

Acme Pay API Reference v2.1

Acme Pay Inc.

12 марта 2026

Contents

Acme Pay API Reference v2.1	1
1. Введение	1
2. Authentication	1
3. Создание платежа	2
4. Получение статуса платежа	3
5. Webhooks	3
6. Rate limits	4
7. Chargebacks	4
8. PCI compliance	4
9. Migration v1 → v2	4
10. Errors	5

Acme Pay API Reference v2.1

Document version: 2.1.0 **Published:** 12 марта 2026 **Status:** PRODUCTION

1. Введение

Acme Pay — платёжный провайдер с поддержкой card payments (Visa, Mastercard, Mir), alternative payment methods (SBP, Apple Pay, Google Pay) и subscription billing. API соответствует REST best practices, поддерживает webhooks для асинх-нотификаций.

Поддерживаемые валюты: RUB, USD, EUR, KZT, AED, GBP.

Base URL (production): <https://api.acmepay.com/v2/> **Base URL (sandbox):** <https://sandbox.acmepay.com/v2/>

[!] **Important:** v1 API deprecated с 01.06.2026, sunset 01.09.2026. Все production-интеграции должны мигрировать на v2.

2. Authentication

Acme Pay использует OAuth 2.0 Client Credentials Grant.

2.1 Получение access_token

```
POST /v2/oauth/token
Content-Type: application/x-www-form-urlencoded
Authorization: Basic {base64(client_id:client_secret)}
```

grant_type=client_credentials&scope=payments.write payments.read webhooks.manage

Response:

```
{
  "access_token": "eyJhbGc...",
  "token_type": "Bearer",
  "expires_in": 86400,
  "scope": "payments.write payments.read webhooks.manage"
}
```

Token lifetime: 24 часа (86400 секунд). После expiry — повторный запрос access_token.

2.2 Использование токена

Все API-запросы должны содержать header:

Authorization: Bearer {access_token}

2.3 Безопасность ключей

client_secret не должен храниться в коде клиента. Рекомендуем secret manager (HashiCorp Vault, AWS Secrets Manager). Ротация ключей — раз в 90 дней.

3. Создание платежа

3.1 POST /v2/payments

Создаёт новый платёжный запрос. Возвращает payment_id и URL для редиректа клиента на checkout.

Required headers: - Authorization: Bearer {token} - Idempotency-Key: {unique_uuid_v4} — **обязательно**. Гарантирует safe retry. Один Idempotency-Key даёт один платёж — повторные запросы с тем же ключом возвращают исходный результат без создания дубля. - Content-Type: application/json

Request body:

```
{
  "amount": 150000,
  "currency": "RUB",
  "customer_id": "cust_abc123",
  "description": "Order #45678",
  "return_url": "https://merchant.example.com/payment/return",
  "webhook_url": "https://merchant.example.com/webhooks/асмепай",
  "metadata": {
    "order_id": "45678",
    "purpose": "subscription_renewal",
    "campaign_id": "summer2026"
  }
}
```

Required fields: - amount (integer, minor units — копейки/центы) - currency (ISO 4217) - customer_id (string, ваш внутренний ID клиента — обязателен начиная с v2.0) - return_url (HTTPS) - webhook_url (HTTPS, TLS 1.2+, см. §5)

Optional fields: - description (string, max 256 chars) - metadata (object, до 20 полей) - metadata.purpose (string, новое поле в v2.1, для категоризации в reporting: one_time, subscription_renewal, subscription_initial, top_up, refund_proxy)

Response (201 Created):

```
{
  "payment_id": "pay_xyz789",
  "status": "pending",
  "checkout_url": "https://checkout.асмепай.com/pay_xyz789",
  "expires_at": "2026-03-12T15:30:00Z",
}
```

```
"amount": 150000,  
"currency": "RUB"  
}
```

Checkout session lifetime: 30 минут с момента создания. После expiry — статус переходит в expired, оплата невозможна.

4. Получение статуса платежа

4.1 GET /v2/payments/{payment_id}

Возвращает текущий статус платежа.

Возможные статусы: - pending — ожидает действий клиента - processing — обработка началась (синхронная обработка, см. §4.2) - succeeded — успешно завершён - failed — отклонён (см. failure_reason) - expired — истёк срок checkout - refunded — возврат произведён

4.2 Синхронная обработка платежа

Асме Pay обеспечивает синхронную обработку платежа: с момента нажатия клиентом «Pay» до получения статуса succeeded/failed проходит до 5 секунд. По истечении 5 секунд статус остаётся processing — клиент уже может покинуть страницу, финальный статус придёт через webhook.

5. Webhooks

5.1 Регистрация webhook URL

Webhook URL передаётся в каждом запросе POST /v2/payments через поле webhook_url.

Требования к webhook URL: - Только HTTPS. - TLS 1.2 или выше. - Сертификат должен быть валидным (не self-signed). - Endpoint должен отвечать 200 OK в течение 10 секунд.

5.2 Webhook signature

Асме Pay подписывает каждый webhook payload через HMAC-SHA256 с использованием webhook_secret (выдаётся при создании merchant account в личном кабинете Асме).

Signature header:

X-Asme-Signature: sha256={hex_digest}

Расчёт:

signature = HMAC-SHA256(webhook_secret, raw_request_body)

Validation на стороне merchant: обязательна. Асме не несёт ответственности за обработку поддельных webhooks, если merchant не валидирует signature.

5.3 Webhook payload

```
{  
  "event_id": "evt_aaa111",  
  "event_type": "payment.succeeded",  
  "created_at": "2026-03-12T15:25:43Z",  
  "payment": {  
    "payment_id": "pay_xyz789",  
    "status": "succeeded",  
    "amount": 150000,  
  }  
}
```

```

    "currency": "RUB",
    "customer_id": "cust_abc123",
    "metadata": {
      "order_id": "45678",
      "purpose": "subscription_renewal"
    }
  }
}

```

5.4 Event types

- payment.succeeded
- payment.failed
- payment.refunded
- payment.expired
- chargeback.created (см. §7)
- chargeback.resolved

5.5 Retry policy

Если merchant вернул не-2xx статус или не ответил в течение 10 секунд — Асме повторяет webhook с **exponential backoff**. Количество retries и точные интервалы не специфицированы в этой версии документа.

6. Rate limits

Информация о rate limits размещена в Developer Portal личного кабинета. Для активации Production-доступа уточняйте у вашего account manager.

7. Chargebacks

При оспаривании платежа клиентом — Асме направляет webhook chargeback.created. Merchant обязан в течение 7 рабочих дней предоставить evidence через POST /v2/chargebacks/{chargeback_id}. Процедура подробно описана в Operations Manual, который отдельный документ.

8. PCI compliance

Асме Pay сертифицирована по PCI DSS Level 1. Через checkout flow Асме — merchant **не получает** доступ к raw card data (PAN, CVV) и поэтому подпадает под SAQ A (минимальная форма compliance).

Если merchant интегрирует Асме через server-to-server API с прямой передачей card data (legacy v1, deprecated) — merchant подпадает под SAQ D (полная форма) и обязан проходить ASV scan ежеквартально.

9. Migration v1 → v2

Основные изменения:

Что	v1	v2
Base URL	/v1/	/v2/
Auth	API Key in header	OAuth 2.0 access token
customer_id	optional	required

Что	v1	v2
Idempotency-Key	optional	required
Webhook signature	optional (SHA-1)	required (HMAC-SHA256)
Currencies	RUB only	6 валют
metadata.purpose	—	новое поле

Sunset v1: 01.09.2026. После этой даты v1 endpoints возвращают 410 Gone.

10. Errors

Стандартные HTTP коды + поле `error.code` в теле:

```
{
  "error": {
    "code": "invalid_currency",
    "message": "Currency XYZ is not supported",
    "details": {"supported": ["RUB", "USD", "EUR", "KZT", "AED", "GBP"]}
  }
}
```

Основные коды: - `invalid_currency`, `invalid_amount`, `invalid_customer_id` - `idempotency_key_required`, `idempotency_key_conflict` - `webhook_url_invalid`, `webhook_url_not_https` - `auth_token_expired`, `auth_token_invalid`, `auth_insufficient_scope` - `rate_limit_exceeded`

End of document.

© 2026 Acme Pay Inc. All rights reserved.