API FOR CORPORATE SERVICES

IMPLEMENTATION GUIDELINE

BNP PARIBAS

The bank for a changing world

Contents

API FOR CORPORATE - IMPLEMENTATION GUIDE

1. INTRODUCTION

The purpose of this document is to describe a step-by-step implementation guideline for new API for Corporate clients.

All the CMCCs APIs are exposed as a product named "API4C" and combine Payment services (Instant SCT, SCT, INTL payments, ...) and Reporting services (compliant with Swift specifications).

BNP PARIBAS provides its customer with a pair of dedicated environments: test/qualification for the integration and testing of the APIs and a Live environment for production.

2. ONBOARDING ON THE TEST/QUALIFICATION ENVIRONMENT:

2.1. PREREQUISITE CUSTOMER INFORMATION

For the onboarding on the qualification environment, please provide the following information to the BNP Paribas implementation team to populate the appendices of the Direct Connectivity Agreement (DCA)

- Name and address of the company
- BNPP client reference: RMPM/SGI
- Your account(s)
- Services required (SCT INST, SCT, reachability, reporting, etc…)
- Signatories and limits/threshold (only for Payments)
- Trusted client contact: name, email, phone number, position in the company.

NB: For the qualification onboarding, the DCA doesn't have to be signed.

2.2. SFS SPACE CREATION

In order to make sensitive information available to you, a secure sharing space will be created by the implementation team and an associated access granted to the person who will act as the customer representative/ point of contact (as provided in the DCA appendices, Schedule 3).

You will have a private directory on SFS to exchange files and sensitive data with the Implementation Team.

The subscription process to SFS will trigger the sending of an automatic email to your point of contact. The email will contain the login name and a link to set up a password. The subscription will be completed after the password has been set.

Connection to the secured sharing is a two-step process:

- The user (customer representative/point of contact) will be asked to type in the login and password
- The user will then need to enter the one-time authentication code received by SMS on the mobile phone (as indicated in the DCA appendices, Schedule 3)

To access SFS: https://securesharing.bnpparibas.com/pfv2/ws/sfs-itg

Mandatory information for the creation of SFS sharing space are the last name, first name, email address and phone number of the person in charge together with the name of the customer. (data to be provided in the DCA Schedule 3)

2.3. SSL CERTIFICATE

To use the APIs, an SSL certificate is required to access the BNP Paribas infrastructure (API gateway) for all the environments (Qualification and Production).

With a validity of at least one year, you can find below certification authorities (CA) currently accepted by BNP Paribas:

Certification Owner	Issuer
CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
CN=DigiCert SHA2 Assured ID CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1	CN=DigiCert Global Root G2
CN = DigiCert SHA2 Extended Validation Server CA	CN = DigiCert High Assurance EV Root CA
CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
CN=Entrust Certification Authority - L1K, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US	CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US
CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3
CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3
CN=Sectigo RSA Client Authentication and Secure Email CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US
CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US

CN = Sectigo RSA Organization Validation Secure Server CA	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US
CN=TBS X509 CA persona 2, OU=TBS INTERNET CA, O=TBS INTERNET, L=Caen, ST=Calvados, C=FR	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US
CN=SSL.com RSA SSL subCA, O=SSL Corporation, L=Houston, ST=Texas, C=US	CN=SSL.com Root Certification Authority RSA, O=SSL Corporation, L=Houston, ST=Texas, C=US
CN=Certinomis Corporate G4, OU=AC Intermediaire - Subsidiary CA, O=CertiNomis, C=FR	CN=CertiNomis, OU=AC Racine - Root CA, O=CertiNomis, C=FR
CN = QuoVadis Global SSL ICA G3, O = QuoVadis Limited, C = BM	CN = QuoVadis Root CA 2 G3, O = QuoVadis Limited, C = BM
CN = USERTrust RSA Certification Authority, O = The USERTRUST Network, L = Jersey City, S = New Jersey, C = US	CN = USERTrust RSA Certification Authority, O = The USERTRUST Network, L = Jersey City, S = New Jersey, C = US
CN = DigiCert Assured ID Root CA G2	CN = DigiCert Assured ID Client CA G2
CN = Certinomis - Corporate CA G5	CN = Certinomis - Root CA G4

Please note that other certificate authorities could be accepted, but BNP Paribas would need to validate that it is aligned with its security norms and would need to onboard it.

The Client SSL certificate must be transmitted encoded in base 64 to the BNP Paribas Implementation team.

To obtain the base 64 certificate, you should:

1. Call the following service **using the SSL certificate**:
   - https://api.staging.cashmanagement.bnpparibas/utilities/testcert
   - The following Curl command can be used to call the URL:

     curl --location -X GET \
     https://api.staging.cashmanagement.bnpparibas/utilities/testcert \

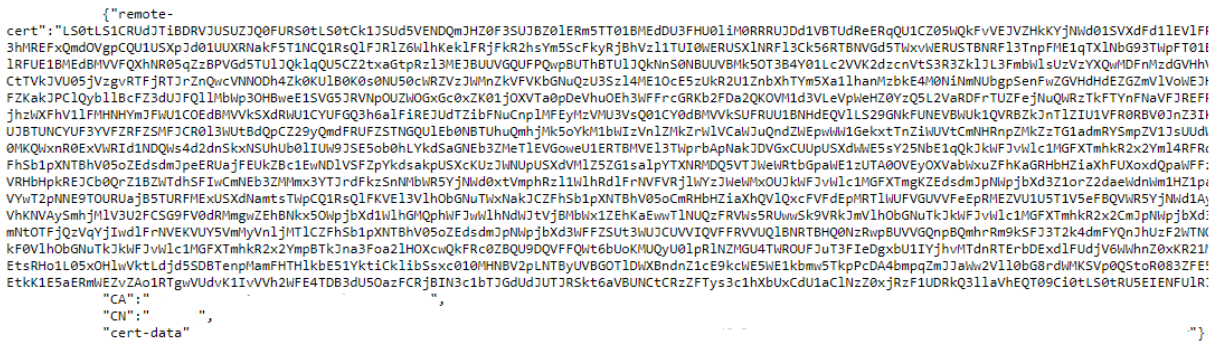
     --cert 'PATH_CRT_FILE:PASSPHRASE' \

     --key 'PATH_KEY_FILE'

2. The result of this call will contain the base64 certificate to be transmitted and will also confirm that the CA issuing the certificate is well recognized by the BNPP API gateway.

   To do so, you can copy/paste the TestCert result in a ".txt" file and upload it in your BNPP SFS dedicated Space.

Screen of a correct TestCert result:



Notes:

- *The procedure will be the same for an onboarding in Production. (Same URL to be used) It will be necessary to specify to the Implementation team if the SSL certificate will be the same for both environments: Qualification and Production.*

- *For SSL Certificate renewal, you will have to make a token API call with your new SSL certificate. If the call is OK, nothing is expected. If the token call fails, the client will have to provide the testcert result to BNP Paribas.*

2.4. SIGNATURE CERTIFICATE (ONLY FOR PAYMENT)

To fulfil its obligation to comply with the European regulation and the market best practice, BNP Paribas relies on an **Electronic Signature mechanism for payment request validation/authorization**.

BNP Paribas requires the payment request sent through the API to be **signed** with an electronic signature (ES) certificate.

The Electronic Signature joined to the payment request is verified and the Signatory is identified through the public key of the certificate/key ID stored in the bank contract repository. The ES grants for:

- Authentication of the signatory (ies)
- Data integrity
- Nonrepudiation

As from DCA contract appendix Schedule 5, the ES certificate will be linked with either the owner of the certificate (acting as a corporate representative) or any other legal corporate representative (with appropriate rights on the corporate account).

Please refer to the technical specification for the format of the ES.

2.4.1. eIDAS/RGS*/RGS**/ Swift 3Skey Electronic Signature

The bank requires an advanced Electronic Signature; all eIDAS/RGS*/RGS** (ES) certificates or Swift 3Skey are compatible with this level of Electronic Signature.

This certificate may be issued by one of the below certifications authorities already recognized by BNP Paribas:

- Swift (3Skey) available thru BNPP
- CertEurope
- GlobalSign
- CertiNomis
- Chambersign
- Certigna

You will need to provide **the Public Key of its Electronic Signature Certificate** to BNP Paribas, preferably in a ".cer" format.

You can use your SFS space to share your public key.

Please note: the maximum accepted length of the private key of the ES certificate is 4096 bits.

2.4.2. Self-Signed Electronic Signature

Only in the qualification environment, a Self-Signed Signature certificate can be accepted. This will allow **you to start API testing while the eIDAS/RGS*/RGS** signature certificate purchase is ongoing.**

You will need to provide **the Public Key of its Signature Certificate** to BNPP, preferably in a ".cer" format.

You can use your SFS space to share your public key using the "qualification" directory.

A guide to create a self-signed certificate can be found here.

NB: we recommend at least 1 year validity for the self-signed Signature certificate to avoid several updates during the testing phase.

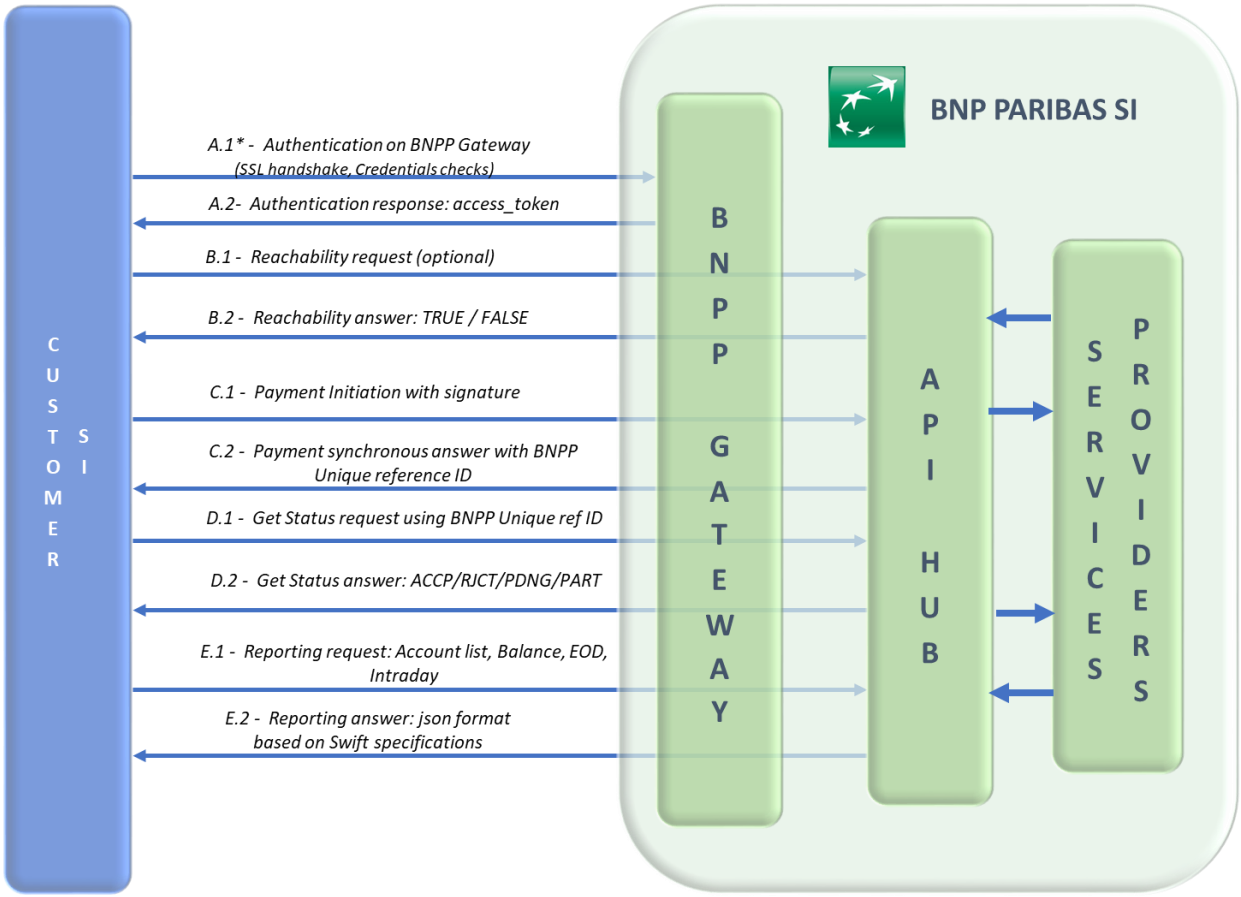
2.5. BNP PARIBAS QUALIFICATION SETUP

Once all the steps 2.1 to 2.4 are completed, BNP Paribas implementation team will set up the testing environment for you. The information below will be exchanged with you using your SFS space:

- Customer Credentials:
  - Client ID: login on BNPP Paribas Gateway
  - Client Secret: Password of the Client ID

- KeyID*: The keyID is a unique identifier that indicates the ES certificate used when signing the payment request and thus identifying the signatory. (*Only for Payments)

2.6. GLOBAL OVERVIEW



**Authentication step, mandatory before accessing all APIs*

2.7. TESTING CHECKLIST

Once you have been setup in qualification, you can start the End-to-End testing.

BNP Paribas requires the following steps to be validated in qualification environment before any production onboarding

2.7.1. BNPP Gateway Authentication for all APIs

For all the API proposed by BNPP, you need to make an Authentication on the BNPP Gateway:

- Call the authentication URL using your SSL Certificate (A.X steps)
- Pass your ClientID and Client Secret, that will return an Access token as part of the json response, inside the field "access_token".
- With this access token, you are now allowed to access BNPP API.

Screen of the Token's answer:

```
{
"access_token": "dDXO25108wjZNEiJivXcEI897LYt",
"token_type": "Bearer",
"expires_in": "899"
}
```

Expected behavior:

- You can ask for a token only when using an API.
- The same token is used for 15 minutes.

2.7.2. Reachability testing checklist

Context / Scope: this API can be used before an SCT Inst payment initiation to check the availability of the beneficiary bank. Please also note that this API is optional.

You can share upfront with the implementation team a sample of your JSON reachability Request for validation.

Testing scenario to be completed:

- E2E test Reachability answer true
- E2E Test Reachability answer false

2.7.3. Payment Testing checklist

- Electronic Signature implementation for payment: part of the testing cycle, uses and format of the Electronic Signature should be validated.

- Payment initiation API: You will need to provide to BNP Paribas implementation team a sample of the JSON used for payment Initiation. BNP Paribas Implementation team will check that the JSON is properly populated. (mandatory fields present, no empty fields…)

- Get status: after a Payment initiation, You will need to call the status URL with the BNPP Channel reference in order to get the final status of the payment transaction.

Testing scenario to be completed:

- E2E Happy cases: Initiate a Payment which is Settled on the testing environment and recovers the final status "ACCP".
- E2E Rejected Case: Initiate a payment which is Rejected on the testing environment and recovers the final status "RJCT". The following Creditor IBAN can be used:

Creditor IBAN	Creditor BIC	Result	Error code
FR7630438001001111111111120	INGBFR21XXX	RJCT	CNOR
FR7630004013280001111111157	BNPAFRPPXXX	RJCT	AC01 Incorrect ACCOUNT

a. The following process is expected for Standard Payments Get Status:

After the Synchronous answer, wait at least 4 minutes before the first Get status call, using the channel Reference (NWC**).

- If the answer of the first Call is RJCT, then no more get status are required.
- If the answer of the first call is PDNG and that the requested execution is equal to request reception date:

File reception	Cut off	Get Status 2nd call
Monday - Friday	D From 6 AM to 3 PM	D + 5 hours
Monday - Friday	D After 3 PM	D+1 (business day) from 11 AM
Saturday - Sunday	/	Monday from 11 AM

*D= Payment reception DAY

b. The following process is expected for SCT INST transaction.

After the Synchronous answer, you need to wait at least 10 seconds before the first Get status call, using the channel Reference (NWC**). 3 Status are possible:

- ACCP: Final Status, the payment is settled
- RJCT: Final Status, the payment has been rejected.
- PDNG: intermediary status. The SCT INST payment has been received and the process is ongoing. Usually*, this means that the get status has been done too early, we ask to wait 10 seconds after the payment reception by BNPP.

*After 10 seconds, you can retrieve a final status (ACCP or RJCT) in 99.8% of cases.

However, in exceptional cases a SCT INST transaction can remain in a PDNG status after 10 seconds. You should therefore set up a specific retry process to retrieve the status of those transaction. We suggest the following process:

*The process is only valid if the SCT INST Payment reception has been confirmed by BNPP / the client has received the BNPP channel reference NWC***

+ 10 seconds = first get status call. If a final status (ACCP or RJCT) is retrieved, break process else
+ 20 seconds after first get status call. If final status retrieved, break process else
+ 40 seconds after second status call. If final status retrieved, break process else

+ 80 seconds after third status call. If final status retrieved, break process else
+ 160 seconds after fourth status call. Break process.

After these 5 get status calls, it is best not to pursue the process with other get attempts as it is verry likely a case of an unexpected error that would require manual investigation from BNPP teams to retrieve the final status of the transaction.

For those cases where the final status of a transaction could only be retrieved after an investigation of BNPP teams, we recommend completing the set up with a second process enabling the client to retrieve a specific transaction status -that has been updated on BNPP side- on the following days of the payment.

2.7.4. Reporting Checklist

For reporting, following data can be used for testing

Accounts	BIC	Cur.	Statements available	Intraday
FR7630004123459876543219870	BNPAFRPPXXX	EUR	22/03/23-25/03/23	23/03/23-26/03/23
FR7630004123450009998887704	BNPAFRPPXXX	EUR	20/03/23-25/03/23	23/03/23-26/03/23
DE70370106000123456789	BNPADEFFVAM	USD	22/03/23-25/03/23	23/03/23-26/03/23
BE18001987654323EUR	GEBABEBB36A	EUR	22/03/23-25/03/23	23/03/23-26/03/23

2.8. MOCK MODE FOR SCT INSTANT PAYMENT

This Mock mode has been developed in order to get specific values in the get status response. This mode is only available for SCT INSTANT Payment scope.

NB: E2E tests described in 2.7.3 remain mandatory before any production onboarding.

The following specific values will have to be populated by the client in his payment initiation JSON:

Step 1: Make a token request as described in point 2.7.1

Step 2: Make an instant payment request with:

- Debtor IBAN: **FR7630004013280001987654373**
- Debtor BIC: **BNPAFRP0XXX**
- Creditor IBAN: **FR7630004123459876543219870**
- Creditor Name according to the expected result:

Expected status in Get Status Response	Creditor name setting in Payment Initiation
ACCP (Accepted transaction)	"creditor": { "name": "ACCP-NULL" },
PDNG (Pending transaction)	"creditor": { "name": "PDNG-NULL" },
RJCT - Rejected transaction for cause XXXX (replace XXXX by existing ISO status error code)	"creditor": { "name": "RJCT-XXXX" },

3. PRODUCTION ONBOARDING

3.1. PREREQUISITE

The following steps are mandatory before any production onboarding on the API Channel:

- All the Qualification onboarding steps have been validated by the client with the BNP Implementation Team.
- Contract and DCA are signed by the client.
- Contract has been validated and set up on production environment was completed by BNPP Back-office team.

3.2. PRODUCTION CERTIFICATES

The client would need to provide the **production certificates** to BNPP using the **SFS Space**:

- SSL Production certificate (please refer to the process explained on 2.3)
- Production Signature Certificate: the public key must be provided to BNPP.

3.3. PRODUCTION CREDENTIALS

Once the client onboarding is completed on the production environment, BNP Paribas will provide the following elements to the client:

- **Client Id**: login on BNPP Paribas gateway
- **Client Secret**: password matching the Client Id. The file containing the Client Secret will be encrypted on the SFS Space. The password will be communicated to **the "Participating user" contact** provided in the DCAs appendixes (schedule 3) via another communication channel and preferably SMS.
- **KeyID***: The keyID is a unique identifier that indicates the ES certificate used when signing the payment request and thus identify the signatory. (*Only for Payment). This id will be shared to the client using his SFS space.

3.4. PENNY TEST / GO LIVE

Before the commercial Go live on Client side, BNPP recommends to perform a few penny tests in production with low transaction's amounts. These Penny tests will have to be schedule with the client and the implementation team for close monitoring.

Once the penny tests are validated, the client can begin his commercial Go Live.

4. APPENDIXES

2.4.2 creation of a self-signed certificate

```
1) Creation of the private key:
openssl genrsa -out CERT_ABO_PRIVATE.key 2048

2) Generation of the CSR (Certificate Signing Request) :
openssl req -new -key CERT_ABO_PRIVATE.key -out CSR_ABO.csr

$ openssl req -new -key CERT_ABO_PRIVATE.key -out CSR_ABO.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:Paris
Locality Name (eg, city) [Default City]:Paris
Organization Name (eg, company) [Default Company Ltd]:BNPP
Organizational Unit Name (eg, section) []:BNPP
Common Name (eg, your name or your server's hostname) []:CSR_ABO
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:test
An optional company name []:



3) Self signed certificate for a period validity of 1j
openssl x509 -req -days 1 -in CSR_ABO.csr -signkey CERT_ABO_PRIVATE.key -out
CRT_ABO.crt
```

N.B.: replace BNPP and ABO by the name of the client