TERMS AND CONDITIONS

for Disig, a.s., ACME TLS Certificate Issuance Services

Effective day from: May 18, 2026

PROVIDER IDENTIFICATION

This agreement is concluded by and between Disig, a.s., a corporate entity established and existing under the legal regulations of the Slovak Republic (Slovenská republika), having its registered seat at Galvaniho 17/C, 821 04 Bratislava - mestská časť Ružinov, Business Identification Number (IČO): 35975946, registered in the Commercial Register maintained by the Business Register of the City Court Bratislava III, Insert No.: 3794/B (hereinafter referred to as the "Provider"), and the Client definition specified herein.

1. INTRODUCTORY PROVISIONS AND DEFINITIONS

For the purposes of these Terms and Conditions (hereinafter referred to as the "T&C" or "Všeobecné obchodné podmienky"), the following capitalized terms shall have the meanings specified below:

ACME Protocol

The Automated Certificate Management Environment is a communication protocol for automatic interaction between a certification authority and their users' servers, enabling automated deployment of public key infrastructure..

Client

Any legal entity or natural person entrepreneur that undergoes successful Pre-registration and utilizes the Provider’s ACME infrastructure to obtain Organization Validated (OV) TLS certificates.

Certificate

A digital Organization Validated (OV) Transport Layer Security (TLS) certificate issued by the Provider through automated execution via the ACME protocol API.

Contract

The corporate service agreement established between the Provider and the Client, governed explicitly by these T&C, regulating the automated issuance of Certificates.

Organization Validation (OV)

The strict vetting framework whereby the Provider verifies the full legal existence, corporate identity, operational address, and valid statutory representation of the Client before allowing automated issuance.

Pre-registration

The mandatory initial administrative vetting procedure during which the Client submits verified organizational credentials and documentation to secure permission for ACME API access.

External Account Binding (EAB)

The cryptographic authentication mechanism within the ACME protocol explicitly utilized to securely bind a designated local ACME client cryptographic key pair to the pre-vetted Client profile inside the Provider's authenticated database.

2. SUBJECT OF THE CONTRACT

2.1 The Provider agrees to grant the Client access to its dedicated ACME server infrastructure for the sole purpose of automated identity challenge verification, issuance, renewal, and management of Organization Validated (OV) Certificates.

2.2 The Client explicitly agrees to access and use the automated infrastructure strictly within the constraints defined under these T&C and to fulfill any associated financial or administrative obligations as separately agreed.

3. PRE-REGISTRATION, VETTING, AND ORGANIZATION VALIDATION (OV)

3.1 **Mandatory Prior Vetting**: The Client explicitly acknowledges and accepts that the ACME service is strictly limited to Organization Validated (OV) Certificates. No automated issuance can occur until the Client has fully satisfied and completed the Provider's manual or administrative Pre-registration identity vetting pipeline.

3.2 **Documentation Requirements**: To complete Pre-registration, the Client must present authentic, legally binding corporate identification records, including but not limited to an official excerpt from the Commercial Register, trade license certificate, or an equivalent primary governmental registration document, alongside verification of the signing authority of the statutory body or authorized representative.

3.3 **Credential Activation via EAB**: Upon satisfactory validation of the Client's corporate identity, the Provider will distribute unique External Account Binding (EAB) credentials, consisting of a custom Key Identifier (KID) and a Hash-based Message Authentication Code (HMAC). The Client must embed these precise EAB configurations within its local ACME client software execution string to bind its automated requests to the verified profile.

3.4 **Validation Validity Limit**: In strict compliance with industry rules and CA/Browser Forum Baseline Requirements, the verified status of Organization Validation (OV) data remains valid for a maximum duration of up 398 days. Upon expiration of this temporal window, the Client must repeat the validation procedure. The Provider retains the absolute operational right to suspend automated issuance instantly if the OV vetting data lapses.

3.5 **Strict Duty to Notify Changes**: The Client is legally bound to immediately notify the Provider of any material adjustments to its corporate layout, including company dissolution, name amendments, restructuring, change of registered office, or alterations regarding its statutory body, which could render the validated information in the issued Certificates inaccurate or misleading.

4. CERTIFICATE ISSUANCE, RENEWAL, AND REVOCATION

4.1 **Two-Tier Validation Framework**: Automated certificate generation via the ACME endpoint is strictly conditional upon the concurrent success of two separate layers of cryptographic and administrative validation:

1. **Organizational Control**: An active, unexpired, and fully verified corporate Pre-registration profile linked via External Account Binding (EAB).
2. **Domain Control Verification**: Real-time automated verification verifying the Client's active administrative command over requested domain identifiers via approved ACME protocol mechanisms (e.g., HTTP-01, DNS-01).

Failure to satisfy both conditions simultaneously results in an immediate, automated refusal of the Certificate Signing Request (CSR) by the ACME API backend.

4.2 **Private Key Security**: The Client assumes full and exclusive technical and legal liability for key generation, storage, and confidentiality preservation concerning its private cryptographic keys. The Provider under no circumstances obtains or has access to the Client's private keys.

4.3 Revocation Enforcement: The Provider maintains the right to immediately execute a Certificate revocation without prior notification or delay under the following conditions:

- An authorized revocation request is processed directly via the ACME protocol layer using a valid account key or private key.

- The Provider receives notice or detects an explicit threat indicating compromise of the Client's private cryptographic key.
- The Client loses legitimate legal or technical domain control over the domain namespaces authorized within the Certificate.
- The Client violates its corporate obligations as set forth under these T&C, or ceases its corporate activities.

5. CERTIFICATE TRANSPARENCY (CT) LOGGING

5.1 **Mandatory Ledger Inclusion**: The Client explicitly understands, acknowledges, and gives unconditional consent for the Provider to transmit all issued OV TLS Certificates to independent, publicly verifiable Certificate Transparency (CT) log systems, in compliance with Internet Engineering Task Force (IETF) regulations and root browser requirements.

5.2 **Public Disclosure**: Information embedded within the Certificate, including the Fully Qualified Domain Name (FQDN), corporate name, public key parameters, issuing authority, and timestamp validity parameters will reside inside an immutable public ledger database.

5.3 **Irrevocability of Publication**: The Client recognizes that due to the immutable, secure structural design of CT cryptosystems, log records cannot be deleted, modified, or redacted. This cryptographic requirement represents a legally accepted exception to the general right to erasure or the right to be forgotten governed by data protection frameworks.

6. SERVICE LEVEL AGREEMENT (SLA) FOR ACME API

6.1 **Target Infrastructure Availability**: The Provider shall leverage professional industry standards to guarantee a target monthly availability rate of 99.9% for the automated ACME API issuance endpoints. Availability calculations are executed across each billing calendar month, excluding intervals reserved for Scheduled Maintenance.

6.2 **System Maintenance Classifications**:

- **Scheduled Maintenance**: Routine platform optimizations, software updates, and infrastructural checks. The Provider will deliver a minimum of forty-eight (48) hours advance administrative notice to the Client via its status page or electronic mail.
- **Emergency Maintenance**: Urgent service interruptions executed to patch immediate critical security vulnerabilities, severe data center errors, or hardware failures. Emergency interventions may be initiated immediately without prior announcement.

6.3 **Explicit SLA Exclusions**: System unavailability or challenge failures shall not constitute a breach of this SLA if driven by:

3. Force Majeure circumstances.
4. Network failures originating from the Client's localized routing environment, misconfigured third-party ACME client clients, or domain registrar errors.
5. Upstream dependency latency, distributed ledger delays, or global DNS propagation lags.
6. Automated rate-limiting restrictions triggered intentionally by the ACME backend due to excessive client failure loops or request volume exceeding standard provisioning profiles.

6.4 **Legal and Financial Remedies**: The Client agrees that the single, exclusive remedy available for a breach of this SLA is limited to the right to terminate the active Contract. No direct financial indemnification, price reductions, or contractual penalties shall be asserted against the Provider, except where explicit financial penalties are formally negotiated in a standalone written agreement signed by the statutory bodies of both parties.

7. LIABILITY AND DISCLAIMER OF WARRANTIES

7.1 Limitation of Damages: In strict compliance with the relevant provisions of the Slovak Commercial Code, the total cumulative liability of the Provider for any actual damages or proven financial loss arising under or in relation to the deployment, operation, or automated issuance of Certificates under this Contract shall be strictly capped at the aggregate financial sum paid by the Client to the Provider for these services over the immediate twelve (12) months prior to the date on which the claim arose.

7.2 Exclusion of Consequential Loss: The Provider shall under no circumstances be held liable to the Client or any third party for lost business profits (ušlý zisk), commercial disruption, depletion of corporate goodwill, data corruption, or any indirect, incidental, or consequential damages whatsoever.

7.3 As-Is Service Execution: Save for the commitments explicitly guaranteed under Section 6 (SLA), the automated ACME environment is deployed on an "as-is" and "as-available" architecture, devoid of any express, statutory, or implied warranties of merchantability or fitness for specific operations.

8. DATA PROTECTION

8.1 The Provider collects and processes necessary personal contact details provided by the Client for Contract execution, administrative Pre-registration vetting, and compliance enforcement, strictly adhering to the General Data Protection Regulation (GDPR) and Act No. 18/2018 Coll. on Personal Data Protection.

8.2 Public dissemination of data inside public Certificate Transparency ledgers is explicitly executed as a fundamental security necessity and legal prerequisite under public key infrastructure security frameworks, establishing a legitimate processing grounds profile.

9. GOVERNING LAW AND DISPUTE JURISDICTION

9.1 This Contract, these T&C, and all surrounding legal relations, interactions, or non-contractual claims arising between the Provider and the Client shall be exclusively governed by, interpreted, and enforced in accordance with the substantive laws of the Slovak Republic, strictly excluding its conflict of law regulations.

9.2 Any legal relationships, liabilities, or business interactions not explicitly detailed within the present document shall be directly governed by the primary provisions of Act No. 513/1991 Coll., the Slovak Commercial Code, as amended.

9.3 Both parties agree that any disputes, legal actions, or litigations emerging out of or connected with the execution, interpretation, or breach of these T&C shall be submitted to the exclusive jurisdiction of the competent courts of the Slovak Republic holding geographical and subject-matter jurisdiction over the registered office of the Provider.

10. FINAL PROVISIONS

10.1 Unilateral Amendments: The Provider maintains the right to introduce updates or amend these T&C unilaterally. The Provider will notify the Client of prospective material alterations via corporate electronic mail or through specific directory announcements inside the ACME API endpoint at least thirty (30) calendar days prior to the enforcement date of the amended version.

10.2 Severability: If any distinct clause or provision of these T&C is declared invalid, void, or legally unenforceable by a court of competent jurisdiction, such invalidity shall not prejudice or impair the legal standing, validity, and enforceability of any remaining provisions outlined in this agreement.