

Onboarding of new network participant - buyerApp or sellerApp

POST

/ondc/verifyParticipant/verifyD/init Generate Verification and Ack Code for Website Ownership Verification

POST

/ondc/verifyParticipant/verifyD/verify Initiate Verification of the website

POST

/ondc/verifyParticipant/verifyK/init Verify signing key of Network Participant that will be used for Signing

Network Participant System URL/Domain

Registry

```
{
  "confReqID": "d290flee-6c54-4b01-90e6-d701748f0851",
  "subscriber_id": "https://sit.grab.in/ondc",
  "subscriber_url": "https://sit.grab.in/ondc/bpp/",
  "city": "std:080",
  "valid_from": "2022-04-05T05:56:52.470618Z",
  "valid_until": "2026-04-05T05:56:52.470618Z",
  "domain": "nic2004:52110",
  "type": "sellerApp",
  "signing_public_key": "QSax2KT4UiTU.....",
  "encr_public_key": "O74ukMymk4KZ.....",
  "callback_url": "QSax2KT4UiTUWU.....",
  "timeStamp": "2016-08-29T09:12:33.001Z"
}
```

```
<html><head><meta
name='ondc-site-
verification'
content='REPLACE WITH Dinit_
ACK_CODE_VALUE' /></head>
<body>ONDC Site Verification
Page </body> </html>
```

Create "ondc-site-verification.html" at URL and copy paste below content. Its important to have a public access to this file for verification.

```
{
  "status": "success",
  "message": {
    "ackCode": "44006271-f8aa-....",
    "details": "create meta tag with the
ackCode(DinitAckCode)"
  }
}
```

```
{
  "verReqID": "d290flee-6c54...",
  "confReqID": "d290flee-6c54...",
  "dInitAckCode": "44006271-f8..."
}
```

keyVerReqID : unique transaction ID. Can be used to trace.
dVerifyAckCode: Success ACK Code issued after successful verification of domain
Signature: signature of successful verification ack code (dVerifyAckCode) of domain using Network Participant's signing private key
encMessage: Encrypted successful verification ack code (dVerifyAckCode) of domain that has been signed using Network Participant's encryption private key

```
{
  "keyVerReqID": "d290flee-...",
  "dVerifyAckCode": "e300f1...",
  "signature": "SDSDSDS...",
  "encMessage": "SDSDSDS..."
}
```

```
{
  "status": "success",
  "message": {
    "ackCode": "44006271-...",
    "details": "Domain Verified. Please save
ackCode(DverifyAckCode) for verification of keys"
  }
}
```

```
{
  "status": "success",
  "message": {
    "ackCode": "44006271-...",
    "details": "Signing Verified. "
  }
}
```

Validate Schema, OSCP Validation, Mark Subscriber ID as "Under Domain Verification", And Generate ACK Code

Match verification

Get Enc and Sig Public keys configured against **dVerifyAckCode** and check if it matches with keymatches if yes issue an Ack

Key rotation of network participant - buyerApp or sellerApp

POST **/ondc/verifyParticipant/verifyK/init** Verify signing key of Network Participant that will be used for Signing

POST **/ondc/subscribe** The network participant will trigger the subscribe call to the registry to register its public keys.

POST **/networkParticipant/on_subscribe** verify network participants encryption key. To be hosted by network participant

POST **/ondc/lookup** Get public keys of network participants

Network Participant System URL/Domain

Registry

```
{
  "reqID": "44006271-f8aa-4540-a57e-7a045282e4b4",
  "subscriber_id": "https://sit.grab.in/ondc",
  "country": "IND",
  "city": "std:080",
  "domain": "nic2004:52110",
  "signing_public_key": "QSax2KT4UiTUWUqoVUaE...",
  "encr_public_key": "O74ukMymk4KZnVs3sZhU2...",
  "valid_from": "2022-04-05T05:56:52.470618Z",
  "valid_until": "2026-04-05T05:56:52.470618Z",
  "nonce": "test-random-nounce",
  "previous_req_id": "2026-04-05T05:56:52.470618Z",
  "signature": "tDUVbfpJCxwKP4rEaJMjHGhIXk5hq..."
}
```

1

POST
/ondc/subscribe

```
{
  "status": "INITIATED"
}
```

3

2

Fetch Public Key configured for previous requested ID and verify the signature

```
{
  "answer": "decrypted_challenge_string"
}
```

5

POST
/networkParticipant/on_subscribe

```
{
  "subscriber_id": "ondc.org",
  "challenge": "encrypted_challenge_string"
}
```

4

4

6

Match Challenge and Answer, if successful then mark subscriber as "SUBSCRIBED"

```
{
  "keyVerReqID": "d290f1ee-...",
  "dVerifyAckCode": "e300f1...",
  "signature": "SDSDSDS...",
  "encMessage": "SDSDSDS..."
}
```

7

POST
/ondc/verifyParticipant/verifyK/init

```
{
  "status": "success",
  "message": {
    "ackCode": "44006271-...",
    "details": "Signing Verified. "
  }
}
```

7

8

8

Get Enc and Sig Public keys configured against **dVerifyAckCode** and check if signature can be verified and whether encmessage can be decrypted ; if yes, issue an Ack