



**Rabobank**

# Rabo OmniKassa 2.0 API

*Handleiding developers versie 1.7*

Version: 1.7 NL Februari 2019

Contact e-mail address: [contact@omnikassa.rabobank.nl](mailto:contact@omnikassa.rabobank.nl)

© Rabobank, 2019 *Klik hier als u tekst wilt invoeren..*

*No part of this publication may be reproduced in any form by print, photo print, microfilm or any other means without written permission by Rabobank.*

*Disclaimer: Deze Handleiding is uitsluitend bedoeld voor derden die voor en in opdracht van klanten zorgdragen voor de technische koppeling van Rabo OmniKassa met de webwinkel van de klant. Rabobank is niet aansprakelijk voor mogelijke schade die voortvloeit uit fouten in of verkeerd gebruik van de Handleiding. Bijvoorbeeld maar niet beperkt tot schade die ontstaat doordat de technische koppeling van Rabo OmniKassa met de webwinkel van de klant niet (geheel) correct werkt. Rabobank heeft het recht deze Handleiding te wijzigen.*

## Inhoudsopgave

|             |  |                  |
|-------------|--|------------------|
| <b>1.</b>   | <b><i>Introductie</i></b>  | <b><i>1</i></b>  |
| <b>1.1.</b> | <b><i>Overzicht</i></b>  | <b><i>1</i></b>  |
| <b>1.2.</b> | <b><i>Opmerking over 'Expect: 100-Continue' header</i></b>                       | <b><i>1</i></b>  |
| <b>2.</b>   | <b><i>Call: Refresh</i></b>  | <b><i>2</i></b>  |
| <b>3.</b>   | <b><i>Call: Order Announce</i></b>   | <b><i>4</i></b>  |
| <b>4.</b>   | <b><i>Call: Notification</i></b>   | <b><i>19</i></b> |
| <b>5.</b>   | <b><i>Call: Status pull</i></b>  | <b><i>21</i></b> |
|             | <b><i>BIJLAGE A: Berekenen signature voor verouderde aanroep punt order.</i></b> | <b><i>25</i></b> |

## 1. Introductie

Dit document beschrijft de API van Rabo Omnikassa. Deze API kan worden gebruikt om een webwinkel aan te sluiten op Rabo OmniKassa. In dit document zal Rabo OmniKassa verder afgekort worden als ROK, maar deze afkorting mag niet zonder meer gebruikt worden in communicatie of documentatie van de plugin naar webwinkels.

De voorbeelden bevatten veel lange teksten, zoals tokens, signatures en URLs. Om de tekst leesbaar te houden, worden deze voorzien van (extra) end-of-lines. Extra end-of-lines moeten niet zelf in de berichten worden gestopt en zullen ook niet in de echte berichten zitten.

### 1.1. Overzicht

De interface voor betalen bestaat uit 3 calls van de webwinkel naar Rabo OmniKassa (ROK) en 1 call van ROK naar de webwinkel.

De betaling van een order bij ROK bestaat uit de volgende stappen.

1. De webwinkel vraagt een Access Token op aan ROK (Refresh call)
2. De webwinkel gebruikt het Access Token om een order aan te kondigen (Order announce call)
3. De webwinkel leidt de consument naar ROK
4. De consument voert de betaling uit met behulp van ROK
5. De consument wordt terug geleid naar de webwinkel
6. ROK stuurt de webwinkel een bericht om aan te geven dat er een order status update beschikbaar is (Notification call)
7. De webwinkel vraagt aan ROK de laatste orderstatussen (Status pull call)

De calls zijn:

- Refresh
- Order announce
- Notification
- Status pull

In de calls worden tokens gebruikt, dit zijn JSON Web Tokens. Het is niet nodig voor de webwinkel om deze tokens te kunnen aanmaken of parsen, alle tokens worden door Rabobank en ROK aangeleverd.

### 1.2. Opmerking over 'Expect: 100-Continue' header

POST requests die naar ROK worden verstuurd mogen geen header 'Expect: 100-continue' bevatten. Deze header wordt niet ondersteund door ROK en leidt tot een significante vertraging in de verwerkingstijd. Deze beperking is met name relevant voor (maar niet beperkt tot) webshops die CURL gebruiken voor het versturen van requests.

## 2. Call: Refresh

Om op een veilige manier met ROK te kunnen communiceren, gebruikt de webwinkel een **access token**. Een access token is beperkt geldig (een aantal uur). Als de webwinkel geen geldig **access token** meer heeft, dan moet de webwinkel zijn **refresh token** gebruiken om een nieuw access token op te halen. Dit access token kan dan gebruikt worden voor de volgende order announce calls. De webwinkel moet bijhouden hoe lang een access token geldig is, en wanneer een nieuw access token opgehaald moet worden.

De webwinkel dient het access token te cachen zo lang het nog geldig is. Het is niet de bedoeling dat voor iedere betaling een nieuw access token wordt opgehaald als dat niet nodig is.

### Request

#### Aanroep

De aanroep is een HTTPS GET request zonder body.

#### URL

Sandbox omgeving: *<https://betalen.rabobank.nl/omnikassa-api-sandbox/gatekeeper/refresh>*

Productie omgeving: *<https://betalen.rabobank.nl/omnikassa-api/gatekeeper/refresh>*

#### Headers

In de header is minimaal de entry nodig:

Authorization: Bearer <refresh-token>

Waarbij <refresh-token> wordt vervangen door het refresh token zoals deze uit het Rabobank Dashboard te kopiëren is.

**Let op:** de *Authorization* header is de enige header die toegevoegd moet worden aan de request om met de Omnikassa te kunnen communiceren.

#### Voorbeeld

```
Authorization: Bearer  
eyJraWQiOiIrcUNTdzlvL2dGcUMxeVlHWVhHZFBReGFVVTVLYlppYWVVCZjNiOHFrYWxvPS  
IsImFsZyI6IktVMjU2In0.eyJta2lkIjoxMDI0LCJleHAiOjE0OTExNDU3MjN9.MEYCIQD  
yt1p3lA3zTyl_s8nQuLwBburgWlw3pIrFk4FDyRXebAIhALnCHKUwc81RA7DAv_IF8uOtb  
VcIzJVUc447I14KVe04
```

### Response

Voorbeeld response:

```
{
  "token":
  "eyJraWQiOiJHS0wiLCJhbGciOiJFUzI1NiJ9.eyJwayMiOiJEWmJQsImNpZCI6ImNjYTUtNmRjYyIsImV4cCI6MTQ4MDAwNjQ5MX0.MEQCIGZoLp7HvBS6SbHVfwCICQz_jvF-abvbET2HsENcAKG_AiAY1I8WouBYYRvkbJHamR_PBL36P1b2fCy2H5mZNQtS9Q",
  "validUntil": "2016-11-24T16:54:51.216+0000",
  "durationInMillis": 28800000
}
```

De inhoud van het token veld is het access token.

### 3. Call: Order Announce

Een order wordt aangekondigd bij ROK door een order announce. Deze bevat de details van de order. Het resultaat hiervan is een redirect URL waar de browser van de consument naartoe gestuurd moet worden.

**Let op: Onderstaande documentatie is voor de vernieuwde endpoint voor het aankondigen van orders waarvoor een cryptografische handtekening niet meer vereist is.**

**Doet u nog de aanroep naar <https://betalen.rabobank.nl/omnikassa-api/order/server/api/order> of <https://betalen.rabobank.nl/omnikassa-api-sandbox/order/server/api/order> bekijk dan bijlage A.**

#### Request

##### Aanroep

De aanroep is een HTTPS POST request met een JSON body.

##### URL

Sandbox omgeving: <https://betalen.rabobank.nl/omnikassa-api-sandbox/order/server/api/v2/order>

Productie omgeving: <https://betalen.rabobank.nl/omnikassa-api/order/server/api/v2/order>

##### Headers

In de header zijn minimaal twee entries nodig:

```
Content-Type: application/json  
Authorization: Bearer <access-token>
```

Waarbij <access-token> wordt vervangen door het, in de Refresh call teruggekregen, access token.

##### Voorbeeld:

```
Authorization: Bearer  
eyJraWQiOiJHS0wiLCJhbGciOiJFUzI1NiJ9.eyJwayMiOiJUwMiwiY2lkIjoIYzhjYy1mMThjIiwizXhwIjoxNDc5MTIyODc2fQ.MEUCIQC2Z5WUVTAKcBHISsOVMJIJE8PAbVe5xlio  
r4bgrTcgCwIgLNoVIWEmSbQekJTccM89sosAY-8JzN47DGjvdPGdF0w
```

##### Body

De details van de order worden als een JSON bericht in de body gestopt. Niet als key value pair maar als kale inhoud van de body. De volgende velden worden ondersteund:

#### JSON structuur

| Veld            | Aantal | Formaat                 | Toelichting en opmerkingen   | Voorbeeld                     |
|-----------------|--------|-------------------------|--|-------------------------------|
| timestamp       | 1      | DT                      | ISO 8601 standaard<br><br>Datum/tijd waarop de order wordt aangekondigd bij ROK. In de regel is dit de actuele datum/tijd.<br><br>Dit veld is verplicht en biedt bescherming tegen zogenaamde replay (playback) attacks. | 2017-02-06T08:32:51.759+01:00 |
| merchantOrderId | 1      | AN (strikt).<br>.max 24 | Door Merchant gegenereerd. Als uw webwinkel gebruik wilt maken van AfterPay moet dit veld uniek zijn. Als de id meer dan 24 karakters bevat dan worden de extra karakters na de 24ste karakter weggehaald.               | order123                      |
| description     | 0..1   | AN..max 35              | Omschrijving van de order. Als de description meer dan 35 karakters bevat dan worden de extra karakters na de 35ste karakter weggehaald.   | Een mooie blauwe strandbal.   |
| orderItems      | 0..1   | Array van OrderItems    | De orderregels, zie hieronder voor meer details.   |                               |



| Veld                | Aantal | Formaat             | Toelichting en opmerkingen  | Voorbeeld  |
|---------------------|--------|---------------------|---|--|
| amount              | 1      | Money               | <p>Het totale orderbedrag in centen, inclusief BTW.</p> <p>Het bedrag moet gelijk zijn aan de som over alle order items van de stukprijs (inclusief BTW) vermenigvuldigd met het aantal exemplaren.</p> <p>Als gevolg van de manier waarop de BTW berekend wordt kan het door afrondingsverschillen voorkomen dat deze niet gelijk zijn. We adviseren daarom om het totale BTW bedrag te baseren op de BTW van de stukprijs in plaats van het totale orderbedrag exclusief BTW. Zie voorbeeld</p> <p><b>Let op:</b> Als het bedrag niet gelijk is aan de som van de bedragen van de order items dan</p> <ol style="list-style-type: none"> <li>1. worden de order items uit de orderaankondiging gefilterd, en</li> <li>2. is AfterPay niet als betaalmethode mogelijk</li> </ol> | <p>Veronderstel dat de stukprijs van een order item (exclusief BTW) € 12,98 bedraagt en een BTW tarief van 21% gehanteerd wordt. Wanneer een consument 7 exemplaren bestelt dan is de stukprijs inclusief BTW € <math>12,98 + 21\% = € 15,71</math> afgerond. Het totale orderbedrag (inclusief BTW) dat in dit veld wordt meegegeven is dan <math>7 \times € 15,71 = € 109,97</math>.</p> |
| shippingDetail      | 0..1   | Address             | Het verzendadres, zie hieronder voor meer details.  |  |
| billingDetail       | 0..1   | Address             | Het factuuradres, zie hieronder voor meer details.  |  |
| customerInformation | 0..1   | CustomerInformation | De consument gegevens, zie hieronder voor meer details.   |  |

| Veld              | Aantal | Formaat      | Toelichting en opmerkingen  | Voorbeeld   |
|-------------------|--------|--------------|---|---|
| language          | 0..1   | AN..2        | ISO 639-1 standaard. Niet hoofdletter gevoelig. Als language is niet bepaald dan wordt NL automatisch door de ROK API geselecteerd.<br><br>De volgende talen zijn toegestaan: NL, EN, FR en DE.   | NL  |
| merchantReturnURL | 1      | AN..max 1024 | De URL waar de browser van de consument naar gestuurd wordt na de betaling  | <a href="https://mijn.webwinkel/betalingsresultaat">https://mijn.webwinkel/betalingsresultaat</a> |
| paymentBrand      | 0..1   | AN..50       | Dit veld is optioneel en wordt gebruikt om een specifieke betaalmethode bij de consument af te dwingen in plaats van dat de consument een betaalmethode selecteert op de betaalmethode-selectie pagina.<br><br>Geldige waarden zijn: <ul style="list-style-type: none"> <li>• IDEAL</li> <li>• AFTERPAY</li> <li>• PAYPAL</li> <li>• MASTERCARD</li> <li>• VISA</li> <li>• BANCONTACT</li> <li>• MAESTRO</li> <li>• V_PAY</li> <li>• CARDS</li> </ul> De waarde CARDS zorgt ervoor dat de consument kan kiezen uit de betaalmethoden: MASTERCARD, VISA, BANCONTACT, MAESTRO en V_PAY. | IDEAL   |

| Veld              | Aantal | Formaat | Toelichting en opmerkingen   | Voorbeeld  |
|-------------------|--------|---------|--|------------|
| paymentBrandForce | 0..1   | AN..50  | <p>Dit veld dient alleen te worden aangeleverd wanneer ook het veld paymentBrand (zie hierboven) is gespecificeerd. Met dit veld kan worden gestuurd of, na een mislukte betaling, de consument wel of geen andere betaalmethode kan selecteren om alsnog de betaling te voldoen.</p> <p>Geldige waarden zijn:</p> <ul style="list-style-type: none"> <li>• FORCE_ONCE</li> <li>• FORCE_ALWAYS</li> </ul> <p>In geval van FORCE_ONCE wordt de aangegeven paymentBrand alleen bij de eerste transactie afgedwongen. Wanneer deze faalt dan kan de consument alsnog een andere betaalmethode kiezen. Wanneer voor FORCE_ALWAYS is gekozen kan de consument geen andere betaalmethode kiezen.</p> | FORCE_ONCE |

#### OrderItems

| Veld        | Aantal | Formaat     | Toelichting en opmerkingen  | Voorbeeld  |
|-------------|--------|-------------|---|--|
| id          | 0..1   | AN..max 25  | Item id. Als de id meer dan 25 karakters bevat dan worden de extra karakters na de 25ste karakter weggehaald.                       | A1000  |
| name        | 1      | AN..max 50  | Item naam   | Jackie O Round Sunglasses  |
| description | 0..1   | AN..max 100 | Item omschrijving. Als de omschrijving meer dan 100 karakters bevat dan worden de extra karakters na de 100ste karakter weggehaald. | These distinct, feminine frames balance a classic Jackie-O styling with a modern look. |

| Veld        | Aantal | Formaat   | Toelichting en opmerkingen  | Voorbeeld  |
|-------------|--------|-----------|---|--|
| quantity    | 1      | N         | Aantal: 1-2147483647  | 1  |
| amount      | 1      | Money     | Het bedrag in centen, inclusief BTW, van het item per stuk, zie hieronder voor meer details.  | Als de stukprijs van een order item (exclusief BTW) € 12,98 bedraagt en een BTW tarief van 21% gehanteerd wordt. De stukprijs inclusief BTW € $12,98 + 21\% =$ € 15,71 |
| tax         | 0..1   | Money     | De BTW van het item per stuk, zie hieronder voor meer details.  |  |
| category    | 1      | AN..max 8 | Product categorie: PHYSICAL of DIGITAL.<br>Als de category niet (goed) bepaald is, dan wordt PHYSICAL geselecteerd door de ROK API.   | PHYSICAL   |
| vatCategory | 0..1   | N         | De BTW categorie van het product. De waarden verwijzen naar de verschillende tarieven die in Nederland worden gehanteerd:<br><br>1 = Hoog (momenteel 21%), 2 = Laag (9%), 3 = Nul (0%), 4 = Geen (vrijgesteld van BTW). | 1  |

## Money

| Veld     | Aantal | Formaat | Toelichting en opmerkingen  | Voorbeeld                               |
|----------|--------|---------|---|---|
| amount   | 1      | N       | Het bedrag in centen. .<br><br>Het bedrag kan een negatief getal zijn als er sprake is van een korting. | 1000 of -1000 in het geval van korting. |
| currency | 1      | AN..max | De valuta. Op dit moment ondersteunt ROK alleen EUR   | EUR                                     |

## Address

| Veld        | Aantal | Formaat     | Toelichting en opmerkingen   | Voorbeeld  |
|-------------|--------|-------------|--|------------|
| firstName   | 0..1   | AN..max 50  | Voornaam<br>Als de voornaam meer dan 50 karakters bevat dan worden de extra karakters na de 50ste karakter weggehaald.   | Jan        |
| middleName  | 0..1   | AN..max 20  | Tussenvoegsel of tweede naam.<br>Als de tussenvoegsel meer dan 20 karakters bevat dan worden de extra karakters na de 20ste karakter weggehaald.   | van        |
| lastName    | 1      | AN..max 50  | Achternaam.<br>Als de achternaam meer dan 50 karakters bevat dan worden de extra karakters na de 50ste karakter weggehaald.  | Jansen     |
| street      | 1      | AN..max 100 | Straat.<br><b>Let op:</b> In het geval van betalen met <b>Visa, Mastercard, Bancontact, V PAY</b> en <b>Maestro</b> wordt de straatnaam afgekort tot 50 characters.  | Beukenlaan |
| houseNumber | 0..1   | AN..max 100 | Huisnummer.<br>Als de huisnummer meer dan 100 karakters bevat dan worden de extra karakters na de 100ste karakter weggehaald.<br><b>Let op:</b> In het geval van betalen met <b>Visa, Mastercard, Bancontact, V PAY</b> en <b>Maestro</b> worden dit veld en houseNumberAddition (zie onder) samengevoegd en afgekort tot 10 characters. | 12         |

| Veld                | Aantal | Formaat    | Toelichting en opmerkingen   | Voorbeeld |
|---------------------|--------|------------|--|-----------|
| houseNumberAddition | 0..1   | AN..max 6  | Huisnummer toevoegingen.<br>Als de huisnummer toevoeging meer dan 6 karakters bevat dan worden de extra karakters na de 6de karakter weggehaald. | a         |
| postalCode          | 1      | AN..max 10 | Postcode   | 1234AA    |
| city                | 1      | AN..max 40 | Stad.<br>Als de stad meer dan 40 karakters bevat dan worden de extra karakters na de 40ste karakter weggehaald                                   | Amsterdam |
| countryCode         | 1      | A..2       | landcode, ISO 3166-1 alpha-2   | NL        |

### CustomerInformation

| Veld            | Aantal | Formaat    | Toelichting en opmerkingen  | Voorbeeld       |
|-----------------|--------|------------|---|-----------------|
| emailAddress    | 0..1   | AN..max 45 | Het e-mailadres van de consument.<br>Als het e-mailadres meer dan 25 karakters bevat dan worden de extra karakters na de 25ste karakter weggehaald.       | jan@example.org |
| dateOfBirth     | 0..1   | DD-MM-YYYY | De geboortedatum van de consument.<br>Als de geboortedatum meer dan 10 karakters bevat dan worden de extra karakters na de 10de karakter weggehaald.      | 21-11-1977      |
| gender          | 0..1   | M/F        | Het geslacht van de consument   | F               |
| initials        | 0..1   | A..max 256 | De initialen van de consument.<br>Als de initialen meer dan 256 karakters bevat dan worden de extra karakters na de 256ste karakter weggehaald.           | J.A.N.          |
| telephoneNumber | 0..1   | AN..max 31 | Het telefoonnummer van de consument.<br>Als het telefoonnummer meer dan 31 karakters bevat dan worden de extra karakters na de 31ste karakter weggehaald. | +31204971111    |

### **Veldformaten**

| Formaat | uitleg | voorbeeld |
|---------|--------|-----------|
|---------|--------|-----------|

|                     |   |                               |
|---------------------|---|-------------------------------|
| A..max nn           | Een veld dat uit letters en andere karakters, zoals ".", "@", etc. bestaat. Dit veld bevat maximaal nn karakters.<br><br>HTML tags zijn niet toegestaan.      | J.A.N.                        |
| N                   | Een veld met dit formaat bestaat uit alleen nummers   | 234                           |
| AN (strikt)..max nn | Een veld dat strikt uit alfanumerieke karakters van max nn karakters bestaat  | order123                      |
| AN..max nn          | Een veld dat uit Alfanumeriek en andere karakters, zoals ".", "@", etc. bestaat. Dit veld bevat maximaal nn karakters.<br><br>HTML tags zijn niet toegestaan. | jan@example.org               |
| DT                  | ISO 8601 datum formaat.   | 2017-02-06T08:32:51.759+01:00 |
| DD-MM-YYYY          | Datum formaat gebruikt bij geboorte datum van de consument.   | 25-11-2000                    |
| M/F                 | Het geslacht van de consument.  | F                             |

Een voorbeeld van een minimaal JSON bericht:

```
{
  "timestamp": "2017-02-06T08:32:51.759+01:00",
  "merchantOrderId": "order123",
  "amount": {
    "currency": "EUR",
    "amount": "4999"
  },
  "merchantReturnURL": "http://www.example.org"
}
```

Een voorbeeld van een volledig bericht:

```
{
  "timestamp": "2017-09-11T14:54:57+02:00",
  "merchantOrderId": "order123",
  "description": "Aankoop mijn webwinkel ordernummer 123",
  "orderItems": [
    {
      "id": "A1000",
      "name": "Jackie O Round Sunglasses",
      "description": "These distinct, feminine frames balance a classic Jackie-O styling with a modern look.",
      "quantity": 1,

```

```

        "amount": {
            "currency": "EUR",
            "amount": 22500
        },
        "tax": {
            "currency": "EUR",
            "amount": 4725
        },
        "category": "PHYSICAL",
        "vatCategory": "1"
    }
},
"amount": {
    "currency": "EUR",
    "amount": 22500
},
"shippingDetail": {
    "firstName": "Jan",
    "middleName": "van",
    "lastName": "Jansen",
    "street": "Beukenlaan",
    "houseNumber": "12",
    "houseNumberAddition": "a",
    "postalCode": "1234AA",
    "city": "Amsterdam",
    "countryCode": "NL"
},
"billingDetail": {
    "firstName": "Jan",
    "middleName": "van",
    "lastName": "Jansen",
    "street": "Kersenstraat",
    "houseNumber": "385",
    "houseNumberAddition": "b",
    "postalCode": "1234BB",
    "city": "Haarlem",
    "countryCode": "NL"
},
"customerInformation": {
    "emailAddress": "jan@example.org",
    "dateOfBirth": "21-11-1977",
    "gender": "M",
    "initials": "J.A.N.",
    "telephoneNumber": "+31204971111"
},
"language": "nl",
"merchantReturnURL": "https://mijn.webwinkel.nl/betalingsresultaat",
"paymentBrand": "IDEAL",
"paymentBrandForce": "FORCE_ONCE"
}

```

## Korting

Een korting in de order wordt eveneens aangeleverd middels een OrderItem maar waarbij de velden amount en (indien van toepassing) en tax een negatieve waarde hebben. In onderstaande voorbeelden wordt een korting vastgelegd van 10 euro:



JSON:

```
{
  "id": "1234",
  "name": "Korting",
  "description": "Eenmalige korting",
  "quantity": 1,
  "amount": {
    "currency": "EUR",
    "amount": -1000
  },
  "tax": {
    "currency": "EUR",
    "amount": -210
  },
  "category": "PHYSICAL",
  "vatCategory": "1"
}
```

## Response

Het antwoord is een JSON object met daarin de redirectURL en de omnikassaOrderId. Dit is een unieke waarde die door ROK aan de order wordt toegekend. De omnikassaOrderId kan gebruikt worden om de eindstatus van de order te bepalen in de ordergegevens die via het notificatie mechanisme worden gecommuniceerd. .

Voorbeeld response:

```
{
  "redirectUrl": "https://betalen.rabobank.nl/omnikassa-api/payment-brand?token=eyJraWQiOiJFTU8iLCJhbGciOiJFUzI1NiJ9.eyJlbW8iOiJhYWZhMDAxM y1lYmNiLTQ1ZjZjYTRmYi01OGNjMmQ5MDM2MDIiLCJjaWQiOiIxOTQwLTBkNTgiLCJleHA iOjE0ODAxNTA0Mjd9.MEQCIHJLZjlcNYShX7YzVFvghfwmvH7WTV2Lj5IQIejFyjh7AiBK mvahL29DgiA5vMhGLOHoHaT3SjQKgR4RVxJetG7Fdw&lang=nl",
  "omnikassaOrderId": "1d0a95f4-2589-439b-9562-c50aa19f9caf"
}
```

## Verplichte velden per betaalmethode

Ongeacht de betaalmethode dient in elke order tenminste de merchantOrderId, amount en de merchantReturnUrl te zijn opgenomen. Afhankelijk van de betaalmethode dienen extra gegevens in de order te worden opgenomen. Onderstaande tabel toont welke gegevens dit zijn, uitgesplitst naar betaalmethode:

| Betaalmethode | Aanvullende gegevens in de order  |
|---------------|---|
| iDEAL         | Voor deze betaalmethode zijn geen aanvullende gegevens nodig.   |
| PayPal        | Hoewel niet verplicht adviseren we om ook de order items in de order op te nemen voor extra zekerheid over de betaling van PayPal aan de eigenaar van de webwinkel. |

| Betaalmethode  | Aanvullende gegevens in de order   |
|--|--|
| Bancontact<br><br>VISA<br><br>MasterCard<br><br>V PAY<br><br>Maestro | Hoewel niet verplicht adviseren we om het afleveradres (of indien niet bekend het factuuradres) in de order op te nemen voor extra zekerheid over een succesvolle betaling.  |
| AfterPay   | Voor AfterPay zijn de volgende aanvullende gegevens verplicht: <ul style="list-style-type: none"> <li>• Order items waarbij voor elk order item het id en het description veld verplicht zijn. Ook dient het BTW bedrag of de BTW categorie te worden gespecificeerd.</li> <li>• Factuur- of afleveradres (indien afwijkend dan zijn beide adressen verplicht).</li> </ul> Daarnaast vereist AfterPay dat het veld merchantOrderId uniek is.<br><br>Het orderbedrag dient minimaal 5 euro te zijn. |

Indien voor een betaalmethode de verplichte aanvullende gegevens ontbreken in de order dan kan de consument deze methode niet gebruiken om het betaalverzoek te voldoen. Als de betaalmethode middels het veld paymentBrand in de order was opgenomen dan zal de aankondiging worden geweigerd door Rabo Omnikassa.

Consument wordt geredirect naar de ROK hosted payment pages

De webwinkel moet de redirectUrl gebruiken om de consument te redirecten naar de ROK betalingspagina. Op deze pagina kan de consument kiezen tussen verschillende betalings methode om de betaling af te ronden of de consument kan kiezen om direct terug te gaan naar

### Consument keert terug bij de webwinkel

Als de consument terugkeert naar de webwinkel, dan worden URL parameters toegevoegd om iets te zeggen over de status van de order. Helaas is de definitieve status van een order niet in alle gevallen bekend, bijvoorbeeld bij een iDEAL betaling kan het even duren voordat de status definitief is.

De URL parameters zijn:

| URL Parameter | Betekenis  | Voorbeeld |
|---------------|--|-----------|
| order_id      | Het "merchantOrderId" zoals gebruikt in de Order announce. | order123  |

|           |   |  |
|-----------|---|--|
| status    | De status van de order, zie hieronder voor meer details.                    | COMPLETED  |
| signature | De handtekening van de gegevens in de URL, zie hieronder voor meer details. | 14bf9e935956546887c7c8fd020a0702cd4462d3dd97b48752f3d4d4c5a9cf0afbd8c60d2b7b0e0c46564b1bfeb0a4f7ffc160005c71a1f7c504ef7ca8bbfb82 |

### Statussen

#### **COMPLETED**

De betaling was succesvol.

#### **EXPIRED**

De consument heeft niet betaald binnen de daarvoor gestelde periode.

#### **IN\_PROGRESS**

De betaling is nog niet afgerond. Dit kan voorkomen als gevolg van een storing of vertraging in het achterland van de betalingsverwerking. Dit is een mogelijke uitkomst van een iDEAL of credit card betaling.

#### **CANCELLED**

De consument koos ervoor om niet te betalen.

### Signature

De signature is het resultaat van het toepassen van HMAC-SHA512 (geïnitieerd met de signing key) op het bericht.

De signing key is te kopiëren uit het Rabobank Dashboard. Dit is een shared secret tussen de Rabobank en de webwinkel. Hiermee kan de Rabobank controleren dat het de webwinkel is die het bericht verstuurt. De key wordt aangeleverd in base64 encoded vorm. Bij het initialiseren van de HMAC-SHA512 dient deze eerst base64 gedecodeerd te worden.

### Berekening

Om tot de signature te komen wordt een HMAC-SHA512 berekening uitgevoerd. De HMAC-SHA512 wordt geïnitieerd met de signing key uit het dashboard. Merk op dat deze signing key in base64 encoded vorm wordt aangeleverd en daarom eerst base64 gedecodeerd moet worden. Vervolgens wordt de byte representatie van de string van de aan elkaar geplakte signature velden (op basis van UTF-8 encoding) aan de HMAC-SHA512 aangeboden om tot de signature te komen. De hexadecimale representatie in kleine letters van deze signature wordt tenslotte in het bericht opgenomen.

### Voorbeeld

## PHP

```
$signatureFields = 'order123,COMPLETED';  
$signingKey = '<signing key uit Rabobank Dashboard>';  
$signingKeyDecoded = base64_decode($signingKey);  
  
$signature = hash_hmac('sha512', $signatureFields,  
$signingKeyDecoded);
```

## Java

```
String signatureFields = "order123,COMPLETED";
String signingKey = "<signing key uit Rabobank Dashboard>";
byte[] signingKeyDecoded = Base64.getDecoder().decode(signingKey);

Mac macAlgorithm = Mac.getInstance("HmacSHA512");
Key secretKey = new SecretKeySpec(signingKeyDecoded, "HmacSHA512");
macAlgorithm.init(secretKey);

byte[] result = macAlgorithm.doFinal(signatureFields.getBytes(UTF_8));
String signature = Hex.encodeHexString(result);
```

## C#

```
String signatureFields = "order123,COMPLETED";
String signingKey = "<signing key uit Rabobank Dashboard>";
byte[] signingKeyDecoded = Convert.FromBase64String(signingKey);

string signature = "";
using (var hmacsha512 = new HMACSHA512(signingKeyDecoded))
{
    var stream = new
MemoryStream(Encoding.UTF8.GetBytes(signatureFields));
    foreach (var b in hmacsha512.ComputeHash(stream))
    {
        signature = signature + $"{b:x2}";
    }
}
```

In dit geval worden de twee velden (in de volgorde: order\_id, status) gebruikt als input.

De inhoud van deze velden worden door middel van een komma aan elkaar geplakt.

**Let op dat de volgorde van belang is bij het berekenen van alle soorten signatures.**

## 4. Call: Notification

Een notification is een bericht van ROK aan de webwinkel om aan te kondigen dat er minstens één order een definitieve status heeft bereikt. De notification is een uitnodiging aan de webwinkel om de statussen van deze orders op te halen (Status pull call). De webwinkel is vrij om dit onmiddellijk te doen (nog voordat er antwoord is gegeven op de notification) of op een later moment. De notification bevat een token dat gebruikt moet worden in de status pull call, en dit token heeft een beperkte geldigheid (minuten). Als de webwinkel geen status update call doet, zal ROK later een nieuwe notification sturen. Echter na een aantal uur zal ROK het opgeven, tot de volgende order wordt afgehandeld.

De notification wordt ondertekend door ROK zodat de webwinkel de integriteit ervan kan controleren. Analooq aan de andere berichten wordt de handtekening berekend met behulp van de signeursleutel zoals deze voor de webwinkel geconfigureerd is.

Indien bij ROK meerdere signeursleutels actief zijn voor de web winkel dan zal ROK voor elke sleutel afzonderlijk een notification naar de webwinkel versturen. ROK weet immers niet welke van deze signeursleutels geconfigureerd is binnen de webwinkel. Van precies één notification kan de webwinkel een succesvolle controle uitvoeren van de handtekening. De authentication van deze notification kan door de webwinkel gebruikt worden voor de status pull call. ROK zal de statussen van deze orders met dezelfde signeursleutel ondertekenen.

### Request

De call is een HTTPS POST met in de body de relevante informatie als JSON object.

### URL

ROK stuurt het notification bericht naar de webhook URL zoals die opgegeven is in het Rabobank Dashboard.

### Headers

De header bevat minimaal de entry:

Content-Type: application/json

### Body

De body van de notification is een JSON object met daarin de volgende velden:

| Veld | Betekenis | Voorbeeld |
|------|-----------|-----------|
|------|-----------|-----------|

|                |   |  |
|----------------|---|--|
| authentication | Het token dat gebruikt kan worden om de status pull te doen   | eyJraWQiOiJOTyIsImFsZyI6IktVTMjU2In0.eyJubyMiOiJyMywibWtpZCI6NSwibm8kIjoibWVyY2hhbnQub3JkZXIuc3RhdHVzLmNoYW5nZWQiLCJjaWQiOiJhYmNkLTEyMzQiLCJleHAiOiJlE0ODg0NjQ1MDN9.MEUCIHtPFoKmAxc7JNQjj0U5rWpl0zR9RsQvgj_n-ckHBngHAiEAmbtgrxaiky4cS3BTHd0DJ8md3Rn7V13Nv35m5DurY1wI |
| expiry         | De geldigheidsduur van het token, in het ISO-8601 formaat (yyyy-MM-ddTHH:mm:ss.SSSZZ)   | 2016-11-25T09:53:46.765+01:00  |
| eventName      | Het type notificatie. Voorlopig is dit altijd: merchant.order.status.changed  | merchant.order.status.changed  |
| poiId          | Identificatie van de webwinkel (point of interaction), vanuit ROK gezien. Dit is relevant indien er meerdere webwinkels gebruik maken van dezelfde webhook URL. | 123  |
| signature      | Het signature van het bericht, zie kopje signature voor details.  |  |

### Signature

De handtekening over het notification bericht wordt berekend op dezelfde manier als de handtekening bij de terugkeer URL van de webshop (zie vorige hoofdstuk). De gebruikte velden zijn in volgorde:

- authentication
- expiry
- eventName
- poiId

Voor het voorbeeld wordt de signature bepaald op basis van de volgende string:

```
eyJraWQiOiJOTyIsImFsZyI6IktVTMjU2In0.eyJubyMiOiJyMywibWtpZCI6NSwibm8kIjoibWVyY2hhbnQub3JkZXIuc3RhdHVzLmNoYW5nZWQiLCJjaWQiOiJhYmNkLTEyMzQiLCJleHAiOiJlE0ODg0NjQ1MDN9.MEUCIHtPFoKmAxc7JNQjj0U5rWpl0zR9RsQvgj_n-ckHBngHAiEAmbtgrxaiky4cS3BTHd0DJ8md3Rn7V13Nv35m5DurY1wI,2016-11-25T09:53:46.765+01:00,merchant.order.status.changed,123
```

### **Response**

Bij succesvolle ontvangst van de notificatie verwacht ROK HTTP response code 200. Wanneer een HTTP response code anders dan 200 wordt verstuurd dan veronderstelt Omnikassa dat de notificatie niet kon worden verwerkt. ROK zal dan geen nieuwe poging ondernemen totdat een nieuwe order verwerkt is.

## 5. Call: Status pull

Met deze call haalt de webwinkel definitieve statussen op van orders.

### Request

#### Aanroep

De call is een HTTPS GET met lege body.

#### URL

Sandbox omgeving: *https://betalen.rabobank.nl/omnikassa-api-sandbox/order/server/api/events/results/merchant.order.status.changed*

Productie omgeving: *https://betalen.rabobank.nl/omnikassa-api/order/server/api/events/results/merchant.order.status.changed*

#### Headers

In de header is minimaal de entry nodig:

Authorization: Bearer <notification-token>

Het <notification-token> is het veld "authentication" uit de notificatie.

### Response

De response body bevat een JSON object met de volgende velden:

| Veld                      | Betekenis  | Voorbeeld  |
|---------------------------|--|--|
| moreOrderResultsAvailable | Indicatie of er nog meer order resultaten beschikbaar zijn dan in dit bericht zitten. In dat geval kan (met hetzelfde notification token) nog een status pull call gedaan worden. Dit kan herhaald worden totdat het resultaat false is. | true   |
| orderResults              | Een array met daarin per order de resultaten   | zie kopje orderResults voor details  |
| signature                 | Het signature van het bericht, zie kopje signature voor details.   | 99ca2487243fbad72bbaa456a3219db7b0d2a19777f436cedb3c045e999b86c05001bb0837b43caa3d1757321d00959ac2a161f473a103af72bf440db5147b4a |



### orderResults velden

| Veld                 | Betekenis   | Voorbeeld                            |
|----------------------|---|--------------------------------------|
| merchantOrderId      | OrderId zoals aangeleverd tijdens de Order announce   | order123                             |
| omnikassaOrderId     | Dit is het unieke ID dat ROK aan deze order heeft toegekend. De waarde komt overeen met de waarde van het gelijknamige veld in het responsebericht van de orderaankondiging (zie hoofdstuk 3) | 1d0a95f4-2589-439b-9562-c50aa19f9caf |
| poiId                | Unieke identificatie van de webwinkel (point of interaction), vanuit ROK gezien. Dit is relevant indien er meerdere webwinkels gebruik maken van dezelfde webhook URL.                        | 2004                                 |
| orderStatus          | De status van de order. Zie hoofdstuk "Consument keert terug bij de webwinkel" voor een overzicht van de mogelijke statussen.   | CANCELLED                            |
| orderStatusDateTime  | Het moment dat deze status is bereikt.  | 2016-11-25T13:20:03.157+01:00        |
| errorCode            | Toekomstig veld, voor nu: altijd leeg   |                                      |
| paidAmount currency  | De valuta waarin betaald is   | EUR                                  |
| paidAmount amount    | Het bedrag dat door de consument betaald is   | 0                                    |
| totalAmount currency | De valuta van de order  | EUR                                  |
| totalAmount amount   | Het totaalbedrag van de order, in centen  | 4999                                 |

### Voorbeeld response

```
{
  "signature":
    "99ca2487243fbad72bbaa456a3219db7b0d2a19777f436cedb3c045e999b86c05001b
    b0837b43caa3d1757321d00959ac2a161f473a103af72bf440db5147b4a",
  "moreOrderResultsAvailable": false,
  "orderResults": [
    {
      "merchantOrderId": "order123",
      "omnikassaOrderId": "1d0a95f4-2589-439b-9562-c50aa19f9caf",
      "poiId": "2004",
      "orderStatus": "CANCELLED",
      "orderStatusDateTime": "2016-11-25T13:20:03.157+01:00",
      "errorCode": "",
      "paidAmount": {
        "currency": "EUR",
        "amount": "0"
      },
    },
  ],
}
```

```

        "totalAmount": {
            "currency": "EUR",
            "amount": "4999"
        }
    }
]
}

```

### Signature

De handtekening over het resultaat wordt berekend op dezelfde manier als de andere handtekeningen. De gebruikte velden zijn in volgorde:

- moreOrderResultsAvailable
- De orderResults

Voor iedere orderResult worden de volgende velden in volgorde gebruikt:

- merchantOrderId
- omnikassaOrderId
- poiId
- orderStatus
- orderStatusDateTime
- errorCode
- paidAmount currency
- paidAmount amount
- totalAmount currency
- totalAmount amount

Voor het voorbeeld wordt de signature bepaald op basis van de volgende string:

```

false,order123,1d0a95f4-2589-439b-9562-
c50aa19f9caf,2004,CANCELLED,2016-11-
25T13:20:03.157+01:00,,EUR,0,EUR,4999

```



## **BIJLAGE A: Berekenen signature voor verouderde aanroeppunt order.**

Wanneer de webshop een order aankondiging doet naar de verouderde endpoint voor de order aankondiging is het berekenen van de signature een vereiste.

### Verouderde URL

Sandbox omgeving: *<https://betalen.rabobank.nl/omnikassa-api-sandbox/order/server/api/order>*

Productie omgeving: *<https://betalen.rabobank.nl/omnikassa-api/order/server/api/order>*

### De signature moet als extra veld vermeld worden in body van de aankondiging.

Een voorbeeld van een minimale JSON bericht zal er dan zo uitzien:

```
{
  "timestamp": "2017-02-06T08:32:51.759+01:00",
  "merchantOrderId": "order123",
  "amount": {
    "currency": "EUR",
    "amount": "4999"
  },
  "merchantReturnURL": "http://www.example.org",
  "signature":
  "1795e71284f9e3e5805fe43964259f28810cd5047a726a5aaa48043eac69e87e28ce2
  3e97032f4a08444b0509dbe9f247a2c99f06017fdb7b85b06710a1c666a"
}
```

Een voorbeeld van een complete bericht zal er dan zo uitzien:

```
{
  "timestamp": "2017-09-11T14:54:57+02:00",
  "merchantOrderId": "order123",
  "description": "Aankoop mijn webwinkel ordernummer 123",
  "orderItems": [
    {
      "id": "A1000",
      "name": "Jackie O Round Sunglasses",
      "description": "These distinct, feminine frames balance a classic Jackie-O styling with a modern look.",
      "quantity": 1,
      "amount": {
        "currency": "EUR",
        "amount": 22500
      },
      "tax": {
        "currency": "EUR",
        "amount": 4725
      },
      "category": "PHYSICAL",
      "vatCategory": "1"
    }
  ],
}
```

```

"amount": {
  "currency": "EUR",
  "amount": 22500
},
"shippingDetail": {
  "firstName": "Jan",
  "middleName": "van",
  "lastName": "Jansen",
  "street": "Beukenlaan",
  "houseNumber": "12",
  "houseNumberAddition": "a",
  "postalCode": "1234AA",
  "city": "Amsterdam",
  "countryCode": "NL"
},
"billingDetail": {
  "firstName": "Jan",
  "middleName": "van",
  "lastName": "Jansen",
  "street": "Kersenstraat",
  "houseNumber": "385",
  "houseNumberAddition": "b",
  "postalCode": "1234BB",
  "city": "Haarlem",
  "countryCode": "NL"
},
"customerInformation": {
  "emailAddress": "jan@example.org",
  "dateOfBirth": "21-11-1977",
  "gender": "M",
  "initials": "J.A.N.",
  "telephoneNumber": "+31204971111"
},
"language": "nl",
"merchantReturnURL": "https://mijn.webwinkel.nl/betalingsresultaat",
"paymentBrand": "IDEAL",
"paymentBrandForce": "FORCE_ONCE",
"signature":
"1a0f6e4526fb81d5bf70fe2a9d7a3c46a2a1e85993b5df08cd2a7ff5324d48da6a12f
b38a38ccb4c4d44b9901f7f3a5b5fe6aec475db6fe24c57fcc4f2d6eff2"
}

```

De voorwaarden van de signature veld staan hieronder vermeld:

| Veld      | Aantal | Formaat | Voorbeeld  |
|-----------|--------|---------|--|
| signature | 1      | AN..128 | 1795e71284f9e3e5805f<br>e43964259f28810cd504<br>7a726a5aaa48043eac69<br>e8728ce23e97032f4a08<br>44b0509dbe9f247a2c99<br>f06017fdb7b85b06710a<br>1c666a |

### Signature

De signature is het resultaat van het toepassen van HMAC-SHA512 (geïnitieerd is met de signing key) op het bericht.

De signing key is te kopiëren uit het Rabobank Dashboard. Dit is een shared secret tussen de Rabobank en de webwinkel. Hiermee kan de Rabobank controleren dat het de webwinkel is die het bericht verstuurt. De key wordt aangeleverd in base64 encoded vorm. Bij het initialiseren van de HMAC-SHA512 dient deze eerst base64 gedecodeerd te worden.

### Input

De signature wordt berekend over onderstaande velden, in dezelfde volgorde als aangegeven, van het JSON object:

1. timestamp
2. merchantOrderId,
3. amount currency
4. amount amount
5. language\*\*
6. description\*\*
7. merchantReturnURL
8. (order items)\*
9. (shipping detail)\*
10. (paymentBrand)\*
11. (paymentBrandForce)\*
12. (customerInformation)\*
13. (billing detail)\*

De inhoud van deze velden wordt komma gescheiden aan elkaar geplakt.

De (..)\* velden zijn optioneel, als deze velden voor een gegeven order geen waarde hebben dan worden ze niet opgenomen in de payload voor de berekening van de signature (ook niet als lege waarde).

De \*\* velden zijn optioneel, maar worden wel altijd als onderdeel van de signature gebruikt. Als deze voor een gegeven order geen waarde hebben dan wordt voor elk een lege string in de payload opgenomen.

#### *Voorbeelden:*

De aan elkaar geplakte signature velden van het minimale voorbeeldbericht zijn:

```
2017-02-06T08:32:51.759+01:00,order123,EUR,4999,,http://www.example.org
```

De aan elkaar geplakte signature velden van het volledige voorbeeldbericht zijn:

```
2017-09-11T16:28:07+02:00,order123,EUR,22500,nl,Aankoop mijn webwinkel  
ordernummer  
123,https://mijn.webwinkel.nl/betalingsresultaat,A1000,Jackie O Round  
Sunglasses,These distinct, feminine frames balance a classic Jackie-O  
styling with a modern  
look.,1,EUR,22500,EUR,4725,PHYSICAL,1,Jan,van,Jansen,Beukenlaan,12,a,1  
234AA,Amsterdam,NL,IDEAL,FORCE_ONCE,jan@example.org,21-11-  
1977,M,J.A.N.,+31204971111,Jan,van,Jansen,Kersenstraat,385,b,1234BB,Ha  
arlem,NL
```

Als de order aankondiging de volgende waarden bevat:

```
timestamp = 2017-02-06T08:32:51.759+01:00  
merchantOrderId = order123  
language = nl  
description = Beschrijving order  
currency = EUR  
amount = 4999  
merchantReturnURL = http://www.example.org
```

Dan zal de payload voor het bereken van de signature als volgt eruit zien:

```
2017-02-06T08:32:51.759+01:00,order123,EUR,4999,nl,Beschrijving  
order,http://www.example.org
```

In bovenstaand voorbeeld hebben de velden timestamp t/m merchantReturnURL elke een waarde. Deze worden daarom opgenomen in de payload. De (..)\* velden hebben in dit voorbeeld geen waarde en worden daarom niet de payload opgenomen.

Als de order aankondiging de volgende waarden bevat:

```
timestamp = 2017-02-06T08:32:51.759+01:00  
merchantOrderId = order123  
language =  
description =  
currency = EUR
```

amount = 4999  
merchantReturnURL = <http://www.example.org>

Dan zal de payload voor het berekenen van de signature als volgt eruit zien:

```
2017-02-  
06T08:32:51.759+01:00,order123,EUR,4999,,,http://www.example.org
```

De velden language en description hebben geen waarden. Voor deze velden wordt daarom op positie 5 en 6 in de payload een lege string opgenomen. De (..)\* velden hebben in dit voorbeeld wederom geen waarde. Deze worden daarom niet de payload opgenomen.

Als de order aankondiging de volgende waarden bevat:

```
timestamp = 2017-02-06T08:32:51.759+01:00  
merchantOrderId = order123  
language =  
description =  
currency = EUR  
amount = 4999  
merchantReturnURL = http://www.example.org  
orderitems =  
shippingDetail =  
paymentBrand = IDEAL  
paymentBrandForce = FORCE_ONCE
```

Dan zal de payload voor het berekenen van de signature als volgt eruit zien:

```
2017-02-  
06T08:32:51.759+01:00,order123,EUR,4999,,,http://www.example.org,IDEAL  
,FORCE_ONCE
```

In dit voorbeeld hebben de velden paymentBrand en paymentBrandForce een waarde en worden daarom aan de payload toegevoegd. Omdat de (..)\* velden customerInformation en billingDetail geen waarde hebben worden deze niet meegenomen.

### *Order Items*

De velden van de order items worden toegevoegd in de volgende volgorde:

1. (id)\*
2. name
3. description
4. quantity
5. amount currency



6. amount amount
7. (tax velden) \*\*
8. category
9. (vatCategory)\*

De velden worden op eenzelfde manier aan elkaar geplakt als bij de order. Indien een veld niet aanwezig is, dan wordt de inhoud als leeg beschouwd.

De (..)\* velden zijn optioneel, als ze niet meegegeven worden in de request dan moet de webwinkel applicatie deze velden niet gebruiken voor het berekenen van de signature.

\*\* tax is een optioneel veld, als dat niet aanwezig is, wordt het als een enkel leeg veld beschouwd. Indien het wel aanwezig is, worden de amount en currency als twee losse velden toegevoegd.

### *Voorbeelden*

Als de order aankondiging de volgende waarden bevat:

```
timestamp = 2017-02-06T08:32:51.759+01:00
merchantOrderId = order123
language = nl
description = Beschrijving order
currency = EUR
amount = 100
merchantReturnURL = http://www.example.org
id = itemId123
name = naam item
description = beschrijving item
quantity = 2
currency = EUR
amount = 50
currency (tax) = EUR
amount (tax) = 0
category = PHYSICAL
vatCategory = 3
```

Dan zal de payload voor het berekenen van de signature er als volgt eruit zien:

```
2017-02-06T08:32:51.759+01:00,order123,EUR,100,nl,Beschrijving
order,http://www.example.org,itemId123,naam item,beschrijving
item,2,EUR,50,EUR,0,PHYSICAL,3
```

Als de order aankondiging de volgende waarden bevat:

```
timestamp = 2017-02-06T08:32:51.759+01:00
merchantOrderId = order123
language = nl
description = Beschrijving order
currency = EUR
amount = 100
merchantReturnURL = http://www.example.org
```

id =  
name = naam item  
description = beschrijving item  
quantity = 2  
currency = EUR  
amount = 50  
currency (tax) =  
amount (tax) =  
category = PHYSICAL  
vatCategory =

Dan zal de payload voor de berekening van de signature er als volgt eruit zien:

```
2017-02-06T08:32:51.759+01:00,order123,EUR,100,nl,Beschrijving  
order,http://www.example.org,naam item,beschrijving  
item,2,EUR,50,,,PHYSICAL
```

In dit voorbeeld hebben de (..)\* velden currency (tax) en amount (tax) geen waarde. Daarom wordt voor deze velden een lege string in de payload opgenomen (op posities 13 en 14).

### *Shipping & billing details*

De velden van de shipping- en billingdetails worden toegevoegd in de volgende volgorde:

1. firstName
2. middleName
3. lastName
4. street
5. (houseNumber)\*
6. (houseNumberAddition)\*
7. postalCode
8. city
9. countryCode

De velden worden op eenzelfde manier aan elkaar geplakt als bij de order.

De (..)\* velden zijn optioneel, als ze niet meegegeven worden in de request dan moet de webwinkel applicatie deze velden niet gebruiken voor het berekenen van de signature.

### *Customer information*

De velden van de customer information worden toegevoegd in de volgende volgorde:

1. emailAddress\*\*

2. dateOfBirth\*\*
3. gender\*\*
4. initials\*\*
5. telephoneNumber\*\*

De \*\* velden zijn optioneel, maar worden wel altijd als onderdeel van de signature gebruikt. Als ze niet meegegeven worden in de request dan moet webwinkel applicatie een lege waarde als deelinput voor de signature gebruiken.

### Berekening

Om tot de signature te komen wordt een HMAC-SHA512 berekening uitgevoerd. De HMAC-SHA512 wordt geïnitieerd met de signing key uit het dashboard. Merk op dat deze signing key in base64 encoded vorm wordt aangeleverd en daarom eerst base64 gedecodeerd moet worden. Vervolgens wordt de byte representatie van de string van de aan elkaar geplakte signature velden (op basis van UTF-8 encoding) aan de HMAC-SHA512 aangeboden om tot de signature te komen. De hexadecimale representatie in kleine letters van deze signature wordt tenslotte in het bericht opgenomen.

### Voorbeeld

#### **PHP**

```
$signatureFields = '2017-02-06T08:32:51.759+01:00,order123,EUR,4999,,,http://www.example.org';
$signingKey = '<signing key uit Rabobank Dashboard>';
$signingKeyDecoded = base64_decode($signingKey);

$signature = hash_hmac('sha512', $signatureFields,
$signingKeyDecoded);
```

#### **Java**

```
String signatureFields = "2017-02-06T08:32:51.759+01:00,order123,EUR,4999,,,http://www.example.org";
String signingKey = "<signing key uit Rabobank Dashboard>";
byte[] signingKeyDecoded = Base64.getDecoder().decode(signingKey);

Mac macAlgorithm = Mac.getInstance("HmacSHA512");
Key secretKey = new SecretKeySpec(signingKeyDecoded , "HmacSHA512");
macAlgorithm.init(secretKey);

byte[] result = macAlgorithm.doFinal(signatureFields.getBytes(UTF_8));
String signature = Hex.encodeHexString(result);
```

#### **C#**

```
String signatureFields = "2017-02-06T08:32:51.759+01:00,order123,EUR,4999,,,http://www.example.org";
String signingKey = "<signing key uit Rabobank Dashboard>";
byte[] signingKeyDecoded = Convert.FromBase64String(signingKey);
```

```

string signature = "";
using (var hmacsha512 = new HMACSHA512(signingKeyDecoded))
{
    var stream = new
MemoryStream(Encoding.UTF8.GetBytes(signatureFields));
    foreach (var b in hmacsha512.ComputeHash(stream))
    {
        signature = signature + $"{b:x2}";
    }
}

```

## Response

In de response van de verouderde order aankondiging wordt ook een signature aangeleverd.

De signature in de response wordt op dezelfde manier berekend als de signature van het request voor het aankondigen van de order, het verschil is dat in de response de signature is gebaseerd op het veld redirectUrl.

Voorbeeld response:

```

{
  "signature":
"d3dd97b48752f3d4d4c5a914bf9e935956546887c7c8fd020a0702cd4462fbd8c60d2
b7b0e0c4fc160005c71a1f7c504ef7ca8bbfb82cf0a6564b1bfeb0a4f7f",
  "redirectUrl": "https://betalen.rabobank.nl/omnikassa-api/payment-
brand?token=eyJraWQiOiJFTU8iLCJhbGciOiJFUzI1NiJ9.eyJlbW8iOiJhYWZhMDAxM
y1lYmNiLTQ1ZjZjYTRmYi01OGNjMmQ5MDM2MDIiLCJjaWQiOiIxOTQwLTBkNTgiLCJleHA
iOiJlE0ODAxNTA0Mjd9.MEQCIHJLZjlcNYShX7YzVFvghfwmvH7WTV2Lj5IQIejFyjH7AiBK
mvahL29DgiA5vMhGLOHoHaT3SjQKgR4RVxJetG7Fdw&lang=nl"
}

```