Connectivity Guide

eftpos API Gateway

eftpos
Good for Australia

apidevportal@eftposaustralia.com.au

last updated: 22-Jun-2021

Copyright, confidentially and disclaimer

Copyright in this document belongs to eftpos Payments Australia Limited ABN 37 136 180 366 (eftpos)

This document contains the latest information available at the time of publication. However, eftpos reserves the right to modify the information described herein at any time, with or without published notification. eftpos does not warrant the accuracy of the information contained in this document and eftpos has no liability for any reliance by any party on the information contained in this document or for any direct or indirect, special, consequential losses or punitive damages under any cause of action, whether in contract, tort, under indemnity or statute (including for loss of data, loss of reputation, loss of business opportunity or loss of anticipated savings) in connection with this document.

Written and published in Sydney, Australia by eftpos

eftpos Payments Australia Limited ABN 37 136 180 366
Head Office Level 11, 45 Clarence Street, Sydney NSW 2000 I GPO Box 126, Sydney NSW 2001
Telephone +61 2 8270 1800 I Facsimile +61 2 9299 2885 I Email: info@eftposaustralia.com.au
www.eftposaustralia.com.au

Table of Contents

eftpos Payments Australia Limited ABN 37 136 180 366
Head Office Level 11, 45 Clarence Street, Sydney NSW 2000 I GPO Box 126, Sydney NSW 2001
Telephone +61 2 8270 1800 I Facsimile +61 2 9299 2885 I Email: info@eftposaustralia.com.au
www.eftposaustralia.com.au

1.0 Connecting to the eftpos API Gateway

To successfully connect to the eftpos API Gateway services the following connectivity is required:

1. *Transport Layer Security* - Mutual Transport Layer Security (mTLS) Authentication v1.2 is used for secure connection between systems for PROD and CERT testing.
2. *Application Layer Security* - OAuth 2.0 Client Credentials Grant is used to provide access to different API Products to those only authorised API Clients.
3. *Message Layer Security* – dependent on the backend service; e.g. the eftpos Tokenisation Service uses JWE for passing sensitive card and token information within the request and response to/from the eTSP.

eftpos API environments

Environment	Host	mTLS (v1.2)
1. PROD (SECURE)	**sapi**.eftpos.io/{api-path}	Yes
2. CERT (SECURE)	**cert.sapi**.eftpos.io/stable/{api-path}	Yes
3. SANDBOX (SECURE)	**sandbox.sapi**.eftpos.io/{api-path}	Yes
4. SANDBOX	**sandbox.api**.eftpos.io/{api-path}	No

eftpos Payments Australia Limited ABN 37 136 180 366
Head Office Level 11, 45 Clarence Street, Sydney NSW 2000 I GPO Box 126, Sydney NSW 2001
Telephone +61 2 8270 1800 I Facsimile +61 2 9299 2885 I Email: info@eftposaustralia.com.au
www.eftposaustralia.com.au

eftpos APIs and Paths

eftpos API Products	API Path	Message Layer Security
1. BIN Inquiry API	`/bin/v1`	`Not Required`
2. CNP Payment API	`/payment/v1`	`Not Required`
3. Fast Funds API	`/fastfunds/v1`	`Not Required`
4. Token on File API	`/ets/v1`	`JWE`
5. Issuer Disputes & Chargebacks API	`/issuer/v1`	`Not Required`
6. Acquirer Disputes & Chargebacks API	`/acquirer/v1`	`Not Required`
7. Reference Data API	`/info/v1`	`Not Required`
8. QR Order API	`/qrorder/v1`	`HMAC`
9. QR Wallet API	`/qrcode/v1`	`HMAC`

1.1 Transport Layer Security

For the initial set up and configuration of Mutual Transport Layer Security (mTLS) v1.2 it is necessary to generate a private key and a certificate signing request (CSR) using the command:-

```
openssl req -new -config csr.cnf -keyout key.pem -out certificate.csr
```

Where the following information is contained in the `csr.cnf` file:-

`fqdn` (fully qualified domain name) must be of the format

- `nonprod.<YOUR_ORG_NAME>.api.eftpos.io` for SANDBOX and CERT environment
- `<YOUR_ORG_NAME>.api.eftpos.io` for PROD environment

eftpos Payments Australia Limited ABN 37 136 180 366
Head Office Level 11, 45 Clarence Street, Sydney NSW 2000 I GPO Box 126, Sydney NSW 2001
Telephone +61 2 8270 1800 I Facsimile +61 2 9299 2885 I Email: info@eftposaustralia.com.au
www.eftposaustralia.com.au

`orgName`

- Should be a name that is representative of your company.

`email` must be

- A team or group email, i.e. a persistent email address. Do not use an individual employee's email address or email address that is not likely to be in place in the longer term.

The full template for the CSR file is as follows

```
# OpenSSL configuration file for creating a CSR for a server certificate
# Adapt at least the fqdn and orgName lines, and then run
# openssl req -new -config csr.cnf -keyout key.pem -out certificate.csr
# on the command line.

# The fully qualified server (or service) name.
# Omit the "nonprod." prefix for production requests.


fqdn = nonprod.<ORGANISATION_NAME>.api.eftpos.io

# The name of the organization that will own this client certificate
orgName = <ORGANISATION_NAME>

# The email address to send the signed certificate to. This should ideally
be a distribution
# list to minimise impact during certificate rotations. A near-expiry
reminder email will
# also be sent to this address.
email = <ORGANISATION_EMAIL_DISTRIBUTION_LIST>

# subjectAltName entries: to add DNS aliases to the CSR.
# This parameter is only be necessary when issuing a server certificate, but
it doesn't hurt to include it.
# Delete the '#' character in the ALTNAMES line (to comment it out), and
change the subsequent
# 'DNS:' entries accordingly. Please note: all DNS names must resolve to the
same IP address as the FQDN.
altNames = DNS:$fqdn   # , DNS:bar.example.org , DNS:www.foo.example.org

# --- no modifications required below ---
[ req ]
default_bits = 2048
default_md = sha256
prompt = no
encrypt_key = no
distinguished_name = dn
req_extensions = req_ext
```


eftpos Payments Australia Limited ABN 37 136 180 366
Head Office Level 11, 45 Clarence Street, Sydney NSW 2000 I GPO Box 126, Sydney NSW 2001
Telephone +61 2 8270 1800 I Facsimile +61 2 9299 2885 I Email: info@eftposaustralia.com.au
www.eftposaustralia.com.au

```
[ dn ]
countryName = AU
stateOrProvinceName = NSW
localityName = Sydney
organizationName = $orgName
commonName = $fqdn
emailAddress = $email

[ req_ext ]
subjectAltName = $altNames
```

Once the command is executed, this should generate a private key file named `key.pem` and a CSR file named `certificate.csr`.

Keep your private key in a secure location and send only the `certificate.csr` file to ems@eftposaustralia.com.au for review.

2.1 Application Layer Security

Authorization to call an eftpos API follows the standard OAuth 2.0 Client Credentials Grant.

An `access_token` must be obtained, at least every 60minutes, by the API Client (app) authenticating against the eftpos authorisation server's token URL endpoint using its unique Client Credentials. The Client

eftpos Payments Australia Limited ABN 37 136 180 366
Head Office Level 11, 45 Clarence Street, Sydney NSW 2000 I GPO Box 126, Sydney NSW 2001
Telephone +61 2 8270 1800 I Facsimile +61 2 9299 2885 I Email: info@eftposaustralia.com.au
www.eftposaustralia.com.au

Credentials consist of a `client_id` (referred to as a "Key" in the eftpos API Developer Portal) and `client_secret` which are obtained when creating an app in the eftpos API Developer Portal.

The following table shows how client credentials are obtained from eftpos for each environment and the URL that should be used to obtain an `access_token`.

eftpos API environments

Environment	Access Token URL	OAuth 2.0 Client Credentials
10. PROD	`https://sapi.eftpos.io/oauth/v1/token`	eftpos supply via the Dev Portal.
11. CERT	`https://cert.sapi.eftpos.io/oauth/v1/token (mTLS)`	eftpos supply upon request
12. SANDBOX	`https://sandbox.api.eftpos.io/oauth/v1/token (mTLS)` `https://cert.api.eftpos.io/oauth/v1/token (no mTLS)`	Self service from Dev Portal

The eftpos API Gateway uses a Bearer Token for authorization; i.e. the following is included in the header of the POST request to obtain a token

```
Authorization: Basic <credentials>
```

Where `<credentials>` is the base64 url encoding of the concatenated string of

`<client_id>` + `:` + `<client_secret>`

And the Request body contains the the `client_id` and `grant_type` as `x-www-form-urlencoded` content type (as shown in the following cURL) example

```
curl --location --request POST
'https://sandbox.api.eftpos.io/oauth/v1/token' \
--header 'Authorization: Basic
aFNpM09YaDZacEtyb2FteDhlQ0VjNUdrUkoyZUh4T0g6SG9YR0FNYUNXbXQ0akVSdA==' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=hSi3OXh6ZpKrtalx8eCEc5GkRJ2eHxOH' \
--data-urlencode 'grant_type=client_credentials'
```


eftpos Payments Australia Limited ABN 37 136 180 366
Head Office Level 11, 45 Clarence Street, Sydney NSW 2000 I GPO Box 126, Sydney NSW 2001
Telephone +61 2 8270 1800 I Facsimile +61 2 9299 2885 I Email: info@eftposaustralia.com.au
www.eftposaustralia.com.au

If everything is valid the `access_token` will be returned in the response as follows:-

```
{
     "client_id", "<client_id>",
     "access_token": "<access_token>",
     "expires_in": "3599",
     "scopes": "",
     "token_type": "Bearer"
}
```

The `access_token` may then be used in the header of an API request as a Bearer Token

```
Authorization: Bearer <access_token>
```

The following is a cURL example of an API call:-

```
curl --location --request GET
'https://sandbox.api.eftpos.io/stable/bin/v1/bins' \

--header 'Authorization: Bearer 2vxXgYNh0SOdWdXz5YEz7htVT1XV'
```


eftpos Payments Australia Limited ABN 37 136 180 366
Head Office Level 11, 45 Clarence Street, Sydney NSW 2000 I GPO Box 126, Sydney NSW 2001
Telephone +61 2 8270 1800 I Facsimile +61 2 9299 2885 I Email: info@eftposaustralia.com.au
www.eftposaustralia.com.au

3.1 Message Layer Security

The backend service for some APIs may also require a level of security between the API Client. The type of security is specific to the backend service and hence where required it is listed as a separate sub section:-

3.1.1 Token on File API

JSON Web Encryption (JWE) is used to protect sensitive fields. The complete message is not encrypted, only the fields indicated in API definitions will be encrypted. This constitutes an additional security layer on top of the transport layer security mechanisms.

In order to use JWE, the Token Requestor must generate a certificate and share it with eftpos to be configured on the eTSP. The Token Requestor's mTLS/SSL client certificate may satisfy this requirement.

The eTSP shall generate a certificate dedicated to JWE with each Token Requestor it communicates with. The certificates shall be exchanged in PEM encoded X509 format (base64url encoding).

The JSON Web Encryption may be configured to use either Compact or JSON Serialization and is broken into five pieces as per the JWE specification:

- **JWE Protected Header**: Encoded JSON string with information regarding the cryptography used for the remaining sections.
    - `alg` - algorithm: Algorithm used to encrypt the Content Encryption Key (CEK). Currently, RSA1_5 is an acceptable algorithm.
    - `enc` - encryption: Algorithm used to encrypt the content and protected header. Currently, A128CBC_HS256 is an acceptable algorithm.
- **JWE Encrypted Key**: A random value known as the Content Encryption Key (CEK). It is used to encrypt the JSON value and create the JWE Cipher Text. The Content Encryption Key is RSA encrypted and then encoded. For requests, the public key is used to encrypt the key. For responses, the private key for your Service or Organization is used to decrypt this value.
- **JWE Initialization Vector**: A random value to use as the initialization vector. It will be used encrypt the JSON value and create the JWE Cipher Text. The initialization vector is base64url encoded.
- **JWE Cipher Text**: A block of Encrypted and encoded content. The data is encrypted with the algorithm specified in the header with the Content Encryption Key and Initialization Vector.

eftpos Payments Australia Limited ABN 37 136 180 366
Head Office Level 11, 45 Clarence Street, Sydney NSW 2000 I GPO Box 126, Sydney NSW 2001
Telephone +61 2 8270 1800 I Facsimile +61 2 9299 2885 I Email: info@eftposaustralia.com.au
www.eftposaustralia.com.au

- **JWE Authentication Tag**: The encrypted and encoded content of the JWE Protected Header. The data is encrypted with the algorithm specified in the header with the Content Encryption Key and Initialization Vector.

For more details about the JWE standard, please refer to the Internet Engineering Task Force RFC7516 document (ISSN: 2070-1721).

eftpos Payments Australia Limited ABN 37 136 180 366
Head Office Level 11, 45 Clarence Street, Sydney NSW 2000 I GPO Box 126, Sydney NSW 2001
Telephone +61 2 8270 1800 I Facsimile +61 2 9299 2885 I Email: info@eftposaustralia.com.au
www.eftposaustralia.com.au