API Endpoints > Cryptography > Sign Testing JWT

Sign Testing JWT

Endpoint

URL: `/:projectId/crypto/sign-testing-jwt`

Method: `POST`

Authentication Required: No

Description

Generate a signed JWT for testing purposes using a provided private key, project ID, and payload.

Request

Headers

None

Body Parameters

Parameter	Type	Required	Description
`projectId`	`string`	Yes	Project ID to use as the token issuer.
`privateKey`	`string` (base64)	Yes	Private key in base64-encoded PEM format.
`payload`	`object`	Yes	Payload to embed in the token. Must include an `id`.

Example Request

```
{
  "projectId": "proj_123",
  "privateKey": "LS0tLS1CRUdJTiBSU0EgUFJ...",
  "payload": {
    "id": "user_abc",
    "name": "Jane Doe",
    "role": "editor"
  }
}
```

Response

Success Response (200 OK)

Returns a signed JWT string:

```
<JWT_STRING>
```

Error Responses

Missing Params (400 Bad Request)

```
{
  "error": "Missing user id in payload.",
  "code": "crypto/missing-params"
}
```

Server Error (500 Internal Server Error)

```
{
  "error": "Internal server error",
  "code": "crypto/server-error",
  "details": "<Error message>"
}
```

Notes

- This endpoint is intended for testing and should not be exposed in production environments.
- The `payload` must contain an `id` field which will be used as the `sub` in the JWT.
- The signed token uses the RS256 algorithm and is valid for 5 minutes.
- The audience (`aud`) is set to `replyke.com`.

Last updated on May 11, 2025