

# Access Point Implementation Guide

Version 1.0

27 July 2016



**Digital  
Business  
Council**

## Disclaimer & Copyright

### Disclaimer

This document is a publication of the Digital Business Council (Council):

Whilst every effort has been made to ensure that the material contained in the document and related attachments are correct, the Council and any other party involved in the creation of the document hereby state that the document is provided without warranty, either expressed or implied, of accuracy or fitness for purpose; and

Hereby disclaim any liability, direct or indirect, for damages or loss relating to the use of the document. The document may be modified, subject to developments in technology, changes to the standards, or new legal requirements without notice. Any product and company name mentioned herein may be trademarks and/or registered trademarks of its respective company.

### Copyright

The copyright for all drafts and publications belongs to the Council.



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

You are free to copy, communicate and adapt the work, so long as you attribute the work to Council and do not suggest that the Council endorses you or your work.

The AS4 Profile of ebMS 3.0 Version 1.0 technical specification is Copyright © OASIS Open 2013. All Rights Reserved. AS4 is based on the OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features OASIS Standard, which is *Copyright © OASIS® 1993–2007. All Rights Reserved*. The ebMS 3.0 Standard uses the SOAP protocol. The IPR declaration of SOAP submitters to W3C is available from <http://www.w3.org/Submission/2000/05/>.

### Acknowledgements

The Council would like to acknowledge the work of OASIS, Pan European Public Procurement Online (PEPPOL) and the Electronic Simple Electronic Networked Services (e-SENS)\_projects for their contributions to the development of this implementation guide and supporting Profile.

# Contents

Disclaimer & Copyright.....	2
1 Audience .....	5
2 Overview .....	6
3 Conformance.....	8
4 Distribution Package.....	8
5 Terms and Definitions (Normative) .....	9
6 Use Cases.....	12
6.1 Sending a Business Document (including Dynamic Discovery) .....	12
6.2 Maintenance of Dynamic Discovery Information.....	14
6.3 Use Case Descriptions.....	14
7 AS4 Version 1.0 Profile (Normative) .....	18
7.1 Messaging Model.....	18
7.2 AS4 ebHandler Profile.....	19
7.2.1 <i>Message Exchange Patterns</i> .....	20
7.2.2 <i>Message Partitioning</i> .....	20
7.2.3 <i>Message Packaging</i> .....	20
7.2.4 <i>User Message</i> .....	21
7.2.5 <i>Signal Message</i> .....	22
7.2.6 <i>Error Handling</i> .....	22
7.2.7 <i>Security</i> .....	22
7.2.8 <i>Reliable Messaging and Reception Awareness</i> .....	22
7.2.9 <i>Extension Properties</i> .....	23
7.2.10 <i>Processing Mode Parameters</i> .....	23
8 Identifiers.....	25
8.1 Party Identifier.....	25
8.2 Action Identifier .....	26
8.3 Service Identifier .....	26

8.4	Agreement Identifier .....	26
9	Endpoint Discovery .....	26
10	Generic settings .....	28
10.1	PMode Settings .....	28
10.2	User message .....	28
10.2.1	<i>Example User Message</i> .....	30
10.3	Signal Response Message .....	30
10.3.1	<i>Example Response Message</i> .....	31
10.4	Error Message .....	32
10.4.1	<i>Example Error Message</i> .....	36
	APPENDIX A: PMode Parameters .....	37
A.1	Base Agreement .....	37
	APPENDIX B: Use Cases .....	40
	BUC100 Send Business Document to Recipient .....	40
	BUC033 List Participant's Capabilities .....	40
	BUC036 Business On-boarding .....	41
	SUC002 Register DCP Alias Address .....	45
	SUC006 Lookup DCP Alias Address .....	47
	SUC013 Remove DCP Alias Address .....	48
	SUC018 List of Accredited Access Points .....	49
	SUC005 Lookup Participant's Digital Capability .....	50
	SUC003 Register Capability .....	51
	SUC014 Update Capability .....	53
	SUC015 Remove Capability .....	55
	References .....	56

# 1 Audience

 <b>BUSINESS ANALYSTS</b>		 <b>APPLICATION DEVELOPERS</b>	
<b>Business Analysts:</b> <ul style="list-style-type: none"> <li>• Those who analyse and document business or processes or systems, assessing the business model or its integration with technology; or</li> <li>• Those involved in the identification of business requirements for solutions to support accounts receivable, accounts payable and the electronic transmission of the associated documents between businesses.</li> </ul>		<b>Application Developers:</b> <ul style="list-style-type: none"> <li>• Those involved in the design, operation and implementation of software and services for the exchange of electronic documents or messages; or</li> <li>• Those involved in the design, integration and operation of business applications dealing with invoicing.</li> </ul>	
<b>Audience Reading Guide</b>		 <b>BUSINESS ANALYSTS</b>	 <b>APPLICATION DEVELOPERS</b>
Overview	2		
Conformance	3		
Distribution Package	4		
Terms and Definitions (Normative)	5		
Use Cases	6		
AS4 Version 1.0 Profile (Normative)	7		

Identifiers	8		
Endpoint discovery	9		
Generic settings	10		
Appendix A: PMode Parameters			
Appendix B: Use Cases			

Primary Audience 

Secondary Audience 

## 2 Overview

The Access Point Implementation Guide defines the standards for delivering and receiving of digital business documents within the Council's Interoperability Framework (Framework). The Framework defines the following components:

- Access Point: A sender or receiver of digital business documents;
- Digital Capability Locator: A service for looking up the location of the Digital Capability Publisher for a Participant. (Digital Business Council, 2016a);
- Digital Capability Publisher: A service for Participants to store details of their capabilities, and includes what scenarios they can process, the data formats they support and the delivery address for their eInvoices. (Digital Business Council, 2016b); and
- Electronic Business Documents: A digital representation of a business document, e.g. an eInvoice.

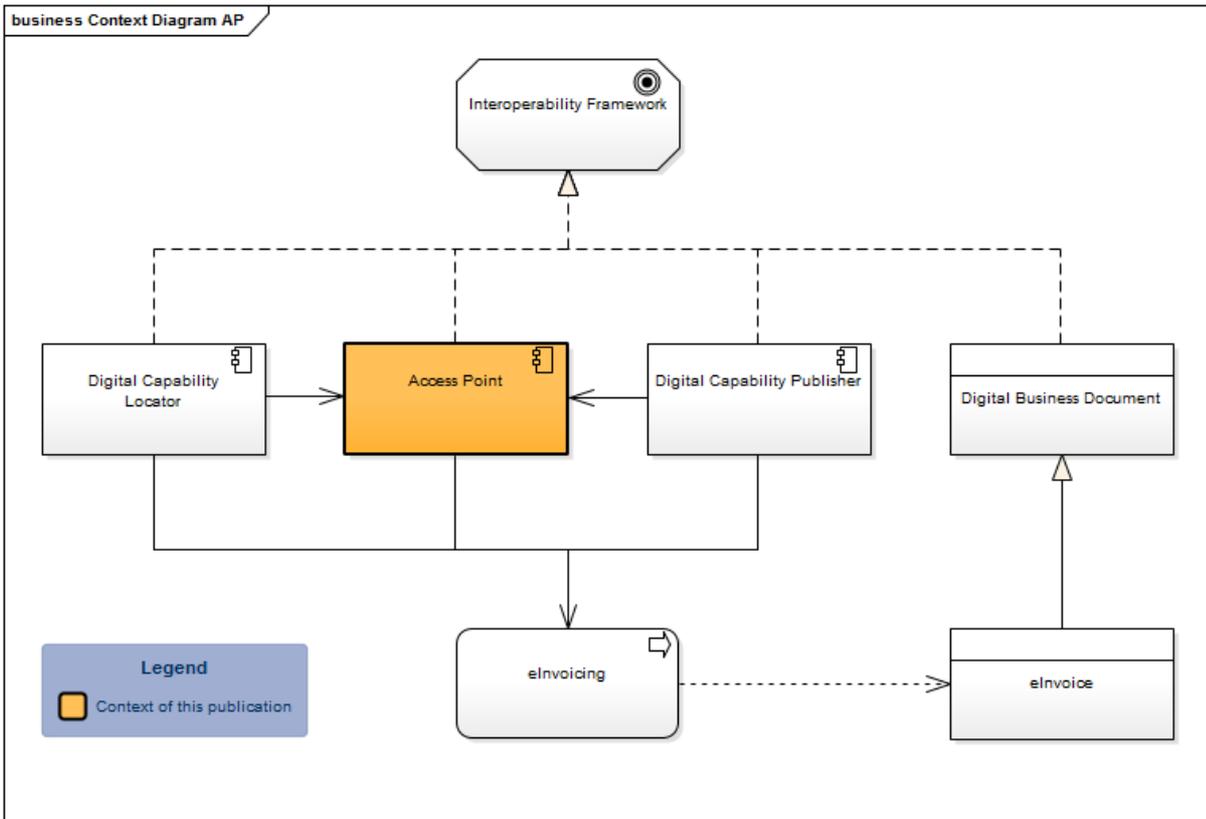


Figure 1: Context of Access Points within the Interoperability Framework

The messaging protocol described in this document is business process and business document agnostic. The underlying OASIS ebMS3 standard has been designed to be flexible and support a large number of use cases. This implementation guide reduces complexity by focusing on the exchange of business documents regardless of their type or the process in which they are used.

The context diagram Figure 1 shows the components included in the Interoperability Framework and where the Access Point (AP) sits. The Digital Capability Publisher and Digital Capability Locator are used by the Access Points and enable the eInvoicing process.

The components of the framework are used in a four-corner model (see Figure 2: Four Corner Model). End users, or participants, don't directly exchange electronic information but connect through a network of Access Points. The digital address for a receiving Access Point is dynamically discovered using the Digital Capability Locator (DCL) and Digital Capability Publisher (DCP) components of the Framework. Access Points may also update a participant's digital endpoint in the DCP.

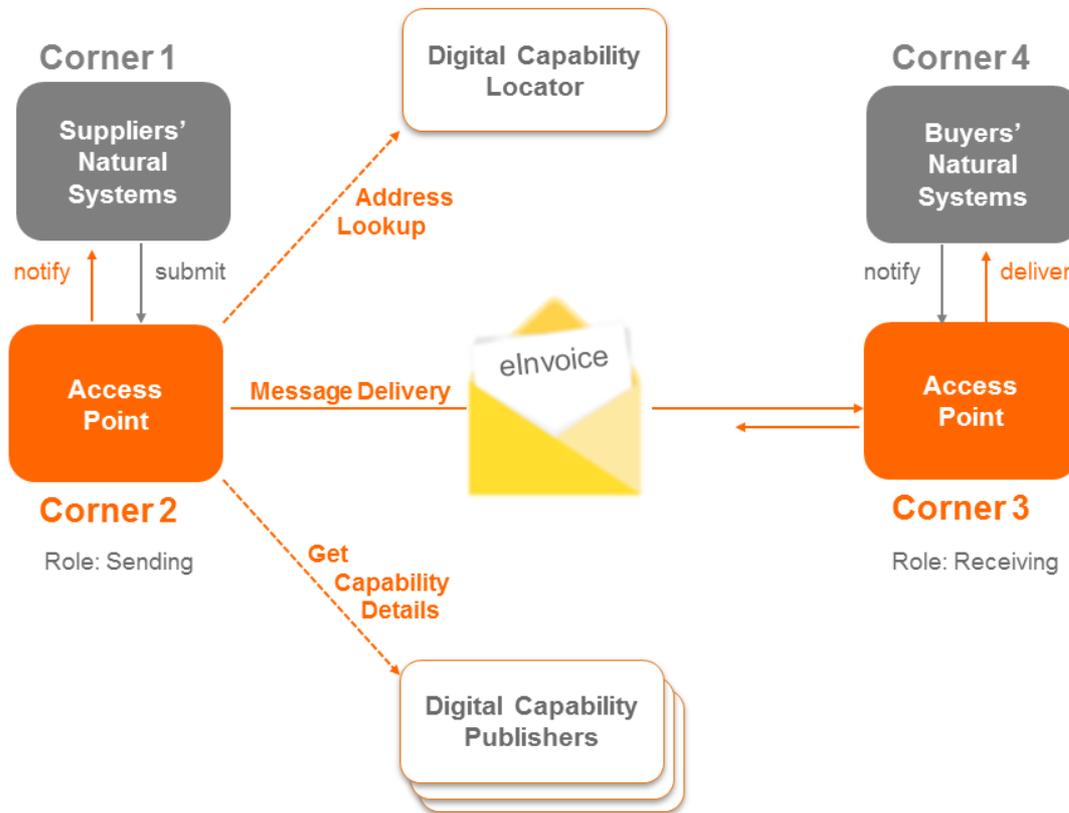


Figure 2: Four Corner Model

### 3 Conformance

Conformance to the Access Point Implementation Guide means conformance with the sections marked as 'Normative' in this Implementation Guide.

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 (Bradner, 1997).

### 4 Distribution Package

The Access Point Implementation Guide and associated artefacts are published at:  
<http://resources.digitalbusinesscouncil.com.au/dbc/services/exchange/implementationguide/current>

This directory contains the following sub-directories:

- testsets – containing example XML fragment instances (used in this document);
- val – test assertions and outcomes for validation testing.

## 5 Terms and Definitions (Normative)

The terms listed in Table 1 are used as defined throughout this specification.

Table 1: Terms and Definitions

Term	Definition
Business Process	A collection of related, structured activities or tasks undertaken by a business (for example, Invoicing).
Code	A set of allowed Values that have standardised meanings that can be resolved unambiguously.
Core	A business requirement, rule, Information Element or supporting UBL Element that Service Interfaces must be able to recognise if they appear in a Document.
CVA	Context/Value Association is an XML Vocabulary using address expressions to specify UBL Elements and their associated constraints.
Data Format	A machine-readable language, syntax or dialect used to present the Information Elements contained in an electronic Document (for example, an eInvoice).
Data Type	A computer representation of well-known abstract concepts such as integer and date.
Distribution Package	A packaged file that contains the technical artefacts to support conformant implementation of the eInvoicing Profile.
Document	A purposeful and self-contained, structured set of Information Elements.
eInvoice	An Invoice, RCTI, Credit Note or Adjustment exchanged using the Council's Data Format.

<b>Term</b>	<b>Definition</b>
eInvoicing	The set of processes required to create and receive eInvoices.
eInvoicing Semantic Model	A structured set of logically interrelated Information Elements used to support eInvoicing.
Extension	A business requirement, rule, Information Element or supporting UBL Element that is not part of the Core Semantic Model.
Genericcode	A standard XML representation for the contents (and associated metadata) of a Code list.
Identification Scheme	The collection of Identifiers applicable for a given type of Information Element governed under a common set of rules.
Identifier	A character string used to establish the identity of, and distinguish uniquely, one instance of an object within an Identification Scheme from all other objects within the same scheme. An Identifier may be a word, number, letter, symbol, or any combination of those.
Information Element	A semantic concept that can be defined independent of any particular data format.
Mandatory	A business requirement, rule, Information Element or supporting UBL Element that must always appear in a Document.
Markup Language	A computer language for marking or tagging a document that indicates its structure either as Information Elements (for data processing) or as display elements (for page layout).
Normative	Sections of a Document conveying criteria to be fulfilled if compliance with the Document is to be claimed and from which no deviation is permitted.
Optional	A business requirement, rule, Information Element or supporting UBL Element that may appear on a Document.
Profile	A conformant subset of a standard specification.

---

Term	Definition
Schema	A World Wide Web Consortium (W3C) recommendation that specifies how to formally describe the UBL Elements in an XML Document.
Schematron	A standard validation language for making assertions about the presence or absence of patterns in UBL Elements.
Service	An application able to process specific Document types for specific business transactions.
Service Interface	A software interface to support a Service.
UBL	Universal Business Language (UBL) is a library of standard XML Schemas for XML Documents such as purchase orders and Invoices.
UBL Extension Element	A UBL Element that enables additions to the standard UBL Schemas.
Value	An expression that cannot be reduced any further. Values are used to express the information for an Information Element and are (generally) formatted as UBL Elements.
XML	Extensible Markup Language (XML) is a Markup Language that defines a set of rules for encoding Documents in a format that is both human-readable and machine-readable.
XML Attribute	XML attributes are normally used to describe or to provide additional information about UBL Elements.
XML Document	A Document encoded using the XML Markup Language.
UBL Element	Each XML document contains one or more elements, the scope of which are either delimited by start and end tags (the characters '<' and '>'). An UBL Element is generally equivalent to an Information Element.

Term	Definition
XML Type	An XML Type consists of a Value space, a lexical space, and a set of facets that characterise properties of the Value space, individual Values or lexical items.
XML Vocabulary	A set of UBL Element definitions for a particular industry or business function.

## 6 Use Cases

This document describes the method of exchange for business documents between two Access Points. Access Points use business discovery services, implemented by DCL and DCP, to determine the receiver of an electronic business document. Access Points therefore act as clients to business discovery services. The DCP and DCL business discovery services are detailed in separate implementation guides.

The use cases listed in this section are separated in two categories:

1. Use cases dealing with the actual operation of sending and receiving business documents; and
2. Use cases dealing with configuration and registration of information to enable the operational use cases.

### 6.1 Sending a Business Document (including Dynamic Discovery)

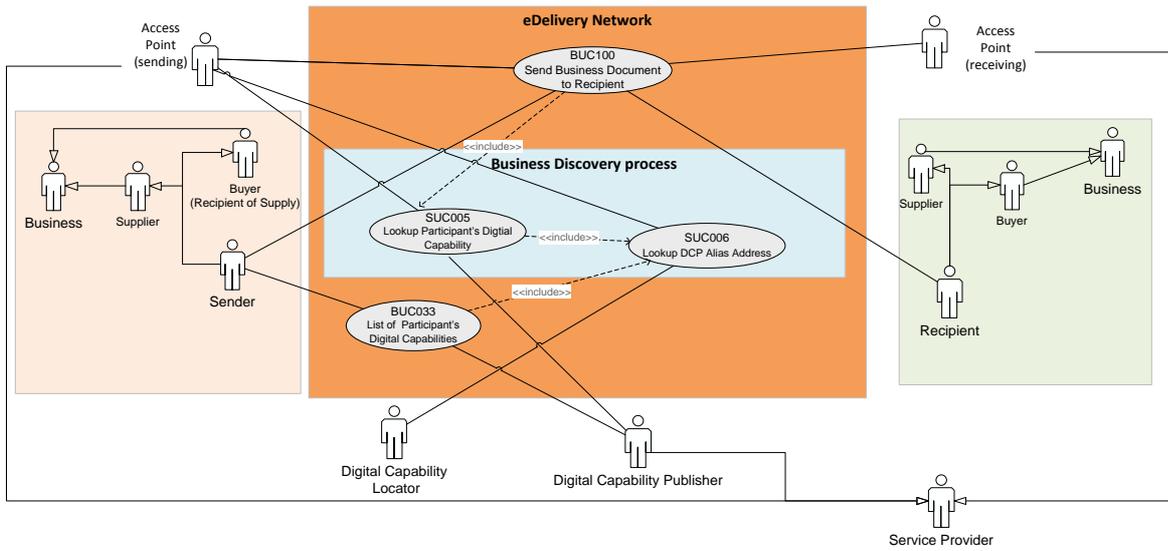


Figure 3: Sending a Business Document (including Dynamic Discovery) Use Case Diagram

## 6.2 Maintenance of Dynamic Discovery Information

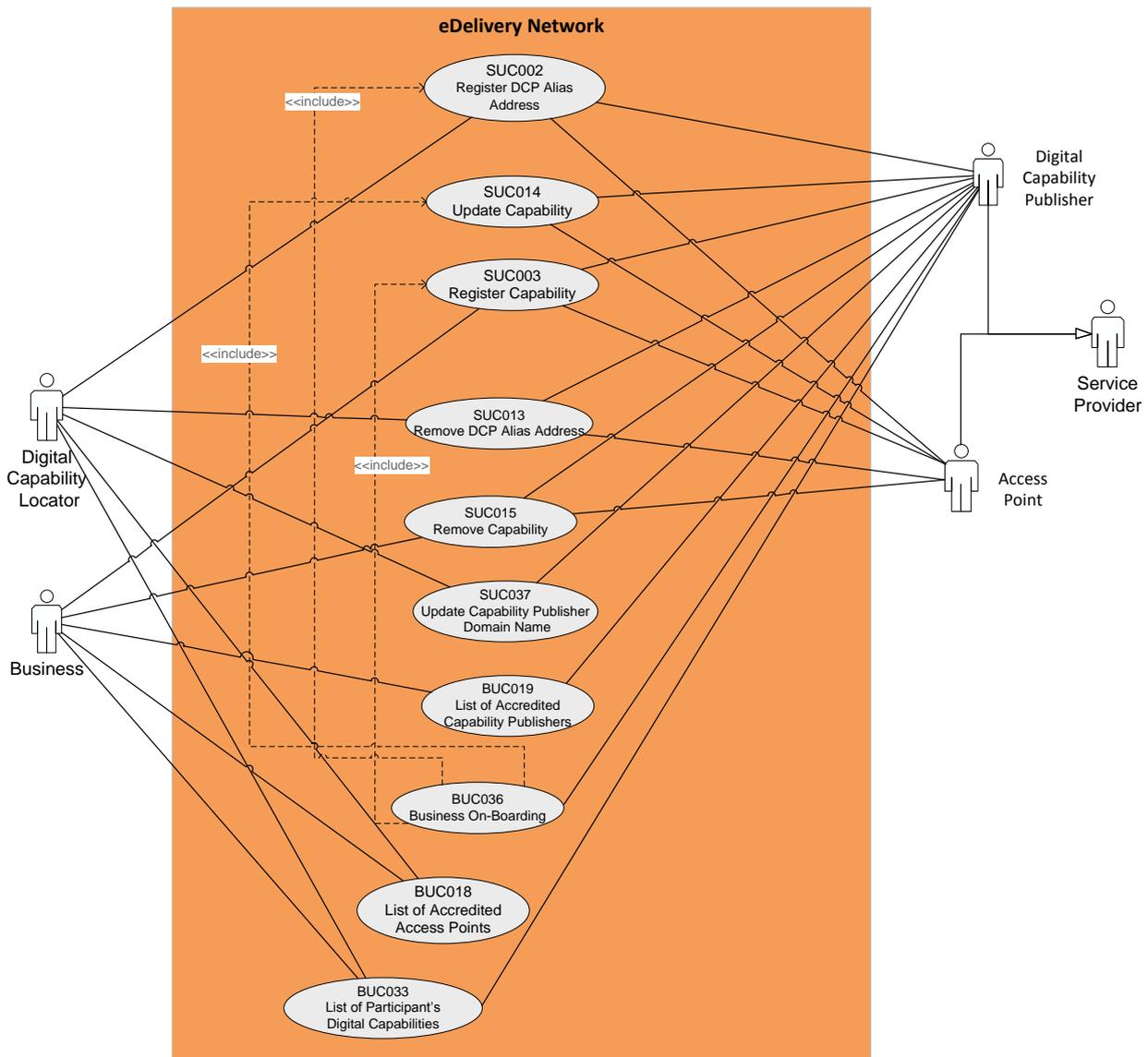


Figure 4: Maintenance Use Case Diagram

## 6.3 Use Case Descriptions

The table below provides a list of business and system use cases that represent the functionality required to support the eDelivery solution.

Table 2: Relevant Use Cases

Use Case ID	Actors	Description	High Level Process	Present In
SUC002	Digital Capability Publisher  Access Point  Digital Capability Locator	Register DCP Alias Address	Maintenance	Implementation guides for:  Access Point, Digital Capability Publisher and Digital Capability Locator
SUC003	Access Point  Digital Capability Publisher	Register Capability	Maintenance	Implementation guides for:  Digital Capability Publisher and Access Point
SUC005	Access Point  Digital Capability Publisher  Digital Capability Locator	Lookup Participant's Digital Capabilities (this includes SUC006)	Sending a business document	Implementation guides for:  Access Point, Digital Capability Publisher and Digital Capability Locator
SUC006	Access Point  Digital Capability Locator	Lookup DCP Alias Address	Sending a business document	Implementation guides for:  Access Point and Digital Capability Locator

Use Case ID	Actors	Description	High Level Process	Present In
SUC013	Access Point Digital Capability Publisher Digital Capability Locator	Remove DCP Alias Address	Maintenance	Implementation guides for:  Access Point, Digital Capability Publisher and Digital Capability Locator
SUC014	Access Point Digital Capability Publisher	Update Capability	Maintenance	Implementation guides for:  Digital Capability Publisher and Access Point
SUC015	Access Point Digital Capability Publisher	Remove Capability	Maintenance	Implementation guides for:  Digital Capability Publisher and Access Point
SUC018	Access Point Business/Sender Digital Capability Locator	List accredited Access Points	eDelivery on boarding / Maintenance	Implementation guides for:  Digital Capability Locator and Access Point

Use Case ID	Actors	Description	High Level Process	Present In
BUC033	Access Point Digital Capability Publisher Digital Capability Locator	List of Participant's Digital Capabilities (Note: looking up all a participant's capabilities is optional, and could be used by the sender to determine a trading partner's ability to receive business documents)  (this includes SUC006)	Maintenance/ Sending a business document	Implementation guides for: Digital Capability Locator, Digital Capability Publisher and Access Point
BUC036	Access Point Digital Capability Publisher Digital Capability Locator	Business On-boarding (Note: this includes a business new to eInvoicing or a business changing a service provider)  (this includes SUC002, SUC003, SUC014)	eDelivery On- boarding / Maintenance	Implementation guides for: Access Point, Digital Capability Publisher and Digital Capability Locator
BUC100	Access Point Digital Capability Publisher Digital Capability Locator	Send Business Document to Recipient  (this includes SUC005)	Sending a business document	Implementation guides for: Access Point , Digital Capability Publisher and Digital Capability Locator

This document addresses BUC100 which is the main responsibility of Access Points i.e. sending and receiving business documents and messages. Access points are also responsible for the

---

maintenance of business capability information in the business discovery components. These services are detailed in the respective implementation guides.

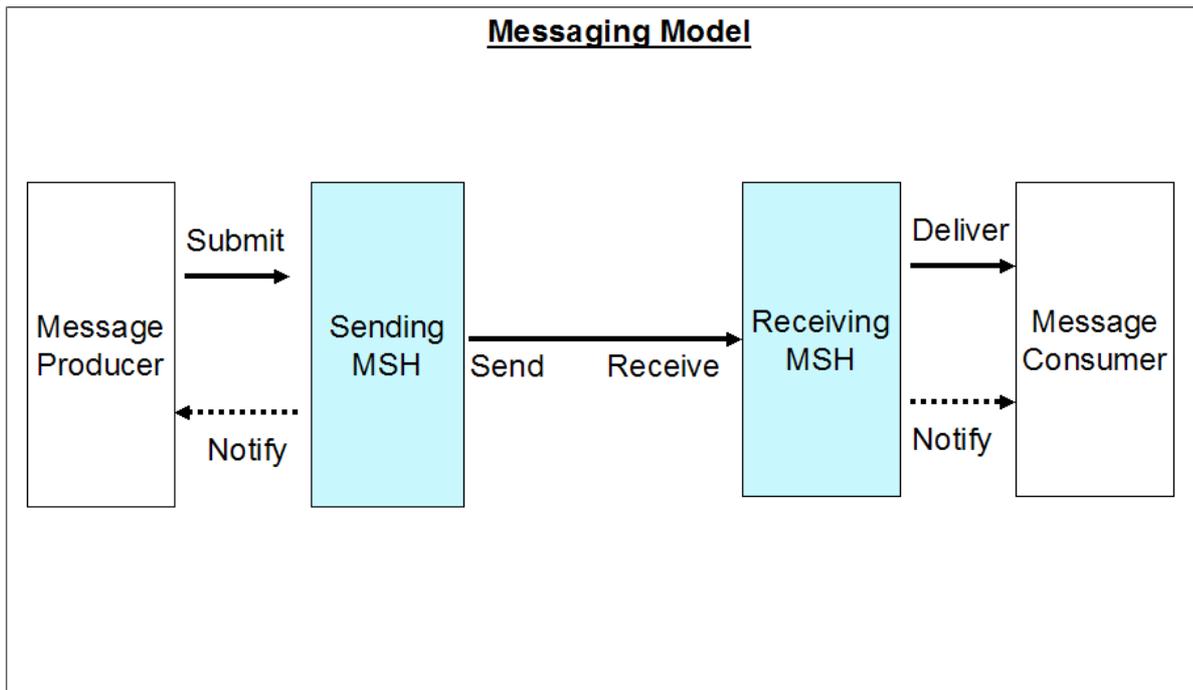
## 7 AS4 Version 1.0 Profile (Normative)

The standards used in the Access Point Implementation Guide are based on freely available open standards. This section describes the Profile of these standards to make the standard suitable for Australian B2B messaging.

### 7.1 Messaging Model

The messaging model in Figure 5 illustrates the following entities:

- **Message Producer:** Business applications or middleware submit message content to the sending Message Service Handler (MSH). A business user typically interacts with the business application and has no knowledge of the MSH;
- **Sending Message Service Handler:** The sending MSH packages the message content and sends the message to the intended receiving MSH;
- **Receiving Message Service Handler:** The receiving MSH receives a message from the sending MSH. The message includes the content which is delivered to the message consumer; and
- **Message Consumer:** The message consumer is the receiver of the business content.



*Figure 5: Messaging Model*

The receiving MSH can be the initiator of the message exchange in the case of pulling a message from the sending MSH. In this Profile however, the sending MSH is always the initiating MSH. The interface between message producer and sending MSH or receiving MSH and message consumer is implementation specific and not defined in this Profile.

## 7.2 AS4 ebHandler Profile

This specification is based on the OASIS standard AS4 ebHandler Profile of ebMS 3.0 Version 1.0 (OASIS, 2013) and provides further guidelines on the use of the Profile in the Australian B2B context. This specification has precedence over the OASIS AS4 standard.

AS4 defines several conformance Profiles each addressing certain use cases. The Profile suitable for use by Access Points is the ebHandler Profile. Other Profiles support occasionally connected endpoints and are useful for sending messages between corners 1 and 2 or 3 and 4. These Profiles are not included in this document.

It should be noted that conforming to this Profile does not mean conformance to the AS4 standard. However, if an implementation conforms to the AS4 standard, it will also conform to this Profile.

### 7.2.1 Message Exchange Patterns

Access Points act as network nodes and are expected to always be connected to the network. It is therefore NOT REQUIRED for Access Points to support pulling of messages when receiving messages from other Access Points.

Although ebMS3 supports choreography of message exchanges, choreography of business processes SHOULD be handled by the business applications. ebMS3 MessageId's correlate messages between two Message Service Handlers and do not carry over to other sections of a transmission (e.g. from corner 3 to corner 4). A two-way Message Exchange Pattern is therefore NOT REQUIRED in the messaging protocol. In this Profile, MessageId and RefToMessageId are only used to correlate signal response messages to user messages. ConversationId is mandatory as per the ebMS3 standard. This element MUST be populated with a tracking identifier.

Support is REQUIRED for the following Message Exchange Pattern:

- 1 One Way/Push

The sending of an eb:Receipt MUST be supported to allow reliable messaging as per the AS4 standard. This Profile only REQUIRES support for the 'response' reply pattern. An eb:Receipt or eb:Error signal message is returned on the back-channel of the underlying transport protocol.

As this Profile is defined in the context of a four-corner model, support for multi-hop message routing (OASIS, 2011) is NOT REQUIRED.

### 7.2.2 Message Partitioning

Pulling of messages is NOT REQUIRED for this Profile when sending or receiving between Access Points which negates the need for message partition channels. If business applications are required to directly submit or receive messages, support for message partitioning is RECOMMENDED.

### 7.2.3 Message Packaging

The Council's AS4 message structure includes a standard message header based on SOAP and MIME enveloping. This Profile does not support payloads in the SOAP body element, all payloads are encoded as MIME parts, including the SOAP envelope as per section 5.1.1 of the ebMS3 standard (OASIS, 2007, p. 34).

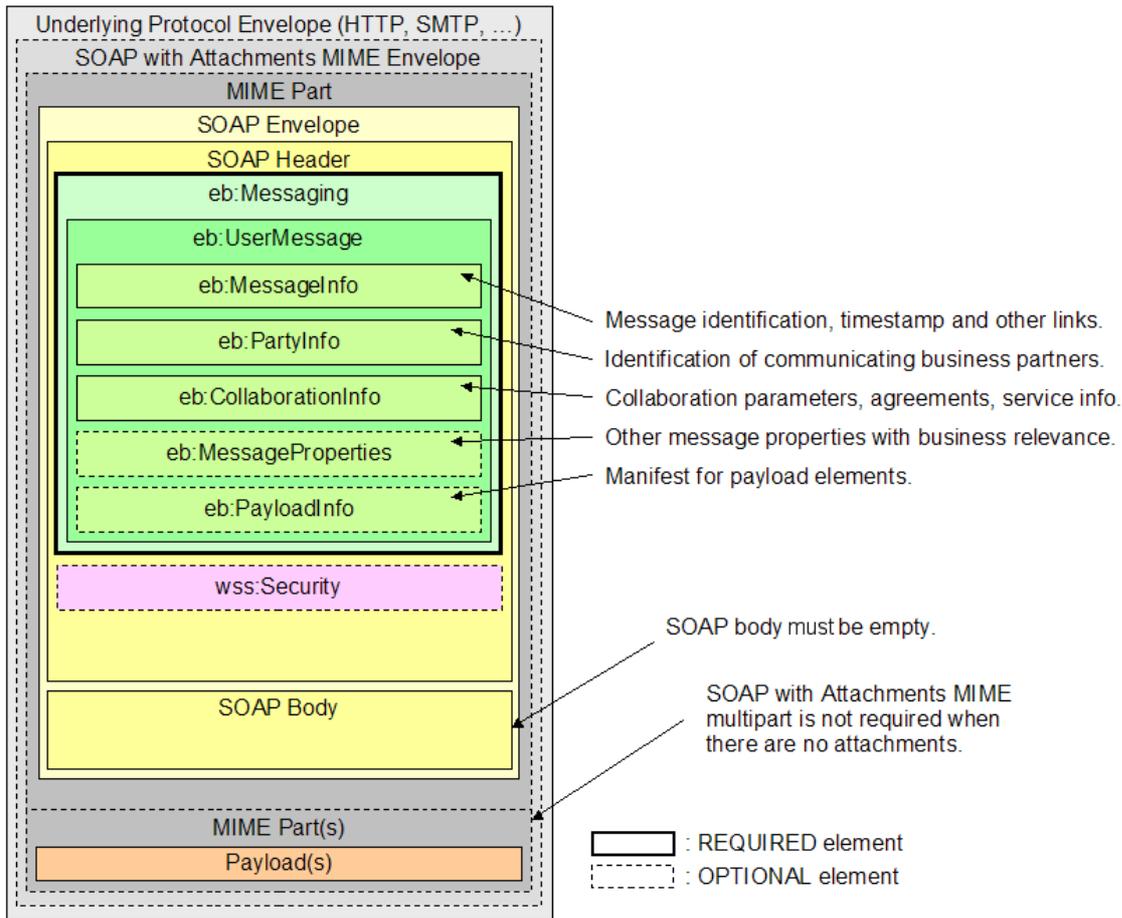


Figure 6: Message Packaging

A message is either a user message or a signal message. Multiple payloads MAY be present and relate to PayloadInfo elements.

Payloads MUST be compressed according to the AS4 Additional Features Compression section 3.1 (OASIS, 2013, p. 24). The size of a message, including compressed payloads, MUST NOT exceed 10 megabytes. Support for large message splitting and joining of messages as defined in (OASIS, 2011) is NOT REQUIRED.

### 7.2.4 User Message

Only one user message is allowed in the SOAP header. The user message describes the transport of business information and includes sender and receiver information.

## 7.2.5 Signal Message

Signal messages do not carry a user message. A signal message is used as a response to a user message. A response can be an acknowledgement of a receipt or an error. The RefToMessageId will refer to the user message for which the response is sent.

## 7.2.6 Error Handling

Errors **MUST** be reported as a response to a request. Sending errors as a separate request is **NOT REQUIRED**.

## 7.2.7 Security

Access Points **MUST** implement security measures when using the public internet for message exchanges.

### 7.2.7.1 Transport Layer Security

Transport layer security provides message confidentiality between Access Points. Implementations **MUST** support TLS version 1.2. Fallback to or earlier versions of TLS or SSL **MUST NOT** be used. TLS versions with known vulnerabilities **MUST NOT** be used.

Ciphers that offer perfect forward secrecy are **RECOMMENDED** when configuring TLS.

Access Points are **REQUIRED** to implement mutual exchange of certificates (Dierks & Rescorla, 2008, p. 55). Receiving Access Points **MUST** only process messages from Access Points that send a known client certificate. Client and server certificates are published in the Digital Capability Locator (Digital Business Council, 2016a). These certificates **SHOULD** be used to verify peer certificates.

### 7.2.7.2 Message Layer Security

Encryption and signing of business messages is the responsibility of business systems and is **NOT REQUIRED** for this Profile between Access Points.

## 7.2.8 Reliable Messaging and Reception Awareness

When a receiving MSH is not available due to unforeseen errors, reliability and reception awareness ensure the message will be delivered once the receiving MSH becomes available. This is enabled

by REQUIRING receipts on the synchronous return leg of the transport protocol. Reception awareness errors SHOULD BE reported to the message producer.

### 7.2.9 Extension Properties

This standard allows the use of Message Properties and Part Properties. The use of these properties must be agreed between partners.

### 7.2.10 Processing Mode Parameters

This section contains a summary of PMode parameters relevant to AS4 features for this conformance Profile. An AS4 handler MUST support and understand those that are mentioned as 'required'. For each parameter, either:

- Full support is required: An implementation MUST support the possible options for this parameter.
- Partial support is required: Support for a subset of values is required.
- No support is required: An implementation is not required to support the features controlled by this parameter, and therefore is not required to understand this parameter.

An AS4 handler is expected to support the PMode set below both as a Sender (of the user message) and as a Receiver.

#### 7.2.10.1 General PMode parameters

- **PMode.ID:** support not required  
PMode.ID is required by AS4 but not required by this Profile. PModes are identified by the PMode.Agreement setting
- **PMode.Agreement:** support required
- **PMode.MEP:** support required for: <http://www.oasis-open.org/committees/ebxml-msg/one-way>
- **PMode.MEPbinding:** support required for: <http://www.oasis-open.org/committees/ebxml-msg/push>
- **PMode.Initiator.Party:** support required
- **PMode.Initiator.Role:** support required for: <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole>
- **(PMode.Initiator.Authorization.username and PMode.Initiator.Authorization.password):** support not required
- **PMode.Responder.Party:** support required

- **PMode.Responder.Role:** support required for: <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole>
- (**PMode.Responder.Authorization.username** and **PMode.Responder.Authorization.password**): support not required

#### 7.2.10.2 PMode[1].Protocol

- **PMode[1].Protocol.Address:** support required for 'http' protocol
- **PMode[1].Protocol.SOAPVersion:** support required for SOAP 1.2

#### 7.2.10.3 PMode[1].BusinessInfo

- **PMode[1].BusinessInfo.Service:** support required
- **PMode[1].BusinessInfo.Action:** support required
- **PMode[1].BusinessInfo.Properties[]:** support not required
- **PMode[1].BusinessInfo.PayloadProfile[]:** support not required
- **PMode[1].BusinessInfo.PayloadProfile.maxSize:** support required for 10000 kilobytes

#### 7.2.10.4 PMode[1].ErrorHandling

- **PMode[1].ErrorHandling.Report.SenderErrorsTo:** support not required
- **PMode[1].ErrorHandling.Report.ReceiverErrorsTo:** support not required
- **PMode[1].ErrorHandling.Report.AsResponse:** support required (true).
- **PMode[1].ErrorHandling.Report.ProcessErrorNotifyConsumer:** support not required
- **PMode[1].ErrorHandling.Report.ProcessErrorNotifyProducer:** support required (true/false)
- **PMode[1].ErrorHandling.Report.DeliveryFailuresNotifyProducer:** support required (true/false)

#### 7.2.10.5 PMode[1].Reliability

Support not required.

#### 7.2.10.6 PMode[1].Security

- **PMode[1].Security.WSSVersion:** support not required
- **PMode[1].Security.X509.Sign:** support not required
- **PMode[1].Security.X509.Encryption:** support not required
- **PMode[1].Security.UsernameToken:** support not required

- **PMode[1].Security.PModeAuthorize**: support required (false)
- **PMode[1].Security.SendReceipt**: support required (true)
- **PMode[1].Security.SendReceipt.NonRepudiation**: support required (false)

#### 7.2.10.7 PMode[1].PayloadService

- **PMode[1].PayloadService.CompressionType**: support required for application/gzip

#### 7.2.10.8 PMode[1].ReceptionAwareness

- **PMode[1].ReceptionAwareness**: support required and when set to true, the **PMode[1].Security.SendReceipt** must also be set to true
- **PMode[1].ReceptionAwareness.Retry**: support required
- **PMode[1].ReceptionAwareness.Retry.Parameters**: support required
- **PMode[1].ReceptionAwareness.DuplicateDetection**: support required
- **PMode[1].ReceptionAwareness.DetectDuplicates.Parameters**: support required.

## 8 Identifiers

The Access Point needs a set of identifiers to determine the recipient of a message exchange (Digital Business Council, 2016c). These values need to be provided to the Access Point, the detail of how this is done is implementation specific and hence not described in this document.

### 8.1 Party Identifier

Party identifiers are used in the following instances:

- Querying DNS for a DCP endpoint (Digital Business Council, 2016a);
- Querying DCP for a list of capabilities (Digital Business Council, 2016b); and
- Identifying participants of a message exchange.

Party identifiers align to ebCore Party Id (OASIS, 2010). The format is:

Type: urn:oasis:names:tc:ebcore:partyid-type:iso6523:<scheme id>

Value: <identifier>

Example:

In this case an Australian ABN is used, ISO 6523 scheme is 0151, and the identifier is the ABN.

```
<eb:PartyId type="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0151" >  
    12345678901  
</eb:PartyId>
```

## 8.2 Action Identifier

The action identifier corresponds to the document identifier in the Digital Capability Publisher (Digital Business Council, 2016b). This value is aligned to the Profile ID in the eInvoicing Implementation Guide (section 9).

Example:

```
dbc-docid:urn:www.digitalbusinesscouncil.com.au:dbc:einvoicing:doctype:core-  
invoice:xsd:core-invoice-  
1#urn:www.digitalbusinesscouncil.com.au:dbc:einvoicing:process:einvoicing01:ver1.0
```

## 8.3 Service Identifier

The service identifier corresponds to the process identifier in the Digital Capability Publisher (Digital Business Council, 2016b). This value is aligned to the Customisation ID in the eInvoicing Implementation Guide (section 9).

The type attribute SHOULD NOT be used. The encoding of the service values is per the Digital Capability Publisher Implementation Guide.

Example:

```
dbc-docid:urn:www.digitalbusinesscouncil.com.au:dbc:einvoicing:ver1.0
```

## 8.4 Agreement Identifier

Agreement value defined by the Digital Business Council:

<http://resources.digitalbusinesscouncil.com.au/dbc/services/exchange/ebms3/Profile>

## 9 Endpoint Discovery

All document exchanges between corners two and three, including dynamic discovery of endpoints, follow a process similar to Figure 7. This implementation guide does not describe how these steps are executed. Dynamic discovery of endpoints changes the way an endpoint is identified.

The endpoint address of a message exchange is determined by querying the Digital Capability Publisher with the following identifiers:

- Recipient Party ID
- Document ID

This returns a signed service metadata structure with a list of processes. Each process has a list of endpoints. A process is identified by a process ID, the endpoint is identified by the transport Profile.

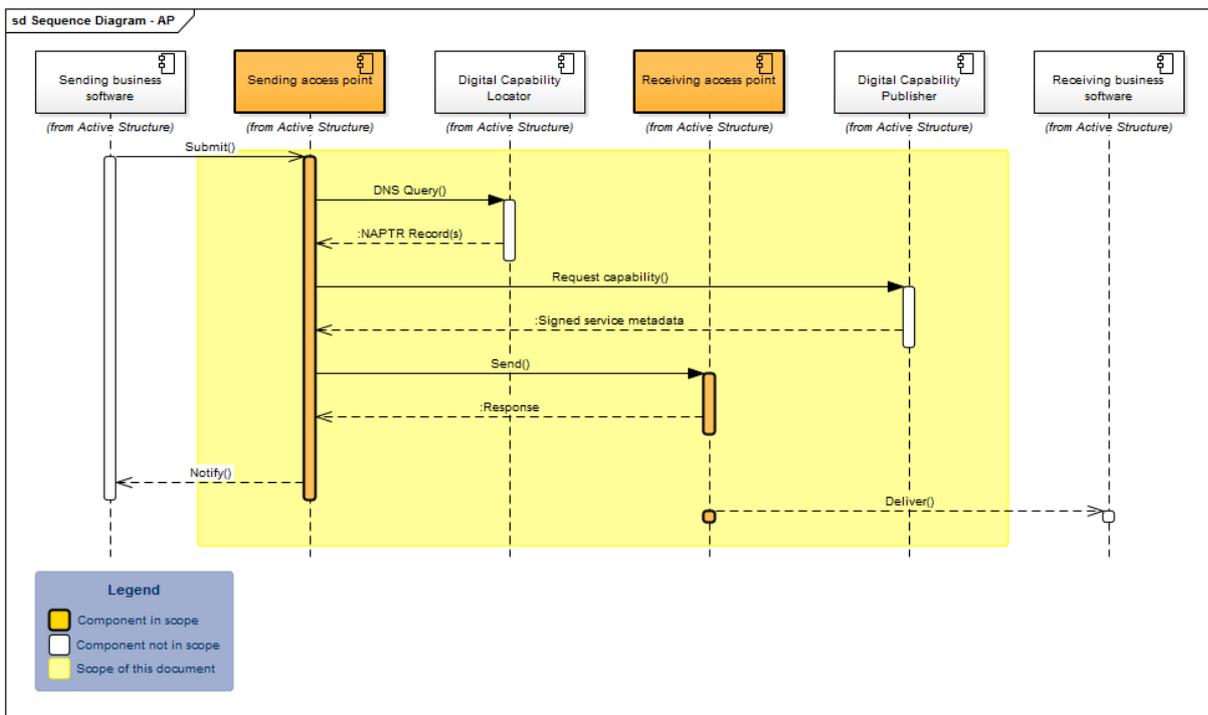


Figure 7: Dynamic Discovery of Endpoints

## 10 Generic settings

This section defines the common settings for exchanging messages within the Council's Framework.

### 10.1 PMode Settings

A list of base PMode settings are listed in Appendix A.1 Base Agreement.

### 10.2 User message

<b>eb:Messaging/eb:UserMessage/eb:MessageInfo</b>	
eb:Timestamp	<p>The REQUIRED Timestamp element has a value representing the date at which the message header was created, and is conforming to a dateTime (W3C, 2012). It MUST be expressed as UTC. Indicating UTC in the Timestamp element by including the 'Z' identifier is optional.</p> <p>E.g. 2016-07-01T00:00:00</p>
eb:MessageId	<p>A unique identifier to identify a message exchange between two Access Points. It is recommended to use a universally unique identifier which can be achieved using a UUID (Leach, Mealling, &amp; Salz, 2005).</p>
<b>eb:Messaging/eb:UserMessage/eb:PartyInfo</b>	
eb:From/eb:PartyId@type	<p>The party ID type uses scheme identifiers from the iso6523 catalog.</p> <p>urn:oasis:names:tc:ebcore:partyid-type:iso6523:&lt;iso6523 scheme&gt;</p>
eb:From/eb:PartyId	<p>The value of the PartyId element depends on the type.</p>
eb:From/eb:Role	<p><a href="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole">http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole</a></p>
eb:To/eb:PartyId@type	<p>The party ID type uses scheme identifiers from the iso6523 catalog.</p> <p>urn:oasis:names:tc:ebcore:partyid-type:iso6523:&lt;iso6523 scheme&gt;</p>
eb:To/eb:PartyId	<p>The value of the PartyId element depends on the type.</p>

eb:To/eb:Role	<a href="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole">http://docs.oasis-open.org/ebxml- msg/ebms/v3.0/ns/core/200704/defaultRole</a>
<b>eb:Messaging/eb:UserMessage/eb:CollaborationInfo</b>	
eb:AgreementRef	<a href="http://resources.digitalbusinesscouncil.com.au/dbc/services/exchange/ebms3profile/current">http://resources.digitalbusinesscouncil.com.au/dbc/services/exchange/ebms3profile/current</a>
eb:Service	The value for this element is copied from the Digital Capability Publisher values when using dynamic discovery.
eb:Action	The value for this element is copied from the Digital Capability Publisher values when using dynamic discovery.
eb:ConversationId	A unique identifier to track a message through the system. This value MUST be a universally unique identifier as described by RFC4122 (Leach, Mealling, & Salz, 2005).
<b>eb:Messaging/eb:UserMessage/eb:PayloadInfo/eb:PartInfo</b>	
@href	Reference to the MIME part
<b>eb:Messaging/eb:UserMessage/eb:PayloadInfo/eb:PartInfo/eb:PartProperties</b>	
<b>These are generic values for attached payloads. Each payload must be compressed as required by the Profile.</b>	
eb:Property@name	CompressionType
eb:Property	application/gzip

## 10.2.1 Example User Message

```

<eb:Messaging S12:mustUnderstand="true">
  <eb:UserMessage>
    <eb:MessageInfo>
      <eb:Timestamp>2016-07-01T00:00:00.000Z</eb:Timestamp>
      <eb:MessageId>0FED9B0A-2150-4EFA-859F-5F7D87D7059A</eb:MessageId>
    </eb:MessageInfo>
    <eb:PartyInfo>
      <eb:From>
        <eb:PartyId type="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0151"
          >12345678901</eb:PartyId>
        <eb:Role>http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/defaultRole</eb:Role>
      </eb:From>
      <eb:To>
        <eb:PartyId type="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0151"
          >12345678902</eb:PartyId>
        <eb:Role>http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/defaultRole</eb:Role>
      </eb:To>
    </eb:PartyInfo>
    <eb:CollaborationInfo>
      <eb:Service>dbc-
docid::urn:www.digitalbusinesscouncil.com.au:dbc:invoicing:ver1.0</eb:Service>
      <eb:Action>dbc-
docid::urn:www.digitalbusinesscouncil.com.au:dbc:invoicing:doctype:core-
invoice:xsd::core-invoice-
1#urn:www.digitalbusinesscouncil.com.au:dbc:invoicing:process:invoicing01:ver1.0</eb:A
ction>
      <eb:ConversationId>22B74363-4608-4EC3-BD14-A3F8717C73CD</eb:ConversationId>
    </eb:CollaborationInfo>
    <eb:PayloadInfo>
      <eb:PartInfo href="cid:invoice">
        <eb:PartProperties>
          <eb:Property name="MimeType">application/xml</eb:Property>
          <eb:Property name="CompressionType">application/gzip</eb:Property>
        </eb:PartProperties>
      </eb:PartInfo>
    </eb:PayloadInfo>
  </eb:UserMessage>
</eb:Messaging>

```

## 10.3 Signal Response Message

A signal response message must be returned by the receiving Access Point. The RefToMessageId value is populated with the value of the MessageId element from the received user message.

---

Non repudiation of receipt is not required in the Profile. Non repudiation of receipt is a business concern and support in this messaging protocol has been removed.

### eb:Messaging/eb:SignalMessage/eb:MessageInfo

eb:Timestamp	<p>The REQUIRED Timestamp element has a value representing the date at which the message header was created, and is conforming to a dateTime (W3C, 2012). It MUST be expressed as UTC. Indicating UTC in the Timestamp element by including the 'Z' identifier is optional.</p> <p>E.g. 2016-07-01T00:00:00</p>
eb:MessageId	<p>A unique identifier to identify a message exchange between two Access Points. It is recommended to use a universally unique identifier which can be achieved using a UUID (Leach, Mealling, &amp; Salz, 2005).</p>
eb:RefToMessageId	<p>This value is copied from the incoming user message.</p>

### 10.3.1 Example Response Message

```

<eb3:Messaging S12:mustUnderstand="true">
  <eb3:SignalMessage>
    <eb3:MessageInfo>
      <eb3:Timestamp>2016-07-01T00:00:01Z</eb3:Timestamp>
      <eb3:MessageId>9925A430-BEB9-42DE-BAD2-3DAD2B46DEF7</eb3:MessageId>
      <eb3:RefToMessageId>0FED9B0A-2150-4EFA-859F-5F7D87D7059A</eb3:RefToMessageId>
    </eb3:MessageInfo>
  </eb3:SignalMessage>
</eb3:Messaging>
  
```

## 10.4 Error Message

All standard ebMS3 and AS4 error codes are supported by this Profile. Table 3 summarises the possible errors that can arise from use of the Council's ebMS3/AS4 Profile. It includes errors specified in section 6.7.1 ebMS Processing Errors (OASIS, 2007) and errors from the AS4 Profile (OASIS, 2013). It does not include errors from sections 6.7.2 Security Processing Errors, 6.7.2 Reliable Messaging Errors and errors from OASIS ebXML Messaging Services Version 3.0: Part 2, Advanced Features (OASIS, 2011).

<b>eb:Messaging/eb:SignalMessage/eb:MessageInfo</b>	
eb:Timestamp	The REQUIRED Timestamp element has a value representing the date at which the message header was created, and is conforming to a dateTime (W3C, 2012). It MUST be expressed as UTC. Indicating UTC in the Timestamp element by including the 'Z' identifier is optional.  E.g. 2016-07-01T00:00:00
eb:MessageId	A unique identifier to identify a message exchange between two Access Points. It is recommended to use a universally unique identifier which can be achieved using a UUID (Leach, Mealling, & Salz, 2005).
<b>eb:Messaging/eb:SignalMessage/eb:Error</b>	
@origin	ebMS
@category	Depends on the error code
@errorCode	ebMS3/AS4 error code
@severity	Depends on the error code
@refToMessageInError	Copied of eb:MessageId from the incoming user message.
eb:Description	A human readable description of the error.

Table 3: Subset of ebMS3 and AS4 Error Codes applicable for this Profile

<b>Error Code</b>	<b>Short Description</b>	<b>Recommended Severity</b>	<b>Category Value</b>	<b>Description or Semantics</b>
EBMS:0001	ValueNotRecognised	Failure	Content	Although the message document is well formed and schema valid, some elements/attribute contains a value that could not be recognised and therefore could not be used by the MSH
EBMS:0002	FeatureNotSupported	Warning	Content	Although the message document is well formed and schema valid, some element/attribute value cannot be processed as expected because the related feature is not supported by the MSH
EBMS:0003	ValueInconsistent	Failure	Content	Although the message is well formed and schema valid, some element/attribute is inconsistent either with the content of other element/attribute, or with, or with the processing mode of the MSH, or with the normative requirements of the ebMS specification.

<b>Error Code</b>	<b>Short Description</b>	<b>Recommended Severity</b>	<b>Category Value</b>	<b>Description or Semantics</b>
EBMS:0004	Other	Failure	Content	<p>An error has occurred that has prevented the message from being correctly processed.</p> <p>A short description SHOULD BE provided by the MSH with this error</p>
EBMS:0005	ConnectionFailure	Failure	Communication	The MSH is experiencing temporary or permanent failure in trying to open a transport connection with a remote MSH
EBMS:0006				Not supported
EBMS:0007	MimeInconsistency	Failure	Unpackaging	The use of MIME is not consistent with the required usage in this specification
EBMS:0008	FeatureNotSupported	Failure	Unpackaging	Although the message is well formed and schema valid, the presence or absence of some element/attribute is not consistent with the capability of the MSH, with respect to the supported features.

<b>Error Code</b>	<b>Short Description</b>	<b>Recommended Severity</b>	<b>Category Value</b>	<b>Description or Semantics</b>
EBMS:0009	InvalidHeader	Failure	Unpackaging	The ebMS header is either not well formed as an XML document, or does not conform to the ebMS packaging rules.
EBMS:0010	ProcessingModeMismatch	Failure	Processing	The ebMS header or another header expected by the MSH is not compatible with the expected content, based on the associated PMode.
EBMS:0011	ExternalPayloadError	Failure	Content	The MSH is unable to resolve an external reference (i.e. a Part that is not contained within the ebMS Message, as identified by a PartInfo/ref URI)
EBMS:0301	MissingReceipt	Failure	Communication	A receipt has not been received for a message that was previously sent by the MSH generating this error
EBMS:0302	InvalidReceipt	Failure	Communication	A Receipt has been received for a message that was previously sent by the MSH generating this error, but the content does not match the message content.

Error Code	Short Description	Recommended Severity	Category Value	Description or Semantics
EBMS:0303	DecompressionFailure	Failure	Communication	An error occurred during the decompression

### 10.4.1 Example Error Message

```

<eb:Messaging S11:mustUnderstand="1">
  <eb:SignalMessage>
    <eb:MessageInfo>
      <eb3:Timestamp>2016-07-01T00:00:01Z</eb3:Timestamp>
      <eb3:MessageId>9925A430-BEB9-42DE-BAD2-3DAD2B46DEF7</eb3:MessageId>
    </eb:MessageInfo>
    <eb:Error origin="ebMS" category="Content"
      errorCode="EBMS:0011" severity="failure"
      refToMessageInError="0FED9B0A-2150-4EFA-859F-5F7D87D7059A">
      <eb:Description xml:lang="en">ExternalPayloadError</eb:Description>
    </eb:Error>
  </eb:SignalMessage>
</eb:Messaging>
  
```

## APPENDIX A: PMode Parameters

### A.1 Base Agreement

This list of PMode parameters defines the default values on which other agreements are based. Other agreements may override these settings if required.

<b>General PMode Parameters</b>	
PMode.Agreement	<a href="http://resources.digitalbusinesscouncil.com.au/dbc/services/exchange/ebms3profile/current">http://resources.digitalbusinesscouncil.com.au/dbc/services/exchange/ebms3profile/current</a>
PMode.MEP	<a href="http://www.oasis-open.org/committees/ebxml-msg/one-way">http://www.oasis-open.org/committees/ebxml-msg/one-way</a>
PMode.MEPbinding	<a href="http://www.oasis-open.org/committees/ebxml-msg/push">http://www.oasis-open.org/committees/ebxml-msg/push</a>
PMode.Initiator.Party	Determined by the message producer
PMode.Initiator.Role	<a href="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole">http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole</a>
PMode.Responder.Party	Determined by the message producer.
PMode.Responder.Role	<a href="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole">http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole</a>
<b>PMode[1].Protocol</b>	
PMode[1].Protocol.Address	Receiving Access Point URL. Determined from DCL/DCP lookup
PMode[1].Protocol.SOAPVersion	1.2
<b>PMode[1].BusinessInfo</b>	
PMode[1].BusinessInfo.Service	The value for this element is copied from the Digital Capability Publisher values when using dynamic discovery.
PMode[1].BusinessInfo.Action	The value for this element is copied from the Digital

	Capability Publisher values when using dynamic discovery.
PMode[1].BusinessInfo.PayloadProfile.maxSize	10000 (kilobytes)
<b>PMode[1].ErrorHandling</b>	
PMode[1].ErrorHandling.Report.AsResponse	true
<b>PMode[1].Security</b>	
PMode[1].Security.PModeAuthorize	false
PMode[1].Security.SendReceipt	true
PMode[1].Security.SendReceipt.NonRepudiation	false
PMode[1].ErrorHandling.Report.ProcessErrorNotifyProducer	true
PMode[1].ErrorHandling.Report.DeliverYFailuresNotifyProducer	true
Pmode[1].Security.SendReceipt.ReplyPattern	response
<b>PMode[1].PayloadService</b>	
PMode[1].PayloadService.CompressionType	application/gzip
<b>PMode[1].ReceptionAwareness</b>	
PMode[1].ReceptionAwareness	true
PMode[1].ReceptionAwareness.Retry	true
PMode[1].ReceptionAwareness.Retry.	maxretries=3;period=120000

Parameters	Period is two minutes which corresponds to the lowest SLA value for response.
PMode[1].ReceptionAwareness.DuplicateDetection	true
PMode[1].ReceptionAwareness.Detect Duplicates.Parameters	maxsize=10Mb;checkwindow=7D Maximum log size is 10Mb for checking. Duplicate check window is guaranteed of seven days minimum.

## APPENDIX B: Use Cases

### BUC100 Send Business Document to Recipient

#### **Purpose**

This high level use case describes the end to end process of sending a business document to a recipient.

#### **Assumptions**

N/A

#### **Preconditions**

1. The Sender, Recipient, Capability Publisher and the Access Points are participants in eDelivery.

#### **Post conditions**

1. The recipient receives the Sender's business document successfully.

#### **Basic Flow**

1. The Sender populates the business document with the required information (identifier and scheme, document type and process);
2. The Sender sends the business document to their Access Point;
3. The sending Access Point performs the business discovery process to obtain the capability of the recipient (which includes obtaining the service endpoint of the receiving Access Point)
  - a. <<include>> SUC005 – Lookup Participant's Digital Capability;
4. The sending Access Point sends the business document to the recipient's nominated Access Point for the business document type;
5. The receiving Access Point receives the business document successfully;
6. The receiving Access Point sends the business document to the recipient;
7. The recipient receives the business document from their nominated Access Point successfully;
8. End flow.

### BUC033 List Participant's Capabilities

#### **Purpose**

This use case describes the steps required for a party, possibly a sender, to discover the entire capabilities (i.e. every process) supported by a participant.

This use case is optional as it would only be useful if there were more than one process supported by a participant. It is not necessary for a Sender to discover all capabilities of a Recipient to send a business document from corners 1 to 4.

### **Assumptions**

1. Any party, even those not participating in eDelivery, can view a Participant's Capabilities; and
2. No authentication or authorisation checks are required.

### **Pre-conditions**

1. The requester needs to know the identifier of the participant they are looking up.

### **Post-conditions**

1. The recipient's digital capabilities have been determined by a participant.

### **Basic Flow**

1. The requester establishes the location of the recipient's digital capabilities
  - a. <<include>> SUC006 - Lookup Participant's DCP Alias Address;
2. The requester constructs the request to retrieve a recipient's capability list;
3. The requester sends the request to the recipient's Digital Capability Publisher;
4. The Digital Capability Publisher creates the response including the capabilities for each process the participant has in their capability record;
5. The requester receives the response;
6. End flow.

## **BUC036 Business On-boarding**

### **Purpose**

This use case describes the process to on-board a business to a single Digital Capability Publisher and/or one or more Access Point services for eDelivery. This does not include Access Point (AP) and Digital Capability Publisher (DCP) service providers themselves, who are covered by the process described in BUC010 i.e. Service Provider On-Boarding.

There are a number of scenarios covered by this use case:

1. A business is entering the eDelivery framework for the first time (new participant); and
2. A business changes their service provider(s) to a single or multiple service provider (noting a business can only have one DCP service provider):
  - a. The business moves both services from one service provider to one or more service providers.
  - b. The business moves only their Access Point service for a particular process to a new service provider.

- c. The business moves only the DCP service to a new service provider.
- d. The business has AP and DCP services with separate providers and consolidates the services with one provider.
- e. The business has different Service Providers for DCP and AP services, and moves each service to two new Service Providers.

### **Assumptions**

1. A Service Provider can operate an Access Point and/or a Capability Register but it is not mandatory to provide both services.
2. Where a Service Provider can provide both services, a business can choose to use both or either service offered by the service provider.

### **Constraints**

1. The Service Provider, when providing both services, must create and maintain the business' DCL entry and DCP capability record.
2. When the business enters into agreements with a DCP service provider and one or more Access Point service providers, the DCP Service provider is responsible for coordinating, creating and maintaining the DCL entry and DCP record on behalf of the business for the duration of this arrangement as it will need all Access Point details to create the business' Capability record in their nominated DCP.
3. When the business has its own Access Point, the Service Provider for DCP services is responsible for creating and maintaining the DCL entry, creating the capability record and responding to requests by the business to update the AP details the business uses as required.
4. In AP service provider change events, the Service Provider holding the business' capability record must comply with AP Service Provider request to update the capability record with the new Access Point details.
5. As defined in the Council's service provider agreements, the losing (Old) Service Provider must cooperate with the gaining (New) Service Provider during portability/change of service events.
6. Only one capability record can exist in the eDelivery framework for a participant; this record contains all the capabilities of the business.

### **Pre-conditions**

1. The business has obtained an Australian Business Number (ABN) from the Australian Business Register (ABR) or a GLN, DUNS or other Council approved identifier.
2. The business is required to receive business documents supported by the Council and the Framework.
3. The New Service Provider is accredited by the Council.

### **Post-conditions**

1. The business has agreements with one or more Service Providers for receiving Council supported business processes and documents through one or more Access Point providers and only one DCP provider, having either become a new participant or changed service providers.
2. The business is discoverable in the Digital Capability Locator and, if the new DCP is listed in the DCL entry.

**Basic Flow – New Participant in Invoicing; Business chooses to use a single Service Provider for both Access Point and DCP services.**

1. The business determines their requirements;
2. The business investigates the services offered and pricing of various service providers;
3. The business determines the Service Provider(s) that meets their requirements;
4. The business enters an agreement with the New Service Provider;
5. The New Service Provider determines if the business' capability is already registered in a capability register (this also determines if the client has an Access Point service in the framework also);
6. The business does not have an existing capability record registered and requires it to be created in the New Service Provider's DCP;
7. The New Service Provider determines the client does not have an Access Point service and will use the New Service Provider's AP;
8. The New Service Provider adds its own supported Access Point address, transport Profiles, document types and processes to the business' capability record in its own Digital Capability Publisher;
  - a. <<include>> SUC003 – Register Capability.
9. The New Service Provider requests the capability address (DCL entry) be added to the Digital Capability Locator;
  - a. <<include>> SUC002 – Register Capability Address.
10. The New Service Provider informs the business the on-boarding activities have been completed;
11. End flow.

**Alternate Flows**

1. **New Participant; Business is signing up to DCP service only (participant may have an AP of its own or is signing a separate agreement with a different AP Service Provider).**
  - a. At step 6, the New Service Provider determines the Business is entering into an agreement with a different Access Point service provider or is using its own Access Point;
  - b. The New Service Provider obtains the AP endpoint address and transport Profile it supports for each document and process, from either the Business (if using its own AP) or the Business' AP Service Provider(s);

- c. The New Service Provider creates a capability record including AP endpoint address, transport Profile, document and process types;
  - i. <<include>> SUC003 – Register Capability.
- d. Resume at step 9.
2. **Existing Participant; the business is moving both services to the New Service Provider.**
  - a. At step 6, the New Service Provider discovers the business has an existing DCP service that needs to be changed to the New Service Provider's DCP service;
  - b. The New Service Provider informs the Losing DCP Service Provider they are now providing the business' DCP service;
  - c. The Losing DCP Service Provider deprecates the business' capability record in their DCP;
  - d. The New Service Provider informs the previous Access Point service provider they are the business' nominated Access Point service provider;
  - e. The New Service Provider creates a capability record including the AP endpoint address(es), transport Profile(s), document and process types;
    - i. <<include>> SUC003 – Register Capability.
  - f. Resume at step 9.

#### **Exception flows**

1. **New Participant; Business is signing up to Access Point service with the New Service Provider, it will use another Service Provider for DCP services.**
    - a. At step 6, the New Service Provider determines the business will use a different service provider for a DCP service;
    - b. The DCP service provider requests the New Service Provider's AP details;
    - c. The New Service Provider provides their AP endpoint address and transport Profile, to enable the DCP Service Provider to successfully create the business' capability record;
    - d. The DCP Service Provider creates the capability record;
      - i. <<include>> SUC003 – Register Capability.
    - e. The DCP Service Provider requests addition of the business' DCL entry in the Digital Capability Locator;
      - i. <<include>> SUC002 – Register Capability Address.
    - f. The DCP Service provider informs the business that all Access Points have been added to the capability record for each document/process and the DCL entry has been created;
    - g. End flow.
  2. **Existing Participant; The Business is changing only to a new AP Service Provider for a particular document type and process**
    - a. At step 9, the service provider discovers the participant has an existing Access Point provider and will be providing this service for the business instead, however the business is retaining its current Digital Capability Publisher Service provider;
-

- b. The New Service Provider informs the previous Access Point service provider they are the business' new AP service provider for the particular document type and process;
- c. The New Service Provider looks up the holder of the business' capability record;
- d. The New Service Provider provides their AP endpoint address and accepted transport protocol for the process and document type to the DCP Service Provider to successfully create the business' capability record;
- e. The DCP Service Provider updates the capability record;
  - i. <<includes>> SUC014 – Update Capability.
- f. The DCP Service Provider informs the business their change in AP service has been updated and they are able to receive documents through the new Access Point;
- g. End flow.

## SUC002 Register DCP Alias Address

### Purpose

This use case describes the interaction required for the Identifier to be mapped to the DCP Alias Address of a participant's Digital Capability Publisher and this mapping added to the Digital Capability Locator, enabling the Participant to be discovered.

### Assumptions

N/A

### Pre-conditions

1. The participant's capability record has been added to an accredited Digital Capability Publisher.
2. The participant does not have a DCP Alias Address already registered.
3. The Digital Capability Publisher has been accredited by the council and added to the Digital Capability Locator.
4. The Digital Capability Publisher has obtained the identifier and the identifier scheme of the participant.

### Post-conditions

1. The DCP Alias Address of the participant's Digital Capability Publisher has been added to the Digital Capability Locator, with the Participant's identifier mapped to the Digital Capability Publisher endpoint address.
2. The participant's Digital Capability Publisher address is discoverable on the Digital Capability Locator.

### Basic Flow

1. The requester constructs the DCP Alias Address record addition request;
2. The requester sends the DCP Alias Address record addition request to the Digital Capability Locator;
3. The Digital Capability Locator receives the DCP Alias Address record addition request;
4. The Digital Capability Locator checks the requester is authorised to request a record addition;
5. The Digital Capability Locator verifies the DCP Alias Address record addition request is in the correct format;
6. The Digital Capability Locator determines no record exists for this participant;
7. The Digital Capability Locator locates the accredited Digital Capability Publisher specified in the request for inclusion in the participant's record;
8. The Digital Capability Locator checks the Digital Capability Publisher in the request is accredited;
9. The Digital Capability Locator publishes the participant's DCP Alias Address record;
10. The Digital Capability Locator responds, informing the requester that the DCP Alias Address has been published successfully;
11. End flow.

### **Exception Flows**

1. At step 4, the Digital Capability Locator determines the requester is not authorised and sends an error response indicating this;
2. At step 5, the Digital Capability Locator is unable to add the DCP Alias Address record successfully because the request format is invalid;
  - a. The Digital Capability Locator sends an error message response to the requester;
  - b. End flow.
3. At step 6, the Digital Capability Locator is unable to add the DCP Alias Address record successfully to the Digital Capability Locator because the participant already has a record;
  - a. The Digital Capability Locator sends an error message response to the requester;
  - b. End flow.
4. At step 7, the Digital Capability Locator is unable to add the DCP Alias Address record successfully because the Digital Capability Publisher identifier provided cannot be found;
  - a. The Digital Capability Locator sends an error message response to the requester;
  - b. End flow.
5. At step 8, the Digital Capability Locator is unable to add the DCP Alias Address record successfully because the Digital Capability Publisher is not accredited;
  - a. The Digital Capability Locator sends an error message response to the requester;
  - b. End flow.

## SUC006 Lookup DCP Alias Address

### Purpose

This use case describes the steps required for a party to discover the DCP Alias Address of a participant.

### Assumptions

1. The Digital Capability Locator does not supply the URL to the capability record in the Digital Capability Publisher, but only the URL of the Digital Capability Publisher, it is up to the requester to construct the location of the capability record URL in the subsequent request.
2. The business document may have been generated by the sender and sent to the Access Point as part of sending a business document. The Access Point may be trying to discover the location of the capability record in order to send the business document to the recipient's Access Point.
3. Any participant can look up the DCP Alias Address of another participant.

### Pre-conditions

1. The requester and Digital Capability Publisher are participants in eDelivery.
2. The requester is aware of the identifier and the identifier scheme of the participant in order to lookup the DCP Alias Address.

### Post-conditions

1. The location of the recipient's Digital Capability Publisher endpoint address has been determined by the requester.

### Basic Flow

1. The requester forms a query to locate the capability record of the recipient;
2. The requester sends the query to their Domain Name System (DNS) server;
3. The Digital Capability Locator receives the query;
4. The Digital Capability Locator locates the DCP Alias Address for the recipient;
5. The Digital Capability Locator sends the query response to the requester;
6. The requester successfully receives the query response;
7. End flow.

### Alternate Flows

1. At step 3, the Digital Capability Locator is unavailable at the time of the query;
  - a. The requester retries a specified amount of attempts;
  - b. The Digital Capability Locator is available during one of the attempts;
  - c. Resume at step 3.

2. At step 2, the DCP Alias Address of a recipient's capability has been previously looked up by the requester, stored locally and is still valid (the Time-To-Life has not expired). The capability location is then determined by the requester based on this cached record and the Digital Capability Locator does not need to be queried.

### **Exception Flows**

1. At step 4 the Digital Capability Locator cannot locate the recipient's DCP Alias Address record and responds with an error message indicating this outcome;
  - a. At step 2 the Digital Capability Locator domain is incorrect;
  - b. The DNS server responds with an error;
  - c. End flow.
2. At step 6 the DCP Alias Address is not present in the DCP Alias Address record
  - a. The Digital Capability Locator responds to the query;
  - b. The requester receives the response but cannot discover the location of the Participant's Digital Capability Publisher;
  - c. End flow.

## **SUC013 Remove DCP Alias Address**

### **Purpose**

This use case describes the steps to remove a DCP Alias Address record from the Digital Capability Locator.

### **Assumptions**

1. The participant no longer trades or decides not to participate in eDelivery.
2. The Digital Capability Publisher or the participant can request removal the participant's DCP Alias Address, so long as they can be authenticated and their permissions allow this.
3. The requester could be removing the record before adding a new one.

### **Pre-conditions**

1. The participant has an existing DCP Alias Address record.

### **Post-conditions**

1. The participant's DCP Alias Address record is no longer discoverable on the Digital Capability Locator.

### **Basic Flow**

1. The Digital Capability Publisher or participant itself sends a request to the Digital Capability Locator to remove the participant's DCP Alias Address record;
  2. The Digital Capability Locator receives the request;
-

3. The Digital Capability Locator checks the requester is authorised to request the record to be removed;
4. The Digital Capability Locator checks the request format is correct;
5. The Digital Capability Locator locates the participant's record;
6. The Digital Capability Locator removes the participant's DCP Alias Address record;
7. The Digital Capability Locator sends a response to the requester confirming the location has been removed;
8. End flow.

### **Exception Flows**

1. At step 3, the Digital Capability Locator determines the requester is not authorised to perform a removal of the Digital Address;
2. At step 4, the Digital Capability Locator is unable to remove the DCP Alias Address record successfully because the request format is not valid;
  - a. The Digital Capability Locator sends an error message response to the requester;
  - b. End flow.
3. At step 5, the Digital Capability Locator cannot find a DCP Alias Address Record for the participant;
  - a. The Digital Capability Locator sends an error message response to the requester;
  - b. End flow.

## **SUC018 List of Accredited Access Points**

### **Purpose**

This may be performed when a requester wants to discover all accredited Access Points accredited or determine the accreditation status of a particular Access Point.

### **Assumptions**

1. This list will be readily available and not require authentication and authorisation checks for requesters.

### **Pre-conditions**

1. The Access Points on the list have been accredited by the accreditation body.

### **Post-conditions**

1. The requester has obtained the list of accredited Access Points.

### **Basic Flow**

1. The requester sends a request to the Digital Capability Locator for a list of accredited Access Points;

2. The Digital Capability Locator receives the request;
3. The Digital Capability Locator compiles the list of accredited Access Points;
4. The Digital Capability Locator sends the response with the list to the requester;
5. End flow.

## SUC005 Lookup Participant's Digital Capability

### Purpose

This use case describes the steps required for a party to discover a specific capability for a particular document and process. The party would discover in the capability the service endpoint and transport Profile for a recipient's Access Point for the specified document and process.

For example, an Access Point could be trying to determine if the Recipient actually accepts eInvoicing process documents such as Tax Invoices, where to send them and in what format.

### Assumptions

1. Capability records should not be cached or stored outside of a Digital Capability Publisher, but the capability looked up in the Digital Capability Publisher each time needs to be discovered.
2. Any party can determine the business processes and capability of a participant in eDelivery without being authenticated or authorised.

### Pre-conditions

1. The requester has obtained the Participant's identifier and its scheme, the document type, and the business process.

### Post-conditions

1. The recipient's digital capability for the document type and business process has been confirmed by a requester.
2. The requester has determined the recipient's Access Point endpoint address and transport Profile needed to send the business document.

### Basic Flow

1. The requester establishes the location of the recipient's Digital Capability Publisher
  - a. <<include>> SUC006 - Lookup Participant's DCP Alias Address;
2. The requester constructs the request to retrieve recipient's capability record including participant identifier, document type and process type;
3. The requester sends the request to the Digital Capability Publisher endpoint;
4. The Digital Capability Publisher receives the request and verifies the format is correct;
5. The Digital Capability Publisher finds the appropriate capability record;

6. The Digital Capability Publisher creates the response including the capability record of the Participant, containing the Access Point service endpoint and transport Profile for the specified process;
7. The Digital Capability Publisher sends the response to the requester;
8. The requester receives the response successfully;
9. End flow.

### **Exception Flows**

1. At step 5, the Digital Capability Publisher cannot find a Capability Record for the participant;
  - a. The Capability Record sends an error message response to the requester;
  - b. End flow.
2. At step 2, the Digital Capability Publisher is unable to find the Capability record successfully because the request format is not valid;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
3. At step 2, the Digital Capability Publisher is unable to find the Capability record successfully because the identifier provided does not conform to an Identifier scheme supported by the Council;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
4. At step 2, the Digital Capability Publisher is unable to find the Capability successfully because the document type or process provided in the request does not conform to any in the capability record for that participant;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.

## **SUC003 Register Capability**

### **Purpose**

This use case describes the steps required for an Access Point provider or a participant to add the digital capability record for the participant on a Digital Capability Publisher.

### **Assumptions**

1. The party adding the capability record is authenticated and authorised to perform the addition of a capability record on behalf of the Participant.

### **Pre-conditions**

1. The Access Point endpoint address and transport Profile for each of the Participant's supported business processes is known to the party adding the capability record.

2. A participant cannot have an existing capability in any Digital Capability Publisher.

### **Post-conditions**

1. The participant's capability record has been added to a Digital Capability Publisher, including the Access Point endpoint address for each business process and the transport Profile used for each process.
2. There is only one Digital Capability Publisher record for a participant in any Digital Capability Publisher.

### **Basic Flow**

1. The Access Point provider or Participant sends the capability record addition request to the Digital Capability Publisher;
2. The Digital Capability Publisher checks the requester is authorised to perform the addition of a capability record;
3. The Digital Capability Publisher checks the request format is correct;
4. The Digital Capability Publisher checks the participant does not have an existing record in this Digital Capability Publisher;
5. The Digital Capability Publisher creates the capability record;
6. The Digital Capability Publisher adds the capability record successfully;
7. The Digital Capability Publisher informs the requester of the successful addition of the record;
8. The Digital Capability Publisher adds the DCP Alias Address of the participant to the Digital Capability Locator;
  - a. <<include>> SUC002 - Register DCP Alias Address
9. End flow.

### **Exception Flows**

1. At step 2, the Digital Capability Publisher is unable to add the Capability Record because the requester is not authorised to add a record;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
2. At step 5, the Digital Capability Publisher is unable to add the Capability Record successfully because the transport Profile in the request does not conform to the supported Council transport Profiles;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
3. At step 5, the Digital Capability Publisher is unable to add the Capability record successfully because the request format is not valid;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.

4. At step 5, the Digital Capability Publisher is unable to add the Capability record successfully because the identifier provided does not conform to an Identifier scheme supported by the Council;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
5. At step 5, the Digital Capability Publisher is unable to add the Capability Record successfully because the document identifier in the request does not conform to a supported document identifier scheme;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
6. At step 5, the Digital Capability Publisher is unable to add the Capability Record successfully because the process identifier in the request does not conform to a supported process identifier scheme;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.

## SUC014 Update Capability

### Purpose

This use case describes the steps to update a participant's capability. This could be, for example, to change Access Point endpoint locations for a business process in the capability record, update a transport Profile for a process, or add a capability for a new business process.

### Assumptions

1. The Access Point or Participant can update the Digital Capability Publisher.
2. The requester needs to be authenticated and only authorised parties can update capability records.

### Pre-conditions

1. The participant has an existing capability record in the Digital Capability Publisher.

### Post-conditions

1. The participant's capability record has had the appropriate detail updated.

### Basic Flow

1. The requester sends a request to the Digital Capability Publisher to update the capability record with the appropriate detail;
2. The Digital Capability Publisher checks if the requester is authorised to an update to the participant's record;

3. The Digital Capability Publisher determines the request format to be valid;
4. The Digital Capability Publisher locates the record to be updated;
5. The capability record is updated by the Digital Capability Publisher with the requested detail;
6. The Digital Capability Publisher responds with confirmation the capability record has been updated;
7. End basic flow.

### **Exception Flows**

1. At step 2, the Digital Capability Publisher is unable to add the Capability Record because the requester is not authorised to add a record;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
2. At step 4, the Digital Capability Publisher cannot find a record belonging to the participant;
  - a. The Digital Capability Publisher responds with an error message;
  - b. End flow.
3. At step 3, the Digital Capability Publisher is unable to update the Capability Record successfully because the transport Profile in the request does not conform to the supported Council transport Profiles;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
4. At step 3, the Digital Capability Publisher is unable to update the Capability record successfully because the request format is not valid;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
5. At step 3, the Digital Capability Publisher is unable to update the Capability record successfully because the participant identifier provided does not conform to an Identifier scheme supported by the Council;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
6. At step 3, the Digital Capability Publisher is unable to update the Capability record successfully because the Access Point endpoint address provided does not conform to the correct format;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.
7. At step 3, the Digital Capability Publisher is unable to update the Capability Record successfully because the document identifier in the request does not conform to a supported document identifier scheme;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.

8. At step 3, the Digital Capability Publisher is unable to update the Capability Record successfully because the process identifier in the request does not conform to a supported process identifier scheme;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.

## SUC015 Remove Capability

### Purpose

This use case describes the steps to remove a participant's capability. This could be to either remove a single business process from the participant's record or to remove the entire capability for all business processes for a participant.

### Assumptions

1. A requester could be the Access Point or the Participant themselves.
2. The requester needs to be authenticated and only authorised parties can remove capability.

### Pre-conditions

1. The participant has an existing capability record in the Digital Capability Publisher.

### Post-conditions

1. The participant's capability record has had the appropriate detail(s) removed.

### Basic Flow

1. The requester sends a request to the Digital Capability Publisher to remove the required capability;
2. The Digital Capability Publisher checks that the requester is authorised to remove the capability;
3. The Digital Capability Publisher determines the remove request format to be correct;
4. The Digital Capability Publisher locates the capability needing to be removed;
5. The Capability requested by the requester is removed by the Digital Capability Publisher;
6. The Digital Capability Publisher responds to the requester with confirmation the capability has been removed;
7. End flow.

### Exception Flows

1. At step 2, the Digital Capability Publisher is unable to remove the capability because the requester is not authorised to add a record;
  - a. The Digital Capability Publisher sends an error message response to the requester;
  - b. End flow.

2. At step 4 the Digital Capability Publisher cannot find a record belong to the participant;
  - a. The Digital Capability Publisher responds with an error message;
  - b. End flow.
3. At step 3 the Digital Capability Publisher finds the request format to be invalid;
  - a. The Digital Capability Publisher responds with an error message;
  - b. End flow.

## References

1. Bradner, S. (1997, March). Key words for use in RFCs to Indicate Requirement Levels. From <https://www.ietf.org/rfc/rfc2119.txt>
  2. Dierks, T., & Rescorla, E. (2008, August). The Transport Layer Security (TLS) Protocol Version 1.2. From <https://tools.ietf.org/html/rfc5246>
  3. Digital Business Council. (2016a). Digital Capability Locator Implementation Guide. Canberra: Digital Business Council.
  4. Digital Business Council. (2016b). Digital Capability Publisher Implementation Guide. Canberra: Digital Business Council.
  5. Digital Business Council. (2016d). eInvoicing Semantic Model. From <http://resources.digitalbusinesscouncil.com.au/dbc/processes/einvoicing/semanticmodel/current.docx>
  6. Digital Business Council. (2016c). Policy on the Use of Business Identifiers. From <http://resources.digitalbusinesscouncil.com.au/dbc/services/discovery/policy/businessidentifiers.docx>
  7. ISO. (1988, July 15). ISO 9735:1988 Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules. From [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=17592](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=17592)
  8. ISO/IEC. (2014a, November 15). ISO/IEC 15459-3:2014 Information technology -- Automatic identification and data capture techniques -- Unique identification -- Part 3: Common rules. From [http://www.iso.org/iso/home/store/catalogue\\_ics/catalogue\\_detail\\_ics.htm?csnumber=54781](http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54781)
  9. ISO/IEC. (2014b, November 15). ISO/IEC 15459-4:2014 Information technology -- Automatic identification and data capture techniques -- Unique identification -- Part 4: Individual products and product packages. From [http://www.iso.org/iso/home/store/catalogue\\_ics/catalogue\\_detail\\_ics.htm?csnumber=54782](http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54782)
  10. ISO/IEC. (1991, December 16). ISO/IEC 646:1991 Information technology -- ISO 7-bit coded character set for information interchange. From [http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=4777](http://www.iso.org/iso/catalogue_detail.htm?csnumber=4777)
-

11. ISO/IEC. (1998, December 20). ISO/IEC 6523-1:1998 Information technology — Structure for the identification of organizations and organization parts — Part 1: Identification of organization identification schemes. From [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=25773](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=25773)
12. Leach, P., Mealling, M., & Salz, R. (2005, July). A Universally Unique IDentifier (UUID) URN Namespace. From <https://www.ietf.org/rfc/rfc4122.txt>
13. OASIS. (2013). AS4 Profile of ebMS 3.0 Version 1.0. (J. Durand, & P. van der Eijk, Eds.) From <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html>
14. OASIS Code List Representation TC. (2007). Code List Representation (Genericcode) Version 1.0. From <http://docs.oasis-open.org/codelist/cs-genericcode-1.0/doc/oasis-code-list-representation-genericcode.html>
15. OASIS. (2007). ebXML Messaging Services Version 3.0: Part 1, Core Features. (P. Wenzel, Ed.) From [http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms\\_core-3.0-spec-os.html](http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.html)
16. OASIS. (2011). ebXML Messaging V3, Part 2: Advanced Features. From <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/part2/201004/csd03/rddl-ebms3-part2.html>
17. OASIS. (2011). ebXML Messaging V3, Part 2: Advanced Features. From <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/part2/201004/csd03/rddl-ebms3-part2.html>
18. OASIS. (2010, July 9). OASIS ebCore Party Id Type Technical Specification Version 1.0. (D. Moberg, & P. van der Eijk, Eds.) From <https://docs.oasis-open.org/ebcore/PartyIdType/v1.0/CD03/PartyIdType-1.0.html>
19. OASIS UBL TC. (2013). Context/value association using genericcode 1.0. . From <http://docs.oasis-open.org/codelist/cs01-ContextValueAssociation-1.0/doc/context-value-association.html>
20. OASIS UBL TC. (2013). Universal Business Language (UBL) 2.1 (ISO/IEC 19845). From <http://docs.oasis-open.org/ubl/os-UBL-2.1/>
21. OASIS. (2013, November 4). Universal Business Language Version 2.1. (J. Bosak , T. McGrath , & G. Holman , Eds.) From <http://docs.oasis-open.org/ubl/os-UBL-2.1/UBL-2.1.html>
22. Schematron. (2004). A language for making assertions about patterns found in XML documents. From <http://schematron.com/spec.html>
23. W3C. (2012, April 5). W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes. From <http://www.w3.org/TR/xmlschema11-2/>