

Technische Documentatie: Axepta BNP Paribas Online API

De Axepta BNP Paribas Online API is een veilige oplossing ontworpen om de integratie van betalingen in uw e-commerceplatform te vereenvoudigen. Deze documentatie biedt alle technische informatie die nodig is om de API effectief te begrijpen, te configureren en te gebruiken.



Volledige API-documentatie: <https://axeptabnpparibas-docs.redocly.app/>

Presentatie van de API

Belangrijkste kenmerken

Functie	Beschrijving
RESTful-architectuur	Gebaseerd op REST-principes voor een voorspelbare en gebruiksvriendelijke interface.
Verhoogde beveiliging	PCI-DSS-compliant met HTTPS (TLS 1.2 of hoger) voor veilige communicatie.
Uitgebreide documentatie	Gedetailleerde technische handleidingen voor eenvoudige integratie.

Gebruiksscenario's

- **Online betalingen** – Verwerk betalingen in real-time.
- **Transactiebeheer** – Raadpleeg en beheer eerdere transacties (bv. terugbetalingen, annuleringen).

Authenticatie

Ondersteunde authenticatiemethoden



Authenticatie verloopt via de productie-API: <https://paymentpage.axepta.bnpparibas/>

De API ondersteunt twee authenticatiemethoden:

- BasicAuth (eenvoudig, maar minder veilig)
- OAuth 2.0 (aanbevolen)

OAuth 2.0 :

Authenticatie moet plaatsvinden via het **OAuth-V2-protocol**.

Stappen:

1. Genereer een **JSON Web Token (JWT)** door te authenticeren met uw **API-sleutel** via het endpoint: **authorization/oauth/token**
2. Het **access_token** en **token_type** moeten worden meegestuurd in **elke serveraanvraag**, in de **HTTP-header Authorization**.

Voorbeeld van een JWT-response:

```
{
  "access_token":
    "eyJhbGciOiJSUzI1NiIsImtpZCI6IkpzZWZlZW0JEQzY2Mjc3MUYwNzYxRUJDRTkwOTMyMDMyQjdGOTQ1NTQ1LCJ4NXQiOiJfOG5UdmNaawR4
    0EHZZXZPa0pNZ01yZjVSVLEiLCJ0eXAiOiJhdCtqd3QifQ.
    eyJpc3MiOiJodHRwciovL2xvY2FsaG9zdDo3MTIxLyIsImV4cCI6MTc0MDQ3NTUwNCwiaWF0IjoxNzQwNDcxOTA0LCJqdGkiOiJiZjU3YmUwM
    i05YThiLTQxYjctYjNjNi02NzlmMTcxNDU2ZjAiLCJzdWIiOiJkVjF9MjB2dLZWV9bV90ZXN0IiwibmFtZSI6IkdX0xvZ2VlY29tX3Rlc3Q1LC
    JtYXJrZXRwbGFjZUlkIjo1Q1RfTG9nZWVjb21fdGVzdF9NYXJrZXRwbGFjZSI6Im1hcmtldHBsYWw0aXZlIjpmYWxzZSwib2lfcHJzdCI6
    IkdX0xvZ2VlY29tX3Rlc3Q1LCJjbGllbnRfawQiOiJkVjF9MjB2dLZWV9bV90ZXN0Iiwib2lfdGtuX2lkIjo1MjEwMjEwMjEwMjEwMjEwMjEw
    ICocWYD4_35bTAiPFU2A4HwWQpg1PZTrdf4riSoA_v_5bwSM-rdHAb-
    Y7fNwQTYAUyDxkcrw9qc5JcjbWBG10gXGTzJR2xyPDTq2s04qAxo00lhCVjhEQR47yq0Fta9rkCcmg1i6T6BxF7Z06tBECfo7NSJ0wgn7G5_Un
    md5MgWuG8V5VdvDxhXa1p_sBQdmy6nBCRi2d2bh1B0rz_uT5U2zngVBPzZBXv046j7971JXZbR20JFpkqwrULCGR6fy78NvkrHNC4U8ZDHmbe
    jBb0bMGcb_8pWMnaLhIg0A1k2x0Q",
  "token_type": "Bearer",
  "expires_in": 3600
}
```

Belangrijk:

- Het toegangstoken is 1 uur geldig.
- Na verloop van tijd moet u opnieuw authenticeren om een nieuw token te verkrijgen.

Idempotentie voor POST en PATCH-verzoeken

Idempotentie voor POST en PATCH-verzoeken

Voor POST en PATCH-verzoeken wordt idempotentie gegarandeerd door de HTTP-header Idempotency-Key.

Vereisten:

- De waarde moet uniek zijn voor elk HTTP-verzoek.
- De client is verantwoordelijk voor het genereren van deze sleutel.
- Aanbevolen formaat: UUID v4 (bv. 123e4567-e89b-12d3-a456-426614174000).