# Dynamic Client Registration (DCR) using eIDAS certificates

Vanquis Bank – Open Banking

Gurdeep Singh
VANQUIS BANK

# Change log

| Date | Remarks/Change description | Author |
|------|---------------------------|--------|
| 6th April 2020 | Initial version | Gurdeep Singh |
| | | |
| | | |

**DCR with Vanquis bank using eIDAS**

Third Party Providers (TPPs) must first be registered with the Financial Conduct Authority (FCA) or National Competent Authority (NCA) of your host country.

TPPs can either use eIDAS issued by QTSP or be enrolled with the Open Banking Directory and use OB issued certificates. We cannot accept any applications from TPPs who do not meet these requirements.

**Note** – TPPs using Open Banking issued certificates (OB Transport/Signing or OBWAC/OBSeal) should follow the guidelines at implementation guide at link below.

https://openbanking.atlassian.net/wiki/spaces/AD/pages/998638840/Implementation+Guide+Vanquis+Bank

This document is only intended for TPPs who are not registered with Open Banking U.K. and wish to onboard with Vanquis Bank directly using eIDAS certificates issued by a QTSP.

**DCR using eIDAS Step by Step**

1. TPP establish MTLS connection with Vanquis Servers using QWAC certificate issued by a QTSP.
2. TPP send's registration data in the form of JWT token signed by TPP's QSEAL Private Key. (NO SSA required)
3. We expect Payload of JWT token contain in the structure explained in Table 1.0 in the document below.
4. TPP must send QSEAL public key in request header with name "**X-OB-SigningCert**" and in the form of **Base64UrlEncoded** format. This is only required for DCR end point.
5. We Verify JWT and registration data and issue client id. This client is not authorised to access the data automatically. This is subject to the manual approval of Vanquis OB team. Clients can try make requests to data to check if the approval is granted or confirm their status by email to openbankingsupport@vanquisbank.co.uk
6. We currently do not support eIDAS in Sandbox environment. - ??
7. In case TPP's public key is changed they must send us the new public key via email us to openbankingsupport@vanquisbank.co.uk. We will then update our records and send you the confirmation once done.

**Table 1.0**

| Field | Data Type | Mandatory | Source | Additional Info | Location (Request/Response) |
|---|---|---|---|---|---|
| org_id | strig | Yes | JWT | Must match Organisation Identifier from certificate | Both |
| software_clie nt_id | string | Yes | JWT | Must match Organisation Identifier from certificate | Both |
| software_redi rect_uris | array of strings | Yes | JWT | Must match SAN(subject alternative names) from transport certificate | Both |
| software_clie nt_uri | string | No | JWT | | Both |
| software_log o_uri | string | No | JWT | | Both |
| grant_types | array of strings | No | JWT | if provided must be authorization _code, client_crede ntials, refresh_token | Both |
| response_typ es | array of strings | No | JWT | If provided must be "code id_token" | Both |
| application_t ype | string | No | JWT | if supplied it must be Web or Mobile, if | Both |

| Field | Data Type | Mandatory | Source | Additional Info | Location (Request/Response) |
|---|---|---|---|---|---|
| | | | | not defaults to Web | |
| scope | array of strings | Yes | JWT | Must match NCA role for ASPSP(accounts, payments), AISP(accounts),PISP(payments), CBPII(fundsconfirmations) we validate these values againest nca roles specified in transport certificate(QWAC) | Both |
| software_environment | string | Yes | JWT | "Sandbox" for test environments and "Production" for production environments | Request |
| software_mode | string | Yes | JWT | "Test" for test environments and "Live" for production environments | Request |
| aud | string | Yes | JWT | Vanquis PSD2 organisation identifier | Request |
| Iss | string | Yes | JWT | TPP PSD2 organisation identifier | Both |

| Field | Data Type | Mandatory | Source | Additional Info | Location (Request/Response) |
|---|---|---|---|---|---|
| iat | string | Yes | JWT | issued time in UNIX format | Both |
| exp | string | Yes | JWT | expiration time in UNIX format | Both |
| Software_statement | JWT | No | JWT | Only returned in response signed by Vanquis | Response |

## Sample cURL

```
curl --location --request POST
'https://mtls.auth.openbanking.vanquis.co.uk/connect/register' \
--header 'Content-Type: application/jwt' \
--header 'Upgrade-Insecure-Requests: 1' \
--header 'Accept: charset=utf-32' \
--header 'X-OB-SigningCert: xxxx \
--header 'Content-Type: text/plain' \
--data-raw xxxx
```

**Sample Request Jwt converted into Json format for illustration**

```
{
  "org_id": "xx",
  "software_client_id": "xx",
  "software_redirect_uris": [
    "xx"
  ],
  "software_client_uri": "xx",
  "software_logo_uri": "xx",
  "grant_types": [
    "authorization_code",
    "client_credentials",
    "refresh_token"
  ],
  "response_types": [
    "code id_token"
  ],
  "application_type": "Web",
  "scope": [
    "accounts",
    "payments",
    "fundsconfirmations"
  ],
  "software_environment": "sandbox",
  "software_mode": "test",
  "iss": "xx",
  "aud": "xx",
  "iat": 1586125555,
  "exp": 1586126155
}
```

**Sample Response Jwt converted into Json format for illustration**

```json
{
    "client_id": "xxx",
    "client_name": "xxx",
    "client_id_issued_at": "1586174875",
    "redirect_uris": [
        "xxx"
    ],
    "token_endpoint_auth_method": "private_key_jwt",
    "grant_types": [
        "client_credentials",
        "hybrid",
        "refresh_token"
    ],
    "response_types": [
        "code id_token"
    ],
    "software_id": "xx",
    "scope": "openid offline_access accounts payments fundsconfirmations",
    "software_statement": "xxx",
    "application_type": "Web",
    "id_token_signed_response_alg": "PS256",
    "request_object_signing_alg": "PS256",
    "token_endpoint_auth_signing_alg": "PS256"
}
```

**Sample Software statement within Response Jwt converted into Json format for illustration**

```json
{
  "iss": "xxxx",
  "iat": 1586174875,
  "exp": 0,
  "jti": null,
  "software_environment": null,
  "software_mode": null,
  "software_id": "xxxx",
  "software_client_id": "xxxx",
  "software_client_name": "xxxx",
  "software_client_description": null,
  "software_version": null,
  "software_client_uri": "xxxx",
  "software_redirect_uris": [
    "xxxx"
  ],
  "software_roles": ["xxxx"],
  "organisation_competent_authority_claims": {
    "authority_id": "xxxx",
    "registration_id": "xxxx",
    "status": "Active",
    "authorisations": [
      {
        "member_state": "xxxx",
        "roles": [ "xxxx"  ]
      }
    ]
  },
  "software_logo_uri": "xxxx",
  "org_status": null,
  "org_id": "xxxx",
  "org_name": "xxxx",
  "org_contacts": null,
  "org_jwks_endpoint": null,
  "org_jwks_revoked_endpoint": null,
  "software_jwks_endpoint": null,
  "software_jwks_revoked_endpoint": null,
  "software_policy_uri": null,
  "software_tos_uri": null,
  "software_on_behalf_of_org": null,
  "ob_registry_tos": null
}
```

**FAQs**

TBA

**Further support**

Any question or further queries must be made to
openbankingsupport@vanquisbank.co.uk