BPC SMP Profile Version 1.0

January 4, 2022

Business Payments Coalition

Table of Contents

1 Version History

Revision Date	Version	Change Description	Editor Name
11/22/2021	0.9	Initial import into template	Britta Holland
1/4/2022	1.0	Incorporated feedback from IOC	Britta Holland

2 Introduction

2.1 Scope

This specification is a profile of the Service Metadata Publishing (SMP) Version 2.0 OASIS Standard (OASIS SMP 2.0) published here: https://docs.oasis-open.org/bdxr/bdx-smp/v2.0/os/bdx-smp-v2.0-os.html.

This document describes the technical and functional requirements of both SMP clients and services. In addition to the policies specified in this document, all SMP clients and services in the BPC network MUST conform to all conformance clauses of the OASIS SMP 2.0 specification.

2.2 Conformance

The keywords 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' in this specification are to be interpreted as described in RFC2119 and RFC 8174 when, and only when, they appear in all capitals, as shown here.

2.3 Terms and Definitions

For the purpose of this specification, all terms shall have the definitions defined in section 2.3 of the *E-invoice Exchange Framework – Approach to Managing a Federated Registry Services Model in a Four-Corner Network* report found here: https://businesspaymentscoalition.org/wp-content/uploads/bpc-e-delivery-network-validation-exercise-2020.pdf

2.4 Disclaimers and Copyright

Views expressed here are not necessarily those of, and should not be attributed to, any particular BPC participant or organization. They are not intended to provide business or legal advice, nor are they intended to promote or advocate a specific action, payment strategy, or product. Readers should consult with their own business and legal advisors.

This specification is the work product of the BPC, and readers are free to republish this specification in whole or in part without further permission, as long as the work is attributed to the BPC, and in no way suggests the BPC sponsors, endorses or recommends any organization or its services or products. Other product names and company names referenced within this document may be either trademarks or service marks of their

respective owners.

<Add MIT licensing statement here.>

3 REST interface

3.1 HTTP and security

SMP services MUST use HTTPS and MUST use TLS/SSL certificates in accordance with BPC network policies. SMP services MUST NOT make SMP resources available through unsecured HTTP connections.

SMP services MUST use the standard HTTPS port 443.

TLS/SSL client authentication MUST NOT be required when accessing SMP resources.

3.2 SMP REST API

Client and server REST communication MUST be implemented as specified in section 5.2 of the OASIS SMP 2.0 standard.

An SMP client SHOULD always call the ServiceGroup resource first to discover if a given service or document type is supported. In other words, an SMP client SHOULD NOT assume that a given ServiceMetadata resource exists without first performing a ServiceGroup discovery. An SMP client MUST NOT use trial and error methods for capability discovery.

3.3 Caching

SMP services

SMP services SHOULD support “If-Modified-Since” request headers as specified in RFC 7232 and SHOULD respond with an HTTP 304 (Not Modified) status code if the requested resource exists and has not been modified since the date in the “If-Modified-Since” header.

SMP services MUST respond with an HTTP 200 (OK) status code if the requested resource exists and:

has been modified since the date in the “If-Modified-Since” header, or

an “If-Modified-Since” header was not included in the request, or

the SMP service does not support “If-Modified-Since” headers.

SMP services MUST include a “Last-Modified” header with every HTTP 200 (OK) response as specified in RFC 7232.

3.4 SMP clients

SMP clients SHOULD cache responses from SMP services and SHOULD implement “If-Modified-Since” requests and responses as specified in RFC 7232 and as follows:

When an SMP resource is already cached by the SMP client, the SMP client SHOULD include a “If-Modified-Since” header in the HTTP request. For the date value of the “If-Modified-Since” header, the SMP client MAY use either a local date of when the resource was cached, or the date value returned by the SMP service for the cached resource.

If an “If-Modified-Since” header is included in a request and the SMP service responds

with an HTTP 304 (Not Modified) status code, then the SMP client MUST use its last cached resource in lieu of a resource returned by the SMP service.

4 Data model

4.1 General

SMP services and clients MUST implement the elements in the tables specified below. Other network profiles and specifications MAY identify and specify the use of additional elements and/or cardinality of elements described in the tables in the sections 4.2 and 4.3 below.

SMP services MAY implement additional SMP elements, including the use of extensions, however they MUST NOT require that an SMP client can understand them. Such elements and extensions, if any, MUST NOT conflict or contradict any use of SMP specified by the network.

4.2 ServiceGroup resource

Element or attribute	Cardinality	Definition and use
ServiceGroup	1..1	Root element of the SMP ServiceGroup resource.
└ SMPVersionID	1..1	The version of the OASIS SMP specification in use. This value MUST be set to: `2.0`
└ ParticipantID	1..1	The Participant Identifier as specified in the BPC Identifier Policy specification. SMP clients SHOULD check that the value returned by the SMP service matches the queried value.
└ ParticipantID/@schemeID	1..1	The identifier of the scheme to which the Participant Identifier belongs, as specified in the BPC Identifier Policy specification. SMP clients SHOULD check that the value returned by the SMP service matches the queried value.
└ ServiceReference	0..n	Contains information about a supported document type. The ServiceGroup resource SHALL have exactly one ServiceReference occurrence for each document type supported, i.e., it MUST NOT have two or more ServiceReference elements describing identical document types. The ServiceGroup MUST NOT include ServiceReference elements describing document types that are not supported by the end user. Each ServiceReference document type MUST have a corresponding ServiceMetadata resource available (see section 3.3).
└ └ ID	1..1	The document type identifier as specified in the corresponding business document profile or specification. When referencing a JSON document, the service reference ID MUST be formatted using the JSON Identifier scheme as specified in section 3.7.1.3 of the OASIS SMP 2.0 specification. When not referencing a JSON document, the service reference ID MUST be formatted using the QName/Subtype Identifier scheme as specified in section 3.7.1.2 of the OASIS SMP 2.0 specification.

		For both the QName/Subtype Identifier scheme and the JSON Identifier scheme goes that Subtype Identifier is REQUIRED and MUST be exactly as specified in the document type's BPC business document profile or specification.
└ └ ID/@schemeID	1..1	When using the JSON Identifier scheme, this MUST be set to exactly: bdx-docid-qns When using the QName/Subtype Identifier scheme, this MUST be set to exactly: bdx-docid-json

└ └ ID/@schemeName	0..1	When used with the JSON Identifier scheme, then the OPTIONAL scheme name MUST be set to exactly:
		`JSON Identifier`
		When used with the QName/Subtype Identifier scheme, then the OPTIONAL scheme name MUST be set to exactly:
		`QName/Subtype Identifier`

└ └ Process	0..n	A supported business process within which the document type is used. The ServiceReference container SHALL have exactly one Process occurrence for each business process supported, i.e., it MUST NOT have two or more Process elements describing identical business processes. The ServiceReference MUST NOT include Process elements describing business processes that are not supported by the end user. The value of this element is specified in the business document type documentation. It is left optional to accommodate document types that use different means to signal business process relations.
└ └ └ ID	1..1	The business process identifier as specified in the corresponding business process or business document profile or specification.

4.3 ServiceMetadata resource

Element or attribute	Cardinality	Definition and use
ServiceMetadata	1..1	Root element of the SMP ServiceMetadata resource.
└ SMPVersionID	1..1	The version of the OASIS SMP specification in use. This value MUST be set to: `2.0`
└ ID	1..1	The document type identifier as specified in the corresponding business document profile or specification. MUST be formatted using either the JSON Identifier scheme or the the QName/Subtype Identifier scheme as specified in the definition of the ServiceGroup/ServiceReference/ID in section 3.2 above. SMP clients SHOULD check that the value returned by the SMP service matches the queried value.
└ ID/@schemeID	1..1	When using the JSON Identifier scheme, this MUST be set to exactly: bdx-docid-json When using the QName/Subtype Identifier scheme, this MUST be set to exactly: bdx-docid-qns
└ ID/@schemeName	0..1	When used with the JSON Identifier scheme, then the OPTIONAL scheme name MUST be set to exactly: `JSON Identifier`

		When used with the QName/Subtype Identifier scheme, then the OPTIONAL scheme name MUST be set to exactly: QName/Subtype Identifier
└ ParticipantID	1..1	The Participant Identifier as specified in the BPC Identifier Policy specification. SMP clients SHOULD check that the value returned by the SMP service matches the queried value.
└ ParticipantID/@schemeID	1..1	The identifier of the scheme to which the Participant Identifier belongs, as specified in the BPC Identifier Policy specification. SMP clients SHOULD check that the value returned by the SMP service matches the queried value.
└ ProcessMetadata	1..1	
└ └ Process	0..n	A supported business process that the document type is part of. The ProcessMetadata container SHALL have exactly one Process occurrence for each business process supported, i.e., it MUST NOT have two or more Process elements describing identical business processes. The ProcessMetadata MUST NOT include Process elements describing business processes that are not supported by the end user. The value of this element is specified in the business document type documentation. It is left optional to accommodate document types that use different means to signal business process relations.
└ └ └ ID	1..1	The business process identifier as specified in the corresponding business process or business document profile or specification.
└ └ Endpoint	0..n	The technical endpoint of the Access Point to where business documents of this document type must be sent. The ServiceMetadata resource MUST have either one Redirect element or one or more Endpoint elements, i.e., it MUST NOT have both and it MUST NOT have none. A ServiceMetadata resource MUST only contain one activated and not expired endpoint with the same TransportProfileID.
└ └ └ TransportProfileID	1..1	The identifier for the transport profile or protocol that the endpoint will expect senders to use when sending business documents.
└ └ └ Description	0..1	An OPTIONAL human readable description of the endpoint.
└ └ └ Contact	1..1	Information for contacting the technical personnel operating the endpoint, such as an email address or a phone number.
└ └ └ AddressURI	1..1	The absolute URL where business documents of this document type shall be sent.
└ └ └ Certificate	1..n	A public key certificate as defined in the protocol or transport profile specification, used to validate the communication and identity of the endpoint. SMP clients MUST ignore endpoints without a valid certificate.
└ └ └ └ TypeCode	1..1	The type and/or use of the certificate, as defined by the protocol or transport profile specification. If an Endpoint element has more than one certificate with the same TypeCode codes, the periods defined by their respective ActivationDate and ExpirationDate dates MUST NOT overlap.
└ └ └ └ Description	0..1	An OPTIONAL human readable description of the certificate.
└ └ └ └ ActivationDate	1..1	The date from which the endpoint will use this certificate.

		The ActivationDate date MUST be the same or a later date than the activation date of the certificate itself. The ActivationDate date MUST be an earlier date than the ExpirationDate date. SMP clients MUST ignore certificates if the ActivationDate date is later than today's date.
└ └ └ └ ExpirationDate	1..1	The date from which the endpoint will no longer use this certificate. The ExpirationDate date MUST be the same or an earlier date than the expiration date of the certificate itself. The ExpirationDate date MUST be a later date than the ActivationDate date. SMP clients MUST ignore certificates if the ExpirationDate date is the same or earlier than today's date.
└ └ └ └ ContentBinaryObject	1..1	The complete base64 portion (i.e., not including the PEM header or footer) of the PEM formatted X.509 public key certificate.
└ └ └ └ ContentBinaryObject/@mimeCode	1..1	An attribute specifying the MIME code of the data contained in the ContentBinaryObject. This value MUST be set to exactly: `application/base64`
└ └ Redirect	0..1	An instruction that the request is redirected to another SMP service. The ServiceMetadata resource MUST have either one Redirect element or one or more Endpoint elements, i.e., it MUST NOT have both and it MUST NOT have none.
└ └ └ PublisherURI	1..1	The absolute URL of the SMP service being redirected to. The PublisherURI MUST only contain the base URL of the new SMP service and MUST NOT contain the resource part. Consequently, when redirected to a new SMP service, an SMP client must therefore construct the complete URL by combining the base URL provided in the PublishURI element with the path to the ServiceMetadata resource as specified in section 5.4 of the OASIS SMP 2.0 specification.
└ └ └ Certificate	0..1	The OPTIONAL X.509v3 Certificate of the redirected SMP service.
└ Signature	1..1	The XML signature, as specified in section 5 below.

5 Redirection

An SMP service MAY redirect a request to another SMP service. This is useful for example when a participant uses multiple SMP services and when migrating from one SMP service to another.

Redirection MUST be done in the manner specified in OASIS SMP 2.0 section 2.1.3. An SMP service MUST NOT use HTTP codes 3xx to redirect to another SMP service. An SMP client MUST NOT follow an HTTP code 3xx redirection to another SMP service.

An SMP client request MUST NOT be redirected more than once. Therefore, an SMP service MUST NOT redirect to another SMP service if the request was already redirected.

Likewise, an SMP client MUST NOT follow the Redirect instruction if already redirected from another SMP service. The SMP client MUST instead abort the operation and report the incompliance in accordance with BPC network policies.

An SMP service MAY include a redirect certificate, however an SMP client is NOT

REQUIRED to validate the redirection certificate.

6 Signing

The ServiceMetadata resource MUST be signed by the SMP service using a valid certificate issued to the SMP service provider as specified in the BPC ??? Policy. The SMP service MUST sign the ServiceMetadata resource in the manner specified in section 5.6.2.1 of the OASIS SMP 2.0 specification.

An SMP client MUST validate the signature of the ServiceMetadata resource in the manner specified in section 5.6.2.2 of the OASIS SMP 2.0 specification. An SMP client MUST NOT send information to any of the endpoints in the SMP service response unless the ServiceMetadata resource is signed using a valid certificate as specified above.

7 Referencing from SML records

When referencing an SMP service from an SML record using OASIS BDXL 1.0, the following identifier MUST be used in the service field of the NAPTR record:

oasis-bdxr-smp-2#bpc1.0

8 Appendix A: Example ServiceGroup resource (non-normative)

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceGroup xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns="http://docs.oasis-open.org/bdxr/ns/SMP/2/ServiceGroup"
 xmlns:ext="http://docs.oasis-open.org/bdxr/ns/SMP/2/ExtensionComponents"
 xmlns:sma="http://docs.oasis-open.org/bdxr/ns/SMP/2/AggregateComponents"
 xmlns:smb="http://docs.oasis-open.org/bdxr/ns/SMP/2/BasicComponents">
    <smb:SMPVersionID>2.0</smb:SMPVersionID>
    <smb:ParticipantID schemeID="urn:oasis:names:tc:ebcore:partyid-
type:iso6523:0060">123456789</smb:ParticipantID>
    <sma:ServiceReference>
        <smb:ID schemeID="bdx-docid-qns" schemeName="QName/Subtype
Identifier"
            >urn:oasis:names:specification:ubl:schema:xsd:Invoice-
2::Invoice##BPC-UBL-Invoice</smb:ID>
        <sma:Process>
            <smb:ID>bpc-simple-invoicing-process</smb:ID>
        </sma:Process>
        <sma:Process>
            <smb:ID>bpc-procurement-process</smb:ID>
        </sma:Process>
    </sma:ServiceReference>
    <sma:ServiceReference>
        <smb:ID schemeID="bdx-docid-qns" schemeName="QName/Subtype
Identifier">urn:oasis:names:specification:ubl:schema:xsd:Order-
2::Order##BPC-UBL-PurchaseOrder</smb:ID>
        <sma:Process>
            <smb:ID>bpc-procurement-process</smb:ID>
        </sma:Process>
    </sma:ServiceReference>
</ServiceGroup>
```

9 Appendix B: Example ServiceMetadata resource (non-normative)

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceMetadata xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns="http://docs.oasis-open.org/bdxr/ns/SMP/2/ServiceMetadata"
 xmlns:ext="http://docs.oasis-open.org/bdxr/ns/SMP/2/ExtensionComponents"
 xmlns:sma="http://docs.oasis-open.org/bdxr/ns/SMP/2/AggregateComponents"
 xmlns:smb="http://docs.oasis-open.org/bdxr/ns/SMP/2/BasicComponents">
    <smb:SMPVersionID>2.0</smb:SMPVersionID>
    <smb:ID schemeID="bdx-docid-qns" schemeName="QName/Subtype Identifier"
        >urn:oasis:names:specification:ubl:schema:xsd:Invoice-
2::Invoice##BPC-UBL-Invoice</smb:ID>
    <smb:ParticipantID schemeID="urn:oasis:names:tc:ebcore:partyid-
type:iso6523:0060">123456789</smb:ParticipantID>
    <sma:ProcessMetadata>
        <sma:Process>
            <smb:ID>bpc-simple-invoicing-process</smb:ID>
        </sma:Process>
        <sma:Process>
            <smb:ID>bpc-procurement-process</smb:ID>
        </sma:Process>
        <sma:Endpoint>
            <smb:TransportProfileID>bdxr-as4-1.0#BPC-
1.0</smb:TransportProfileID>
            <smb:Description>AS4 access point</smb:Description>
            <smb:Contact>as4-ap@example.com</smb:Contact>
            <smb:AddressURI>https://as4.example.com</smb:AddressURI>
            <sma:Certificate>
                <smb:TypeCode>bdxr-as4-signing-encryption</smb:TypeCode>
                <smb:Description>BPC Access Point certificate for both
signing and encryption</smb:Description>
                <smb:ActivationDate>2021-09-01Z</smb:ActivationDate>
                <smb:ExpirationDate>2023-08-31Z</smb:ExpirationDate>
                <smb:ContentBinaryObject
mimeCode="application/base64">MIIFwDCCA...<!—abbreviated--
></smb:ContentBinaryObject>
            </sma:Certificate>
        </sma:Endpoint>
    </sma:ProcessMetadata>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
            <CanonicalizationMethod
Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
            <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256"/>
            <Reference URI="">
                <Transforms>
                    <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                </Transforms>
                <DigestMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <DigestValue>AtTvPa4...<!—abbreviated--></DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>yDMsBn9/...<!—abbreviated--></SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509SubjectName>1.2.840.113549.1.9.1=#16136b62656e6774737
36f6e4065666163742e7065,CN=smp.example.com,OU=IT,O=KH,L=Oracle
Park,ST=CA,C=US</X509SubjectName>
                <X509Certificate>MIIFxzCCA6...<!—abbreviated--
```

```
></X509Certificate>
            </X509Data>
        </KeyInfo>
    </Signature>
</ServiceMetadata>
```