Business Certificate Publisher Interface Documentation, v1

Table of contents

About

This document describes version 1 («v1») of the Business Certificate Publisher (BCP) interface. This document does not describe internal workings of an implementation of BCP.

Introduction to BCP

The BCP service provides a standardized lookup interface to retrieve the qualified certificate for use in end to end encryption of business communication (b2b, g2b, b2g and g2g), known in the four-corner model (link) as corner 1 and 4. BCP provides clear separation of concern between the communicating parties and BCP's function of maintenance, distribution and security clearing of certificates. Each participant is responsible to provide the qualified certificate they preferred used when receiving encrypted messages.

Versioning

This document describes version 1 of the API for lookup. This API uses "v1" as identifier. This is to allow upgrading to newer API versions when needed.

Definitions

Participant Identifier (PPID)

Participant Identifier in BCP reuses the PEPPOL Participant Identifier (PPID) defined by OpenPEPPOL. PPID is defined as a qualified identifier based upon ISO 6523. PPID expressed in BCP uses double colon ("::") as separator.

Example of a Norwegian organization:

> Qualifier: iso6523-actorid-upis
> Identifier: 9908:910076787
> Combined: iso6523-actorid-upis::9908:910076787

Process Identifier (PID)

Process Identifier (PID) in BCP reuses the Process Identifier defined by OpenPEPPOL/CEN BII. PID is defined as a qualified identifier. PPID expressed in BCP uses double colon ("::") as separator.

Example of invoicing process identifier:

> Qualifier: busdox-procid-ubl
> Identifier: urn:www.cenbii.eu:profile:bii01:ver2.0
> Combined: busdox-procid-ubl::urn:www.cenbii.eu:profile:bii01:ver2.0

Role

Role is introduced in BCP to allow organizations to provide different certificates based upon the role they play in complex processes consisting of responses back to initiator of the process.

BCP is currently limited to processes containing maximum two participants, where processes containing more than two participants should be divided into narrower processes.

Role is applied to a process by defining the direction of the first message (sent by initiator) as a REQUEST message. BCP is modelled on having receivers declare capabilities. For encryption of REQUEST messages is the receiver's REQUEST certificate used for encryption in the process. When a message is returned as part of the same process is this direction defined as RESPONSE. Further uses of the same direction in the process uses the same role.

Example of Catalogue process:

> Catalogue – Sent by Economic Operator (Role: REQUEST)
> Catalogue – Sent by Contracting Authority (Role: RESPONSE)

Supported lookups

BCP is inspired by OASIS BDXR SMP, and support two requests for lookup; list of supported profiles for a given PPID and certificates for a combination of PPID, PID and UC.

General

Lookups are performed in the context of the BCP service. In the case of BCP not running as root application for the hostname is URL paths defined by BCP to be applied to the BCP context.

Example 1:

> URL path: /api/v1/[PID]
> BCP context: http://bcp.example.com/
> Request URL: http://bcp.example.com/api/v1/[PID]

Example 2:

> URL path: /api/v1/[PID]
> BCP context: http://example.com/bcp/
> Request URL: http://example.com/bcp/api/v1/[PID]

PPID and PID must be URL encoded when replacing value holders in this document. Service implementations are free to support non-encoded values; however, client implementations must implement with encoding of values. Any other parts of the URL are not subject to encoding.

Example 3:

> Qualifier: iso6523-actorid-upis
> Identifier: 9908:910076787
> Encoded: iso6523-actorid-upis%3A%3A9908%3A910076787

Clients is expected to handle HTTP codes per the list below.

HTTP Code	Description
200	Content available.
3xx	Not in use
404	No content found for the lookup.
5xx	Error in the service, try again later.

It is recommended to provide BCP using HTTPS. BCP services may use the included XML Signature (XMLDsig) for integrity in cases where HTTPS is not used or where such use is specified within domain.

Lookup: Supported profile identifiers

URL path	/api/v1/[PPID]
Supported methods	GET
Response element	Participant

This request is performed for a given PPID, and may be used when performing discovery.

Example response:


```
<Participant xmlns="urn:fdc:difi.no:2017:virksert:v1" xmlns:ns2="http://www.w3.org/2000/09/xmldsig#"><ParticipantIdentifier scheme="iso6523-actorid-upis">9908:910076787</ParticipantIdentifier><ProcessReference scheme="busdox-procid-ubl">urn:www.cenbii.eu:profile:bii01:ver2.0</ProcessReference><ProcessReference scheme="busdox-procid-ubl">urn:www.cenbii.eu:profile:bii03:ver2.0</ProcessReference><ProcessReference scheme="busdox-procid-ubl">urn:www.cenbii.eu:profile:bii04:ver2.0</ProcessReference><ProcessReference scheme="busdox-procid-ubl">urn:www.cenbii.eu:profile:bii05:ver2.0</ProcessReference><ProcessReference scheme="busdox-procid-ubl">urn:www.cenbii.eu:profile:bii28:ver2.0</ProcessReference><ProcessReference scheme="busdox-procid-ubl">urn:www.cenbii.eu:profile:bii30:ver2.0</ProcessReference><ProcessReference scheme="busdox-procid-ubl">urn:www.cenbii.eu:profile:biixx:ver2.0</ProcessReference></Participant>
```


Lookup: Specific profile identifiers and usage scopes

URL path	/api/v1/[PPID]/[PID] (Returns Role=REQUEST) /api/v1/[PPID]/[PID]/[Role]

Supported methods	GET
Response element	Process

This request is performed for a combination of PPID, PID and role to fetch encryption certificates.

Example response (self-signed certificate):


```
<Process xmlns="urn:fdc:difi.no:2017:virksert:v1" xmlns:ns2="http://www.w3.org/2000/09/xmldsig#"><ParticipantIdentifier scheme="iso6523-actorid-upis">9908:910076787</ParticipantIdentifier><ProcessIdentifier scheme="busdox-procid-ubl">urn:www.cenbii.eu:profile:bii01:ver2.0</ProcessIdentifier><Certificate serialNumber="1498123485" expire="1498209918000">MIICuDCCAaCgAwIBAgIEWUuM3TANBgkqhkiG9w0BAQsFADAeMRwwGgYDVQQDDBNFeGFtcGxlIGNlcnRpZmljYXRlMB4XDTE3MDYyMjA5MjUxOFoXDTE3MDYyMzA5MjUxOFowHjEcMBoGA1UEAwwTRXhhbXBsZSBjZXJ0aWZpY2F0ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALboRbrjJIs5aRWTCd23/EO42sn3hbV4/zR56yUuOeCHBKmB8PTnQnNNNi4j7qVMdIrs/eBZU+eVkHGs+beeBh7B9Sm2AQHYqv5FOPEOJs+YBxLu9pGcSDvZwdh0h32K3DHuEWXEuNSQmhJ1+xfLWy+mmR711SNBYls0pE+9PL/qlkmQLJxaTkhCvOjDqv/Xj6FeliKmGiHGBAv4o8hn0VEl9yKQoxCjTPfhFintfpb13pKftKDZvSr04uZERIfcmg/IWbNzFBRffy/xkZWWs1FJ9nqaWKMeqiKK+pvJGjquVDsKKGvOBPPCP3s/PNdqpn9R114rd4MKEQVqX1rlgFkCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAVb11xVQ6iosAxICR49JE+41Uz/Cz4htunKZ8DsTxxfxwJtjPn5fknLNyS6/lCnihrmgqE9VG5ENnNqpTq1ASJnVe+42O+yjvJoPv97YxoOo8Ki0Dhh1gP5dmbYXfXX+RegPpnWPxO/IEYSA/5Nw8S3VFxO4e6IHyXVgC9QN30t7aIxyn2vGPzZzyQdg+EZp0SADCMc4UBCa8XmgNpzCfgKA56VemI/iP3IDxZ4J0rEjhCxoo5ItXJiOFQpCyA9vKqtlbEQ+8ZjzreP5+rDk9XskS/Mih/1rgG/unSh2Tbl0q0L6ucBj0dDNFJDQb4z3cwVo8qNPkom3itKPurTlT1Q==</Certificate></Process>
```


BCP services must perform validation of each certificate at some interval (i.e. 48 hours), meaning certificates received upon lookup is not checked on-the-fly by BCP and is subject to validation by clients before use.

All clients fetching certificates must validate certificates received. In a case where multiple certificates are received may any valid certificate be used. Validation of certificates must be per the chain and rules agreed upon within the domain (i.e. Norwegian Business Certificates).

In a situation where all returned certificates fail validation is the lookup application expected to handle this as if the service returned 404 rather than 200.

Caching services may be used per these rules:

- Use of caching limits must be agreed upon within the domain.
- When 5xx is returned by BCP may cached certificates be used per limits.
- When 404 or no valid certificates are received must cache purge cached certificate.

Appendixes

XSD

XSD file may be found here:
https://github.com/difi/virksert/blob/master/virksert-common/src/main/xsd/virksert-v1-1.0.xsd