Trans-Tasman e-Invoicing

Access Point Implementation Guide

Version 1.2

20 February 2019

Disclaimer & Copyright

Disclaimer

This document is based on a publication of the Digital Business Council (Council) and has been updated by the Trans-Tasman Working Group to include New Zealand particulars.

The policy outlined in this paper has not received final Government approval. Therefore, this publication should be treated as a guide on how this policy may apply and operate.

Whilst every effort has been made to ensure that the material contained in the document and related attachments are correct, the Trans-Tasman Working Group 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

Acknowledgements

The Trans-Tasman Working Group would like to acknowledge the work of the Council, its working groups and other contributors (Superstream, Pan European Public Procurement Online (PEPPOL) and Electronic Simple Electronic Networked Services (e-SENS) projects)) for their leadership and contributions in the development of this Policy.

Version Control

Version	Description	Release Date
1.0	e-Invoicing framework finalised and associated documentation approved and published by the Digital Business Council.	July 2016
1.1	Post the March 2018 announcement by the Prime Ministers of Australia and New Zealand, the framework was updated to become the common approach for both countries (Trans-Tasman framework). Draft version published for industry feedback.	October 2018
1.2	Industry feedback incorporated. Inconsistencies on identifiers fixed. Minor wording changes that have no material impact on framework Minor updates in 'Copyright' section.	February 2019

Contents

1 Audience

 BUSINESS ANALYSTS	 APPLICATION DEVELOPERS
Business Analysts: • Those who analyse and document business or processes or systems, assessing the business model or its integration with technology; • 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.	Application Developers: • Those involved in the design, operation and implementation of software and services for the exchange of electronic documents or messages; or • Those involved in the design, integration and operation of business applications dealing with invoicing.

Audience Reading Guide		 BUSINESS ANALYSTS	 APPLICATION DEVELOPERS
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			

Primary Audience

Secondary Audience

2 Overview

The Access Point Implementation Guide defines the standards for delivering and receiving of digital business documents within the Trans-Tasman e-Invoicing 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. (Trans-Tasman Working Group, 2018);
- 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 e-Invoices. (Trans-Tasman Working Group, 2018); and
- Electronic Business Documents: A digital representation of a business document, e.g. an e-Invoice.

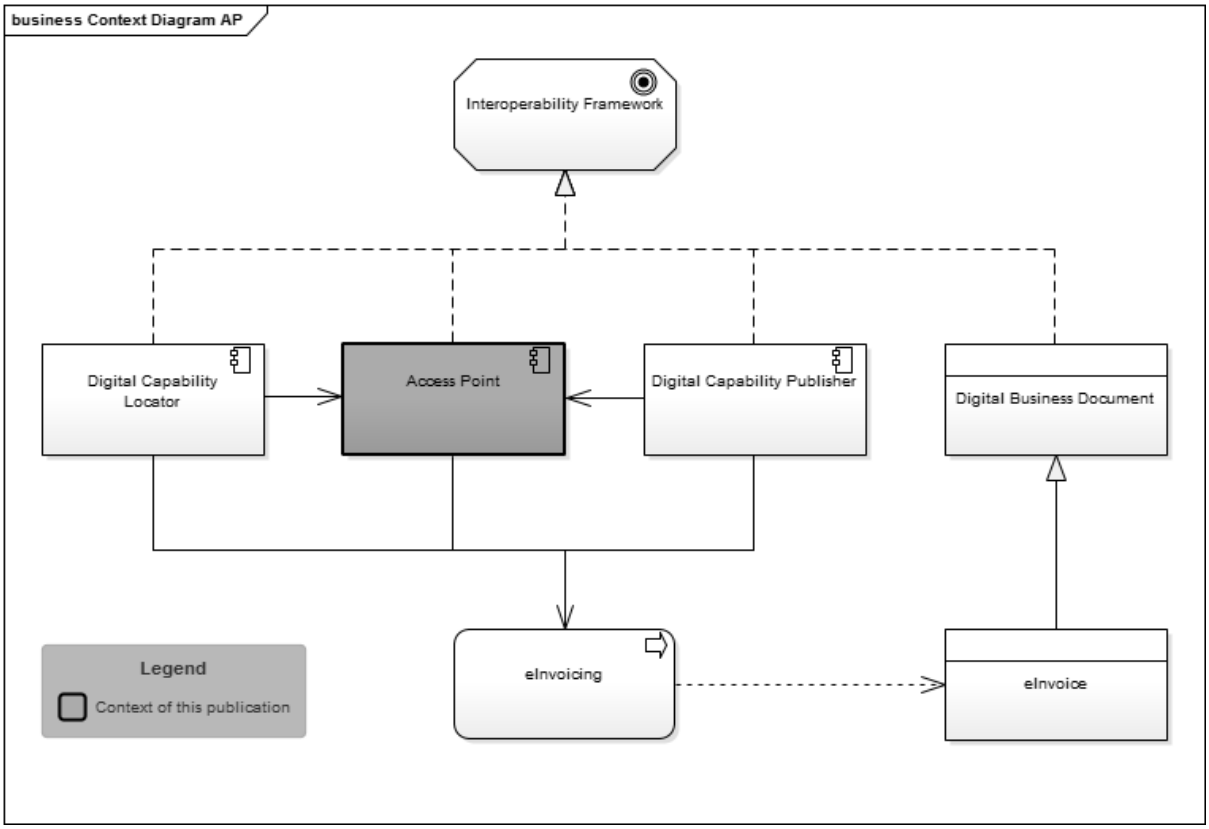

Figure 1: Context of Access Points within the Interoperability Framework

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 e-Invoicing 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.

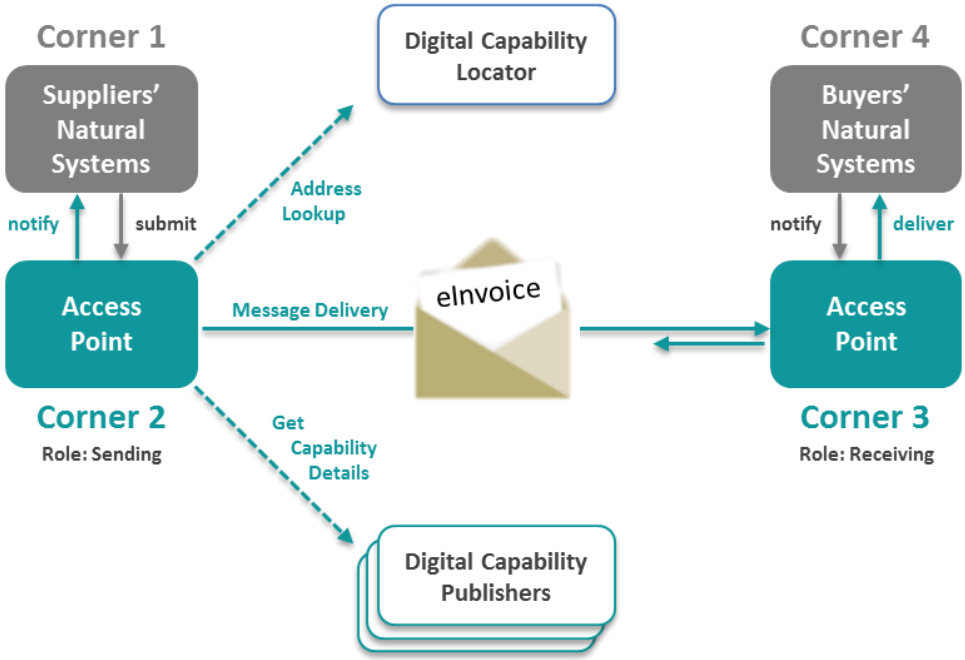

Figure 2: Four Corner Model

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 is published at: https://softwaredevelopers.ato.gov.au/Trans-Tasman-eInvoicing

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 e-Invoice).
Data Type	A computer representation of well-known abstract concepts such as integer and date.
DCL	Digital Capability Locator A master registry of business identifiers associated with a DCP.
DCP	Digital Capability Publisher A registry of electronic capabilities associated with a business identifier. A DCP will answer questions such as 'what electronic document type can the business receive and what is the electronic endpoint for this document?'.
Distribution Package	A packaged file that contains the technical artefacts to support conformant implementation of the e-Invoicing Profile.
Document	A purposeful and self-contained, structured set of Information Elements.
e-Invoice	An Invoice, RCTI, Credit Note or Adjustment exchanged using the Trans-Tasman Data Format.
e-Invoicing	The set of processes required to create and receive e-Invoices.
e-Invoicing Semantic Model	A structured set of logically interrelated Information Elements used to support e-Invoicing.
Extension	A business requirement, rule, Information Element or supporting UBL Element that is not part of the Core Semantic Model.

Term	Definition
Genericode	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.
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.

Term	Definition
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.
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

Use Cases describe 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 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.

Further details can be found in the Trans-Tasman e-Invoicing Use Cases document.

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 3 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.
- **Message Consumer**: The message consumer is the receiver of the business content.

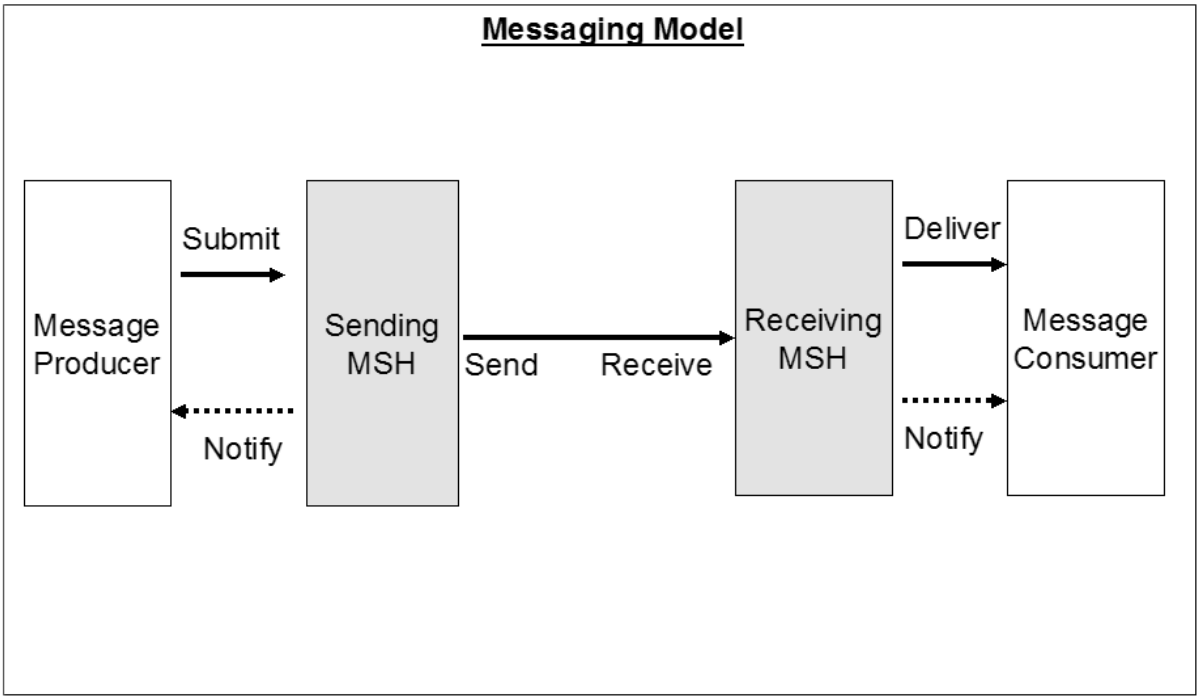

Figure 3: Messaging Model

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 Conformance 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 trans-Tasman 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).

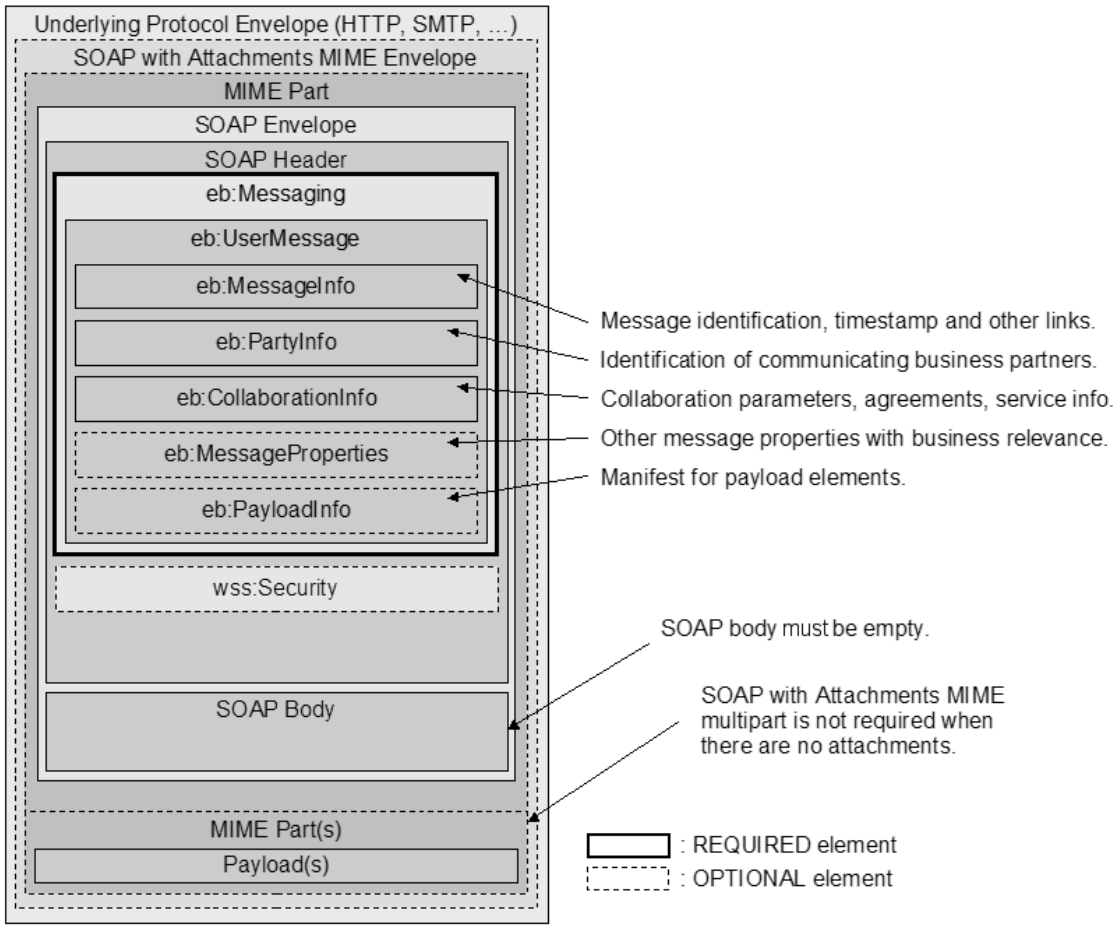

Figure 4: Message Packaging

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. 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 unforseen 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 (Trans-Tasman Working Group , 2018). 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[1]
- Querying DCP for a list of capabilities (Trans-Tasman Working Group, 2018); 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" >
        51083392303
</eb:PartyId>
```

8.2 Action Identifier

The action identifier corresponds to the document identifier in the Digital Capability Publisher. (Trans-Tasman Working Group, 2018). This value is aligned to the Customization ID in the e-Invoicing Implementation Guide (section 10).

Example:

```
dbc-docid::urn:resources.digitalbusinesscouncil.com.au:dbc:invoicing:documents:core-invoice:xsd::core-invoice-1##urn:resources.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 (Trans-Tasman Working Group, 2018). This value is aligned to the Profile ID in the e-Invoicing Implementation Guide (section 9).

[1] Trans-Tasman Digital Capability Locator Implementation Guide, Canberra: Trans-Tasman Working Group.

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

Example:

dbc-procid::urn:resources.digitalbusinesscouncil.com.au:dbc:einvoicing:ver1.0

8.4 Agreement Identifier

Agreement value is defined as:

http://resources.digitalbusinesscouncil.com.au/dbc/services/exchange/ebms3profile/current

9 Endpoint Discovery

All document exchanges between corners two and three, including dynamic discovery of endpoints, follow a process similar to Figure 5. 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.

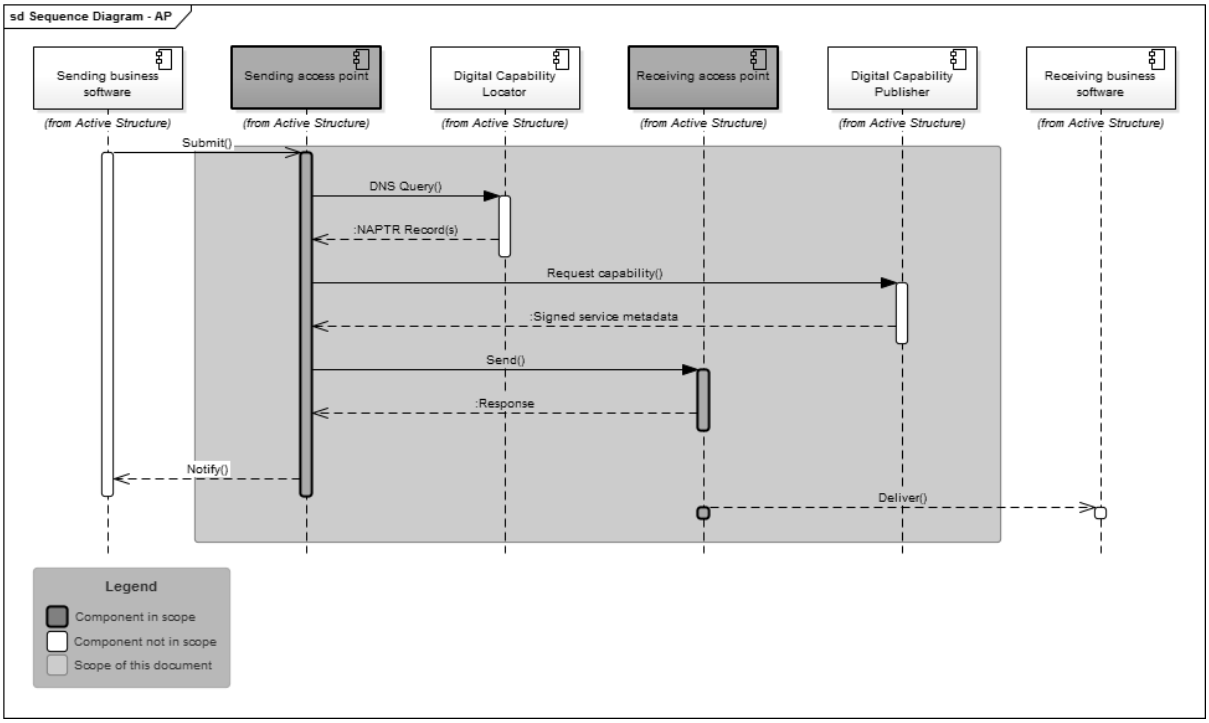

Figure 5: Dynamic Discovery of Endpoints

10 Generic settings

This section defines the common settings for exchanging messages within the trans-Tasman Framework.

10.1 PMode Settings

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

10.2 User message

eb:Messaging/eb:UserMessage/eb:MessageInfo	
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).
eb:Messaging/eb:UserMessage/eb:PartyInfo	
eb:From/eb:PartyId@type	The party ID type uses scheme identifiers from the iso6523 catalog. urn:oasis:names:tc:ebcore:partyid-type:iso6523:<iso6523 scheme>
eb:From/eb:PartyId	The value of the PartyId element depends on the type.
eb:From/eb:Role	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole
eb:To/eb:PartyId@type	The party ID type uses scheme identifiers from the iso6523 catalog. urn:oasis:names:tc:ebcore:partyid-type:iso6523:<iso6523 scheme>
eb:To/eb:PartyId	The value of the PartyId element depends on the type.
eb:To/eb:Role	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole
eb:Messaging/eb:UserMessage/eb:CollaborationInfo	
eb:AgreementRef	http://resources.digitalbusinesscouncil.com.au/dbc/services/exchange/ebms3profile/current

eb:Messaging/eb:UserMessage/eb:MessageInfo	
eb:Service	The value for this element is copied from the Digital Capability Publisher process identifier values when using dynamic discovery.
eb:Action	The value for this element is copied from the Digital Capability Publisher document identifier values when using dynamic discovery.
eb:ConversationId	A unique identifier to track a message though the system. This value MUST be a universally unique identifier as described by RFC4122 (Leach, Mealling, & Salz, 2005).
eb:Messaging/eb:UserMessage/eb:PayloadInfo/eb:PartInfo	
@href	Reference to the MIME part
eb:Messaging/eb:UserMessage/eb:PayloadInfo/eb:PartInfo/eb:PartProperties These are generic values for attached payloads. Each payload must be compressed as required by the Profile.	
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"
                  >51083392303</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:iso6523:0088"
                  >9429041926024</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:AgreementRef>http://resources.digitalbusinesscouncil.com.au/dbc/services/exchange/ebms3profile/current
          </eb:AgreementRef>
          <eb:Service> dbc-procid::urn:resources.digitalbusinesscouncil.com.au:dbc:einvoicing:ver1.0</eb:Service>
          <eb:Action> dbc-docid::urn:resources.digitalbusinesscouncil.com.au:dbc:invoicing:documents:core-invoice:xsd::core-
invoice- 1##urn:resources.digitalbusinesscouncil.com.au:dbc:einvoicing:process:einvoicing01:ver1.0</eb:Action>
          <eb:ConversationId>22B74363-4608-4EC3-BD14-A3F8717C73CD</eb:ConversationId>
        </eb:CollaborationInfo>
        <eb:PayloadInfo>
          <eb:PartInfo href="cid:e-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:Messaging/eb:SignalMessage/eb:MessageInfo	
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).
eb:RefToMessageId	This value is copied from the incoming user message.

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 2 summarises the possible errors that can arise from use of the Trans-Tasman 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).

eb:Messaging/eb:SignalMessage/eb:MessageInfo	
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).

eb:Messaging/eb:SignalMessage/eb:MessageInfo	
eb:Messaging/eb:SignalMessage/eb:Error	
@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 2: Subset of ebMS3 and AS4 Error Codes applicable for this Profile

Error Code	**Short Description**	**Recommended Severity**	**Category Value**	**Description or Semantics**
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

Error Code	Short Description	Recommended Severity	Category Value	Description or Semantics
				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.
EBMS:0004	Other	Failure	Content	An error has occurred that has prevented the message from being correctly processed. A short description SHOULD BE provided by the MSH with this error
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.
EBMS:0009	InvalidHeader	Failure	Unpackaging	The ebMS header is either not well formed as an XML

Error Code	Short Description	Recommended Severity	Category Value	Description or Semantics
				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.
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.

General PMode Parameters	
PMode.Agreement	http://resources.digitalbusinesscouncil.com.au/dbc/services/exchange/ebms3profile/current
PMode.MEP	http://www.oasis-open.org/committees/ebxml-msg/one-way
PMode.MEPbinding	http://www.oasis-open.org/committees/ebxml-msg/push
PMode.Initiator.Party	Determined by the message producer
PMode.Initiator.Role	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole
PMode.Responder.Party	Determined by the message producer.
PMode.Responder.Role	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultRole
PMode[1].Protocol	
PMode[1].Protocol.Address	Receiving Access Point URL. Determined from DCL/DCP lookup
PMode[1].Protocol.SOAPVersion	1.2
PMode[1].BusinessInfo	
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)
PMode[1].ErrorHandling	
PMode[1].ErrorHandling.Report.AsRespo	true

General PMode Parameters	
nse	
PMode[1].Security	
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
PMode[1].PayloadService	
PMode[1].PayloadService.CompressionType	application/gzip
PMode[1].ReceptionAwareness	
PMode[1].ReceptionAwareness	true
PMode[1].ReceptionAwareness.Retry	true
PMode[1].ReceptionAwareness.Retry.Parameters	maxretries=3period=120000 Period is two minutes which corresponds to the lowest SLA value for response.
PMode[1].ReceptionAwareness.DuplicateDetection	true
PMode[1].ReceptionAwareness.DetectDuplicates.Parameters	maxsize=10Mbcheckwindow=7D Maximum log size is 10Mb for checking. Duplicate check window is guaranteed of seven days minimum.

References

Bradner, S. (1997, March). *Key words for use in RFCs to Indicate Requirement Levels.* Retrieved from https://www.ietf.org/rfc/rfc2119.txt

Dierks, T., & Rescorla, E. (2008, August). *The Transport Layer Security (TLS) Protocol Version 1.2.* Retrieved from https://tools.ietf.org/html/rfc5246

ISO. (1988, July 15). *ISO 9735:1988 Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules.* Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=17592

ISO/IEC. (1991, December 16). *ISO/IEC 646:1991 Information technology -- ISO 7-bit coded character set for information interchange.* Retrieved from http://www.iso.org/iso/catalogue_detail.htm?csnumber=4777

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.* Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=25773

ISO/IEC. (2014a, November 15). *ISO/IEC 15459-3:2014 Information technology -- Automatic identification and data capture techniques -- Unique identification -- Part 3: Common rules.* Retrieved from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54781

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.* Retrieved from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54782

Leach, P., Mealling, M., & Salz, R. (2005, July). *A Universally Unique IDentifier (UUID) URN Namespace.* Retrieved from https://www.ietf.org/rfc/rfc4122.txt

OASIS. (2007). *OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features.* (P. Wenzel, Ed.) Retrieved from http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.html

OASIS. (2010, July 9). *OASIS ebCore Party Id Type Technical Specification Version 1.0.* (D. Moberg, & P. van der Eijk, Eds.) Retrieved from https://docs.oasis-open.org/ebcore/PartyIdType/v1.0/CD03/PartyIdType-1.0.html

OASIS. (2011). *ebXML Messaging V3, Part 2: Advanced Features.* Retrieved from http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/part2/201004/csd03/rddl-ebms3-part2.html

OASIS. (2011). *OASIS ebXML Messaging Services Version 3.0: Part 2, Advanced Features.* Retrieved from http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/part2/201004/csd03/rddl-ebms3-part2.html

OASIS. (2013). *AS4 Profile of ebMS 3.0 Version 1.0.* (J. Durand, & P. van der Eijk, Eds.) Retrieved from http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html

OASIS. (2013, November 4). *Universal Business Language Version 2.1.* (J. Bosak , T. McGrath , & G. Holman , Eds.) Retrieved from http://docs.oasis-open.org/ubl/os-UBL-2.1/UBL-2.1.html

OASIS Code List Representation TC. (2007). *Code List Representation (Genericode) Version 1.0.* Retrieved from http://docs.oasis-open.org/codelist/cs-genericode-1.0/doc/oasis-code-list-representation-genericode.html

OASIS UBL TC. (2013). *Context/value association using genericode 1.0. .* Retrieved from http://docs.oasis-open.org/codelist/cs01-ContextValueAssociation-1.0/doc/context-value-association.html

OASIS UBL TC. (2013). *Universal Business Language (UBL) 2.1 (ISO/IEC 19845).* Retrieved from http://docs.oasis-open.org/ubl/os-UBL-2.1/

Schematron. (2004). *A language for making assertions about patterns found in XML documents.* Retrieved from http://schematron.com/spec.html

Trans-Tasman Working Group . (2018). *Trans-Tasman e-Invoicing policy for using business identifiers.* Retrieved from https://softwaredevelopers.ato.gov.au/Trans-Tasman-eInvoicing

Trans-Tasman Working Group . (2019). *Trans-Tasman e-Invoicing - Use cases .* Canberra: https://softwaredevelopers.ato.gov.au/Trans-Tasman-eInvoicing.

Trans-Tasman Working Group. (2018). Trans-Tasman e-Invoicing Digital Capability Locator Implementation Guide. Canberra: https://softwaredevelopers.ato.gov.au/Trans-Tasman-eInvoicing.

Trans-Tasman Working Group. (2018). Trans-Tasman e-Invoicing Digital Capability Publisher Implementation Guide. Canberra: https://softwaredevelopers.ato.gov.au/Trans-Tasman-eInvoicing.

Trans-Tasman Working Group. (2018). *Trans-Tasman eInvoicing Semantic Model.* Retrieved from https://softwaredevelopers.ato.gov.au/Trans-Tasman-eInvoicing

W3C. (2012, April 5). *W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes.* Retrieved from http://www.w3.org/TR/xmlschema11-2/