



# VŠEOBECNÉ OBCHODNÉ PODMIENKY PRE POSKYTOVANIE SLUŽIEB AUTOMATIZOVANÉHO VYDÁVANIA TLS CERTIFIKÁTOV (ACME)

Dátum účinnosti: 18. máj 2026

## POSKYTOVATEĽ

Túto zmluvu sa uzatvára medzi spoločnosťou Disig, a.s., právnickou osobou založenou a existujúcou podľa právnych predpisov Slovenskej republiky, so sídlom na adrese Galvaniho 17/C, 821 04 Bratislava - mestská časť Ružinov, IČO: 35975946, zapísaná v obchodnom registri vedenom Obchodným registrom Mestského súdu Bratislava III, vložka č.: 3794/B (ďalej len „Poskytovateľ“), a medzi Klientom ako je definovaný v časti 1 tejto zmluvy.

## 1. ÚVODNÉ USTANOVENIA A DEFINÍCIE POJMOV

Pre účely týchto Všeobecných obchodných podmienok (ďalej len „VOP“) majú nasledovné pojmy s veľkým začiatočným písmenom tento význam:

### ACME Protocol

(Automated Certificate Management Environment) je komunikačný protokol na automatickú interakciu medzi certifikačnou autoritou a servermi ich používateľov, ktorý umožňuje automatizované nasadenie infraštruktúry verejných kľúčov.

### Klient

Právnická osoba alebo fyzická osoba - podnikateľ, ktorá úspešne absolvovala Predregistráciu a využíva infraštruktúru ACME Poskytovateľa s cieľom získania TLS certifikátov s overením organizácie (OV).

### TLS Certifikát

TLS certifikát (Transport Layer Security Certificate) s overením organizácie (Organization Validated - OV), vydaný Poskytovateľom prostredníctvom automatizovaného spracovania cez API rozhranie ACME protokolu.

### Zmluva

Zmluva o poskytovaní služieb uzatvorená medzi Poskytovateľom a Klientom, ktorá sa riadi týmito VOP a ktorá upravuje podmienky automatizovaného vydávania Certifikátov.

### Overenie Organizácie (OV):

Proces overovania (vetting), pri ktorom Poskytovateľ preveruje právnu existenciu, firemnú identitu, faktickú adresu a oprávnenie štatutárneho orgánu Klienta pred tým, než umožní automatizované vydávanie Certifikátov.

### Predregistrácia

Povinný úvodný administratívny proces overenia totožnosti, počas ktorého Klient predkladá overiteľné firemné dokumenty, aby získal oprávnenie na prístup k ACME API..

### External Account Binding (EAB)

Kryptografický mechanizmus v rámci protokolu ACME, ktorý slúži na bezpečné prepojenie konkrétneho kľúča ACME klienta s vopred overeným profilom Klienta v databáze Poskytovateľa.

## 2. PREDMET ZMLUVY

2.1 Poskytovateľ sa zaväzuje umožniť Klientovi prístup k svojej vyhradenej infraštruktúre ACME servera za účelom automatizovaného overovania výziev, vydávania, obnovovania a správy TLS Certifikátov s overením organizácie (OV)

- 2.2 Klient sa zaväzuje prístupovať k tejto automatizovanej infraštruktúre a využívať ju výhradne v súlade s podmienkami definovanými v týchto VOP a plniť prípadné súvisiace finančné alebo administratívne záväzky, ak boli samostatne dohodnuté.

### 3. PREDREGISTRÁCIA, PREVEROVANIE A OVERENIE ORGANIZÁCIE (OV)

- 3.1 **Povinné predbežné overenie:** Klient výslovne berie na vedomie a súhlasí s tým, že služba ACME je striktné obmedzená na Certifikáty s overením organizácie (OV). K žiadnemu automatizovanému vydaniu Certifikátu nemôže dôjsť, kým Klient úspešne neabsolvuje a nedokončí proces manuálneho a administratívneho overenia identity v rámci Predregistrácie.
- 3.2 **Požadovaná dokumentácia:** Na účely úspešnej Predregistrácie je Klient povinný predložiť autentické a právne záväzné dokumenty preukazujúce jeho právny status, najmä aktuálny výpis z Obchodného registra, živnostenské oprávnenie alebo ekvivalentný úradný register, spolu s overením podpisového oprávnenia štatutárneho orgánu alebo splnomocneného zástupcu.
- 3.3 **Aktivácia prístupu pomocou EAB:** Po úspešnom overení firemnej identity Klienta vygeneruje Poskytovateľ unikátne prístupové údaje pre External Account Binding (EAB), ktoré pozostávajú z identifikátora kľúča (KID) a overovacieho kódu (HMAC kľúč). Klient je povinný tieto údaje presne nakonfigurovať vo svojom lokálnom ACME softvéri (klientovi), aby prepojil svoje automatizované požiadavky s overeným firemným profilom.
- 3.4 **Doba platnosti overenia:** V prísnom súlade s priemyselnými štandardmi a pravidlami CA/Browser Forum (Baseline Requirements) zostáva overený stav údajov organizácie (OV) platný po dobu 398 dní. Po uplynutí tejto lehoty musí Klient proces overenia organizácie absolvovať znova. Poskytovateľ si vyhradzuje absolútne právo okamžite pozastaviť automatizované vydávanie certifikátov, ak platnosť OV overenia expiruje.
- 3.5 **Oznamovacia povinnosť Klienta:** Klient je právne povinný bezodkladne informovať Poskytovateľa o akýchkoľvek podstatných zmenách vo svojej korporátnej štruktúre, vrátane zrušenia spoločnosti, zmeny obchodného mena, reštrukturalizácie, zmeny sídla alebo zmien v štatutárnom orgáne, ktoré by mohli spôsobiť, že overené informácie v Certifikátoch sa stanú nepresnými alebo nepravdivými.

### 4. VYDÁVANIE, OBNOVA A REVOKÁCIA CERTIFIKÁTOV

- 4.1 **Dvojúrovňový proces overovania:** Automatizované vygenerovanie certifikátu cez ACME endpoint je prísne podmienené súčasným splnením dvoch nezávislých úrovní kryptografického a administratívneho overenia:
1. **Kontrola organizácie:** Aktívny, neexpirovaný a plne overený firemný profil prepojený cez External Account Binding (EAB).
  2. **Overenie kontroly domény:** V reálnom čase vykonané automatizované overenie, že Klient má pod technickou kontrolou požadované doménové adresy, a to prostredníctvom schválených výziev ACME protokolu (napr. HTTP-01, DNS-01).  
Ak nie sú obe podmienky splnené súčasne, backend ACME API požiadavku na podpísanie certifikátu (CSR) automaticky a okamžite zamietne.
- 4.2 **Bezpečnosť privátnych kľúčov:** Klient nesie plnú a výhradnú technickú a právnu zodpovednosť za generovanie, bezpečné úložisko a zachovanie dôvernosti svojich privátnych kryptografických kľúčov. Poskytovateľ za žiadnych okolností nedisponuje s privátnymi kľúčmi Klienta a nemá k nim prístup.
- 4.3 **Dôvody na zneplatnenie (revokáciu):** Poskytovateľ si vyhradzuje právo okamžite a bez predchádzajúceho upozornenia zneplatniť (revokovať) Certifikát, ak:
- Klient o zneplatnenie požiada priamo prostredníctvom protokolu ACME s využitím príslušného účtového alebo privátneho kľúča.

- Poskytovateľ zistí alebo získa dôvodné podozrenie, že privátny kryptografický kľúč Klienta bol kompromitovaný (unikol).
- Klient stratí legitímnu právnu alebo technickú kontrolu nad doménami uvedenými v Certifikáte.
- Klient poruší svoje povinnosti vyplývajúce z týchto VOP alebo ukončí svoju podnikateľskú činnosť.

## 5. TRANSPARENTNOSTI CERTIFIKÁTOV (CERTIFICATE TRANSPARENCY LOGS)

- 5.1 **Povinné zaznamenávanie:** Klient výslovne berie na vedomie, súhlasí a udeľuje bezpodmienečný súhlas s tým, že Poskytovateľ odošle každý vydaný OV TLS Certifikát do nezávislých, verejne overiteľných logov Certificate Transparency (CT) v súlade s nariadeniami IETF a požiadavkami popredných webových prehliadačov.
- 5.2 **Verejne dostupné údaje:** Informácie obsiahnuté v Certifikáte, najmä plne kvalifikovaný doménový názov (FQDN), obchodné meno Klienta, verejný kľúč, údaje o vydavateľovi a časová platnosť, sa stanú súčasťou nemennej a verejne prístupnej databázy (záznamu).
- 5.3 **Nezvratnosť zápisu:** Klient berie na vedomie, že vzhľadom na kryptografickú a nemennú povahu CT systémov nie je možné tieto záznamy dodatočne zmazať, upraviť ani anonymizovať. Toto zverejnenie predstavuje právne uznanú výnimku z práva na výmaz alebo práva na zabudnutie v rámci predpisov o ochrane osobných údajov.

## 6. DOHODA O ÚROVNI POSKYTOVANÝCH SLUŽIEB (SLA) PRE ACME API

- 6.1 **Cielová dostupnosť infraštruktúry:** Poskytovateľ vynaloží primerané úsilie zodpovedajúce profesionálnym štandardom, aby zabezpečil cieľovú mesačnú dostupnosť automatizovaných ACME API endpointov na úrovni 99,9% (dostupnosť služby). Dostupnosť sa kalkuluje za každý kalendárny mesiac, s výnimkou plánovanej údržby.
- 6.2 **Klasifikácia údržby systému:**
- **Plánovaná údržba:** Rutinné optimalizácie platformy, aktualizácie softvéru a infraštruktúrne kontroly. Poskytovateľ doručí Klientovi oznámenie o plánovanej odstavke minimálne 48 hodín vopred prostredníctvom status stránky alebo elektronickej pošty.
  - **Núdzová údržba:** Urgentné zásahy vykonané s cieľom okamžite odstrániť kritické bezpečnostné zraniteľnosti, závažné chyby dátového centra alebo zlyhania hardvéru. Tieto zásahy môžu byť spustené okamžite bez predchádzajúceho oznámenia.
- 6.3 **Výluky zo SLA:** Nedostupnosť systému alebo zlyhanie overenia výziev sa nepovažuje za porušenie tejto dohody SLA, ak bolo spôsobené:
1. Okolnosťami vyššej moci (vis maior).
  2. Zlyhaním siete na strane Klienta, nesprávne nakonfigurovaným ACME softvérom Klienta alebo chybami registrátora domény.
  3. Globálnym oneskorením propagácie DNS.
  4. Automatickým uplatnením obmedzení (rate-limiting) zo strany ACME backendu kvôli nadmernému počtu chybových požiadaviek generovaných softvérom Klienta.
- 6.4 **Nápravné prostriedky:** Klient súhlasí s tým, že jediným a výhradným nápravným prostriedkom pri porušení tejto SLA je jeho právo okamžite odstúpiť od Zmluvy. Klientovi nevzniká nárok na priame finančné odškodnenie, zľavu z ceny ani na zmluvnú pokutu, pokiaľ takéto sankcie neboli formálne dohodnuté v samostatnej písomnej dohode podpísanej štatutárnymi orgánmi oboch zmluvných strán.

## 7. ZODPOVEDNOSŤ ZA ŠKODU A VYLÚČENIE ZÁRUK

- 7.1 **Obmedzenie náhrady škody:** V prísnom súlade s príslušnými ustanoveniami Obchodného zákonníka Slovenskej republiky je celková kumulatívna zodpovednosť Poskytovateľa za akúkoľvek skutočnú škodu alebo preukázanú finančnú stratu vzniknutú v súvislosti s prevádzkou, nasadením alebo automatizovaným vydávaním Certifikátov podľa tejto Zmluvy obmedzená (stropovaná) do výšky celkovej sumy, ktorú Klient reálne zaplatil Poskytovateľovi za tieto služby za obdobie dvanástich (12) mesiacov bezprostredne predchádzajúcich mesiacu, v ktorom nárok na náhradu škody vznikol.
- 7.2 **Vylúčenie ušlého zisku:** Poskytovateľ v žiadnom prípade nezodpovedá Klientovi ani žiadnej tretej strane za ušlý zisk, narušenie obchodnej činnosti, stratu dobrého mena spoločnosti, poškodenie dát alebo za akékoľvek nepriame, náhodné či následné škody.
- 7.3 **Poskytovanie služby „tak ako stojí a leží“:** S výnimkou záväzkov výslovne garantovaných v Článku 6 (SLA) je automatizované ACME prostredie prevádzkované na báze „tak ako stojí a leží“ (as-is) a „ako je dostupné“, bez akýchkoľvek výslovných, zákonných alebo predpokladaných záruk za obchodovateľnosť alebo vhodnosť na konkrétny účel.

## 8. OCHRANA OSOBNÝCH ÚDAJOV

- 8.1 Poskytovateľ zhromažďuje a spracúva osobné údaje kontaktných osôb poskytnuté Klientom za účelom plnenia Zmluvy, administratívneho overovania v rámci Predregistrácie a presadzovania súladu s predpismi, pričom prísne postupuje podľa Všeobecného nariadenia o ochrane údajov (GDPR) a zákona č. 18/2018 Z. z. o ochrane osobných údajov.
- 8.2 Zverejnenie údajov vo verejných CT registroch sa uskutočňuje na základe oprávneného záujmu a plnenia zmluvných povinností, nakoľko predstavuje základnú bezpečnostnú nevyhnutnosť a technický predpoklad fungovania moderných PKI systémov.

## 9. ROZHODNÉ PRÁVO A SÚDNA PRÍSLUŠNOSŤ

- 9.1 Táto Zmluva, VOP, ako aj všetky mimozmluvné záväzky a právne vzťahy vznikajúce medzi Poskytovateľom a Klientom sa riadia, budú vykladané a vymáhané výhradne podľa hmotného práva Slovenskej republiky, s vylúčením jeho kolíznych noriem.
- 9.2 Právne vzťahy, zodpovednosť alebo obchodné interakcie výslovne neupravené týmito VOP sa priamo riadia príslušnými ustanoveniami zákona č. 513/1991 Zb. Obchodný zákonník v platnom znení.
- 9.3 Zmluvné strany sa dohodli, že akékoľvek spory, právne kroky alebo súdne konania vzniknuté z týchto VOP alebo v súvislosti s nimi budú predložené na riešenie výhradne vecne a miestne príslušnému súdu v Slovenskej republike, podľa sídla Poskytovateľa.

## 10. ZÁVEREČNÉ USTANOVENIA

- 10.1 **Jednostranné zmeny a doplnenia:** Poskytovateľ si vyhradzuje právo jednostranne aktualizovať alebo meniť tieto VOP. Poskytovateľ o plánovaných podstatných zmenách upovedomí Klienta prostredníctvom firemnej elektronickej pošty alebo prostredníctvom oznámenia priamo v adresári ACME API endpointu, a to najmenej tridsať (30) kalendárnych dní pred dňom účinnosti novej verzie.
- 10.2 **Oddeliteľnosť ustanovení:** Ak súd príslušnej jurisdikcie vyhlási akékoľvek samostatné ustanovenie alebo klauzulu týchto zmluvných podmienok za neplatné, neúčinné alebo právne nevymáhateľné, takáto neplatnosť nebude mať vplyv ani nenaruší právne postavenie, platnosť a vymáhateľnosť akýchkoľvek zostávajúcich ustanovení uvedených v tejto zmluve.