIALITY AND DATA PROTECTION

Atak Domain ensures the protection of customer information under:

- GDPR,
- KVKK,
- CA privacy policies.

14. DISPUTE RESOLUTION

In case of dispute:

- Turkish law shall apply,
- Kocaeli Courts and Enforcement Offices have jurisdiction.

15. ENFORCEMENT OF THE AGREEMENT

When the customer purchases an SSL certificate, they are deemed to have:

- Read,
- Understood,
- Accepted

this agreement.

This agreement becomes effective upon publication on the Atak Domain website.