Access Point Provider Agreement

Between

Digital Business Council

AND

Party 2 – Sole Trader/Company Name

(**Access Point Provider**)

Version 1.0

05 August 2016

Contents

Parties

Digital Business Council

of Address

Email Address

(‘**Council’**)

Party 2 - Sole Trader/Company Name **ABN** ABN

of Address

Email Address

(‘**Access Point Provider’**)

Background

A. The Access Point Provider wishes to provide Access Point services to Clients under the Digital Business Council Limited’s eInvoicing Interoperability Framework (Framework).

B. The Framework details the procedures, standards and guidelines for the electronic exchange of Business Documents between participants under the Framework.

C. The intent of the Framework is to provide a national framework to allow the entire business community to have access to a range of competitive solutions that are able to exchange information digitally. To do this the Access Point Provider must conform to the minimum operating and technical standards required by this Agreement. While commencing with eInvoicing it is intended that the types of transactions implemented will expand over time to include other aspects of the procure to pay life cycle.

D. The Council oversees and may audit the services provided by the Access Point Provider, to ensure that they are provided and maintained in accordance with the Framework.

E. The Parties agree that the Access Point Provider is Accredited to access and adopt the Framework on the terms and conditions set out in this Agreement.

Terms and Conditions

1 Definitions and Interpretation

1.1 Definitions

For the purposes of this Agreement unless otherwise specified.

Access Point means a software messaging service which sends and receives electronic Messages and which can be implemented internally by an organisation or business or provided by an external provider to a Client.

Access Point Provider means a provider of Access Point services to a Client.

Access Point Provider Contact means the contact point appointed by the Access Point Provider and notified in writing to the Council to be the Access Point Provider’s contact for

the purposes of this Agreement and with the responsibility to fulfil the Access Point Provider's obligations under clause 7.5(b).

Accreditation means the approval to operate an Access Point service, granted by the Council to an Access Point Provider, upon committing to adhere to the standards specified under the Framework.

Accreditation Fee means the fee payable by the Access Point Provider to the Council as set by the Council and notified on the Council's Website to be considered for Accreditation under the Framework by the Council.

Agreement means this agreement between the Access Point Provider and the Council comprising the following:

(a) any Binding Implementation Practice Note issued by the Council;

(b) the paragraphs in the body of the Schedules;

(c) the clauses in the body of this Agreement;

(d) the Implementation Guide; and

(e) the Framework.

Available means with respect to an Access Point, being capable of receiving and sending electronic Messages in accordance with the Framework.

Binding Implementation Practice Note means a notification issued by the Council that outlines operational guidance on methods or practices for implementing the Framework.

Business Day means any day other than a Saturday, Sunday or public holiday in Canberra, Australian Capital Territory.

Business Hours means anytime between 9am and 5pm (local time) on a Business Day which are for the purposes of the execution of this Agreement.

Business Documents means Council endorsed documents used by the business in its day-to-day activities such as invoicing which are for the purposes of the execution of this Agreement.

Client means a business, organisation or any other entity, for which the Access Point Provider provides its Access Point services.

Confidential Information of a Party means:

(a) information, know-how, ideas, concepts and technology of a confidential nature relating to or developed in connection with the business or affairs of the Party which is disclosed to, learnt by, or which otherwise comes to the knowledge of or into the possession of the other Party;

(b) information designated by that Party as confidential; or

(c) information regarding clients, customers, employees, contractors of or other persons doing business with that Party,

but it does not include information:

(i) which is or becomes generally available in the public domain, other than through any breach of confidence;

(ii) rightfully received by the other Party from a third person who is under no obligation of confidentiality in relation to the information and who has not obtained that information either directly or indirectly as a result of a breach of any duty of confidence owed to the first Party; or

(iii) that has been independently developed by the other Party.

Contingency means any Disabling Event.

Corporations Act means the *Corporations Act 2001* (Cth).

Council means the Digital Business Council Limited which constitutes the industry representatives, representing business interests.

Council's Website means the Council's Website accessible at:

http://digitalbusinesscouncil.com.au

Defect means any characteristic that makes the whole or any part of Access Point services inoperable or inconsistent with the requirements of this Agreement including any Binding Implementation Practice Note issued by the Council, the clauses in the body of this Agreement; the Implementation Guide; the paragraphs in the body of the Schedules or the Framework.

Digital Capability Locator is a service for looking up the location of the Digital Capability Publisher for a Participant.

Digital Capability Publisher is a provider of 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 Business Documents.

Disabling Event means any:

(a) processing, communications or other failure of a technical nature;

(b) inaccessibility (total or partial) of facilities by means of which exchanges are conducted; or

(c) manifestation of industrial action, which affects, or may affect, the ability of an Access Point Provider to participate to the normal and usual extent in the electronic exchange of Business Documents.

Domain of Responsibility means an Access Point Provider's function and maintenance of its services, required for interacting within the scope of the Framework.

Effective Date means the date from which this Agreement takes effect, which is the day on which the last of the authorised representative of both Parties signs it.

Force Majeure Event means any circumstance not within the reasonable control of the affected Party, to the extent that:

(a) the circumstance cannot be avoided, prevented or remedied despite the exercise of reasonable diligence by the Party;

(b) the circumstance materially affects the ability of the Party to perform its obligations under this Agreement; and

(c) the Party has taken all reasonable precautions to avoid the effect of the circumstance on the Party's ability to perform its obligations under this Agreement and to mitigate the consequences thereof.

Framework means the Digital Business Council's Interoperability Framework which details the procedures and guidelines for the electronic exchange of Business Documents between its Participants as modified from time to time and which is accessible at:

http://digitalbusinesscouncil.com.au

GST has the meaning given to that term in the GST law.

GST Law has the meaning given to that term in the *A New Tax System (Goods and Services Tax) Act 1999* (Cth).

Harmful Code means any computer program, trojan, virus or other code which is not intended to serve a legitimate purpose and which is harmful, destructive or disabling or which assists in or enables theft, alteration, denial of service, unauthorised access to or disclosure, destruction or corruption of information, data or software.

Implementation Guide means documents published by the Council that outline and describe a set of rules and guidelines on the use of the standards.

Insolvency Event in relation to a Party (**Insolvent Party**) means the happening of any one or more of the following events:

(a) the Insolvent Party ceases, or takes steps to cease, to conduct its business in the normal manner;

(b) the Insolvent Party enters into or resolves to enter into any arrangement, composition or compromise with or assignment for the benefit of its creditors or any class of them;

(c) the Insolvent Party is unable to pay its debts when they are due or is deemed under the *Corporations Act 2001* (Cth) to be insolvent;

(d) a liquidator or provisional liquidator is appointed to the Insolvent Party or a receiver, receiver and manager, official manager, trustee or similar official is appointed over any of the assets or undertakings of the Insolvent Party;

(e) an application or order is made or a resolution is passed for the winding up of the Insolvent Party;

(f) being an individual is declared bankrupt, seeks a composition of creditors, suspends payments or in any other way is deemed to be insolvent; or

(g) any act or event analogous or having a substantially similar effect to any of the events specified in paragraphs (a) to (f) of this definition.

Key Operating Staff means Personnel directly responsible for overseeing and maintaining the services provided by an Access Point under the Framework.

Law means any law including any common law, equity, statute, regulation, proclamation, ordinance, by-law, mandatory code of conduct, writ, judgment and any award or other industrial instrument.

Loss means loss, damage, liability, charge, expense, outgoing, payment or cost of any nature or kind, including all legal and other professional costs on a full indemnity basis.

Message means an electronic message or signal sent or received by the Participants under the Framework.

Participant means Council Accredited Access Point Providers, Digital Capability Publisher and Digital Capability Locator services and the businesses, organisations and other entities who have adopted the Framework.

Party means a party to this Agreement being, individually the Digital Business Council Limited or the Access Point Provider and together referred to as the Parties.

Personal Information means:

(a) information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not; or

(b) information or a document that relates to the affairs or personal particulars of another person (such as a company or a business),

which is received or learnt by a Party from any source as a consequence of or in the performance of its rights and obligations under this Agreement.

Personnel means in respect of a Party, employees, secondees, directors, officers, contractors, professional advisers and agents of that Party, and in relation to the Access Point Provider includes such individuals of its subcontractors.

Privacy Laws means the *Privacy Act 1988* (Cth), the *Spam Act 2003* (Cth), the *Telecommunications Act 1997* (Cth), any registered Australian Privacy Principles Code that binds a Party, the Privacy Policy issued by the Council (available at: www.[insert]/privacy), and any other Laws, industry codes and policies relating to the handling of Personal Information.

Related Body Corporate has the meaning given to that term in section 9 of the *Corporations Act 2001* (Cth).

Testing Requirement means the requirements under clauses 3.1 and 5.2 as set out in more detail in Schedule 3.

Warning Note means a written notice directed to the Access Point Provider describing an issue of concern or complaint and a timeframe to rectify the issue of concern or complaint.

1.2 Interpretation

In this document:

(a) headings are for convenience only and do not affect interpretation;

(b) the singular includes the plural and vice versa;

(c) a gender includes every other gender;

(d) where a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(e) a reference to a Party to this Agreement includes the Party's successors and permitted assignees;

(f) a reference to a person includes a firm, a body corporate, an unincorporated association or an authority and vice versa;

(g) a reference to this Agreement or another document includes any variation, novation, replacement or supplement to any of them from time to time;

(h) a reference to a part, clause, annexure, exhibit, appendix or schedule is a reference to a part of, clause of, an annexure, exhibit, appendix or schedule to this Agreement and a reference to this Agreement includes any annexure, exhibit, appendix and schedule;

(i) a reference to a right or obligation of two or more persons confers that right, or imposes that obligation, as the case may be, jointly and severally;

(j) a reference to any legislation or to any provision of any legislation includes any modification or re-enactment of it, any legislative provision substituted for it and any regulations and statutory instruments issued under it;

(k) a reference to conduct includes any omission, representation, statement or undertaking, whether or not in writing;

(l) mentioning anything after includes or including does not limit what else might be included;

(m) no rule of construction applies to the disadvantage of a Party because that Party was responsible for the preparation of this document;

(n) a reference to dollars or $ is to Australian currency;

(o) all references to time are to Canberra time; and

(p) all references to accounting and financial terms have the meaning commonly given to them in accordance with the accounting principles generally accepted in Australia.

1.3 Relationship with the Framework

This Agreement refers to, and is to be read in conjunction with the Framework, published by the Council on its website at:

http://digitalbusinesscouncil.com.au

1.4 Precedence of documents

The documents comprising this Agreement must be read in the following order of precedence:

(a) Binding Implementation Practice Note;

(b) the paragraphs in the body of the Schedules;

(c) the clauses in the body of this Agreement;

(d) the Implementation Guide; and then

(e) the Framework.

2 Term of this Agreement

2.1 When agreement commences

This Agreement commences on the Effective Date which is set out in the execution page, and is the day on which the last of the duly authorised representative of both Parties has signed this Agreement.

2.2 When agreement ends

This Agreement will end according to clause 20.

3 Eligibility

3.1 Eligibility to be Accredited as an Access Point Provider under the Framework

The Access Point Provider will be eligible to obtain the Council's Accreditation to provide Access Point services and participate under the Framework as an Accredited Access Point Provider if:

(a) it successfully satisfies the Testing Requirements set out in Schedule 3 and in accordance with the processes and requirements of this Agreement and the Framework and submits to the Council the signed declaration/application as required by clause 3.4;

(b) it commits to cooperating as a Participant under the Framework by signing this Agreement;

(c) its Key Operating Staff are all fit and proper persons as demonstrated by those persons:

(i) being competent to operate an Access Point (as demonstrated by the person's knowledge, skills and experience);

(ii) having the attributes of good character, diligence, honesty, integrity and judgement;

(iii) not being disqualified by law from performing their role for the Access Point Provider; and

(iv) either having no conflict of interest in performing their role for the Access Point Provider , or if any conflict exists it will not create a material risk that the person will fail to properly perform their role for the Access Point Provider under the Framework;

and the Access Point Provider makes a declaration in accordance with clauses 3.3 and 3.4; and

(d) it pays the Accreditation Fee as set by Council from time to time.

3.2 Eligibility to Remain Accredited as an Access Point Provider under the Framework

The Access Point Provider will continue to remain Accredited to provide Access Point services under the Framework and to participate under the Framework as a Participant provided it continues to satisfy the requirements of clause 3.1.

3.3 Accreditation Process

The process an Access Point Provider must follow to obtain accreditation and become a Participant under the Framework is as follows:

(a) Step 1 Downloading the Testing Requirements from the Council's Website;

(b) Step 2 Testing its software against the Testing Requirements described in clause 3.1 and recording the results;

(c) Step 3 Uploading the test results into the Council's Website and ensure that the test results are stored in a form that can be audited by the Council in accordance with clause 17 for a period of not less than two (2) years;

(d) Step 4 Uploading the declaration providing the information required by clause 3.1(c) in the form required by clause 3.4;

(e) Step 5 Signing this Agreement and undertaking to comply with the terms of use for the application of the Council's name and logo as published on the Council's website from time to time and uploading the signed copy of this Agreement to the Council's Website;

(f) Step 6 The Council will notify the Access Point Provider with confirmation of Accreditation or will request more information; and

(g) Step 7 The Access Point Provider is Accredited once it has received a written notice of confirmation from the Council in accordance with clause 4.1.

3.4 Evidence

The Access Point Provider must when applying to the Council for Accreditation provide the Council with a declaration of self assessment in the form required by the Council's Website.

4 Assessment and Appeals

4.1 Council Assessment

The Council will assess the Access Point Provider's information provided under clause 3 against the eligibility and testing requirements in clause 3 and Schedule 3 and determine in its sole discretion whether the Access Point Provider will be admitted as an Accredited Access Point Provider under the Framework.

4.2 Appeals

If the Access Point Provider is not satisfied with the outcome of its application to obtain the Council's Accreditation, it may appeal the Council's decision in accordance with the Council's Constitution or By-Laws from time to time.

5 Testing

5.1 Access Point Provider must provide Current Test Results

(a) The Access Point Provider must, when requested by the Council, submit the current test results for its Access Point services to the Council for review covering the most recent build or configuration of the Access Point Provider's system within five (5) Business Days of the request.

(b) If unable to produce the required test results within the timeframe specified in (a) the Council may request the Access Point Provider to retest its Access Point services in accordance with the Testing Requirements to remain eligible as an Accredited Access Point Provider.

5.2 Testing requirements

The Testing Requirements with which the Access Point Provider must comply are contained in Schedule 3. These testing requirements may be updated at any time by the Council. Following an update, the Council will notify the Access Point Providers, if it determines that the changes to the testing requirements are significant enough to undertake reassessment and retesting pursuant to clauses 4 and 5 respectively.

5.3 Logical Separation of environments

The Access Point Provider must ensure that an appropriate level of logical separation is enforced between its internal applications, particularly between its testing environment and its production environment. As a minimum, the Access Point Provider must ensure that an unauthorised business document (i.e. a test version) is not accidentally or otherwise accepted into the Access Point Provider's production system.

6 Access Point Provider's Obligations

6.1 The Access Point Provider must:

(a) provide the Access Point services relevant to its role as an Access Point Provider as set out in this Agreement including, in particular, the requirements of Schedule 3 and the Framework;

(b) ensure that its Access Point services are provided and maintained in a reliable manner including as set out in Schedule 3;

(c) as far as it is possible, without violating confidentiality commitments to third parties or Privacy Laws, the Access Point Provider must make available to other Participants relevant information held by it which is needed by those Participants for providing and maintaining their services;

(d) protect its own data systems against illicit use, Harmful Code, malicious code, viruses, computer intrusions, infringements and illegal tampering of data and other comparable actions by third parties;

(e) use reasonable endeavours to avoid the transmission of any Harmful Code, viruses, time bombs, worms or similar items or any computer programming routines that may adversely affect any other Participant's computer systems;

(f) notify all relevant Participants within sixty (60) minutes if they observe disruption of service or an infrastructure failure as specified in Schedule 3 within its Domain of Responsibility which may endanger the fulfilling of agreed tasks under the Framework;

(g) if unable to fulfil its obligations under this Agreement, promptly inform the Council in writing; and

(h) ensure that it has sufficient resources for the delivery of the Access Point services and for the maintenance of its own software systems.

6.2 Disputes between Accredited Access Point Providers

Any dispute between Accredited Access Point Providers must be:

(a) resolved amicably by negotiations between the Accredited Access Point Providers, or if the Accredited Access Point Providers have not reached agreement within fifteen (15) days following notice from one Accredited Access Point Provider to the other regarding the dispute;

(b) escalated to the Council, in which case both Accredited Access Point Providers must agree on whether the decision from the Council, or from one or more technical experts appointed by the Council, will be considered binding or only advisory (as a basis for further negotiations); or

(c) when none of the other options provides a satisfactory solution within thirty (30) days following notice from one Accredited Access Point Provider to the other the parties may pursue other alternatives for resolution, including but not limited to mediation or court proceedings.

7 Access Point Interoperability

7.1 Access Point Connectivity

The Access Point Provider:

(a) must, as a part of locating the digital address of other Access Points, ensure that its Access Point is able to connect to the Digital Capability Locator and the relevant Digital Capability Publisher;

(b) if it becomes aware that one of its Clients' business identifiers are not valid notify the Client of this at the Access Point Provider's earliest convenience;

(c) must, once the digital address of the Access Point of another Access Point Provider is located, ensure that its Access Point is able to establish and maintain a Messaging connection with the other Access Point; and

(d) must ensure that its Access Point supports and conforms to any connectivity standards set out in the Implementation Guide published by the Council.

7.2 Access Point Availability

The Access Point Provider must ensure that in relation to its Access Point:

(a) the Access Point availability requirements set out in Schedule 3 are met;

(b) that it notifies all accredited Service Providers and Council of any non-availability due to any issues for a planned period of time prior to the non-availability; and

(c) if its Access Point does not receive an acknowledgement of receipt from any other Accredited Access Point it must follow the retry protocol outlined in the Implementation Guide published by the Council.

7.3 Access Point Processing

The Access Point Provider must ensure that its Access Point:

(a) adheres to the interoperability standards detailed in the Implementation Guide published by the Council; and

(b) follows the processing requirements set out in Schedule 3.

7.4 Messaging Service Infrastructure and Security Protocols

The Access Point Provider must comply with the most recent Messaging services infrastructure and security protocols as set out in the Implementation Guide published by the Council.

7.5 Problem and Error Management

(a) The Access Point Provider must comply with all applicable error management protocols and procedures set out in the Implementation Guide, including technical retry processes and procedures.

(b) If, when the Access Point of the Access Point Provider has sent another Accredited Access Point Provider a Message and a success notification is not achieved within the timeframe set out in Schedule 3 after sending the original Message and all retry protocols have been exhausted, as set out in the Implementation Guide the Access Point Provider, at its earliest convenience, must notify this issue to the Client on whose behalf the original Message was sent.

7.6 Service Support

(a) The Access Point Provider's infrastructure and support arrangements for their Access Point must meet the availability requirements set out in clause 7.2 of this Agreement.

(b) The Access Point Provider must ensure that it has a nominated Access Point Provider Contact with the Council.

7.7 Contingency and Cooperation

The Access Point Provider must cooperate with other Access Point Providers in resolving any Access Point service difficulties including due to or during a Contingency. To the extent that this cooperation does not adversely affect its own processing environment, an Access Point Provider receiving a request for assistance from another Access Point Provider may not unreasonably withhold that assistance.

8 Disconnections

8.1 Notice of Disconnection required

Before the Access Point Provider may be permitted to, or may implement, any disconnection of its connectivity or systems to its Access Point and maintain its Accreditation under the Framework, it must provide no less than fifteen (15) Business Days prior written notice to accredited Service Providers and Council of the disconnection.

8.2 Revocation of Accreditation if Notice of Disconnection not provided

Where the Access Point Provider does not provide the relevant accredited Service Providers and Council with a notice of disconnection as required by clause 8.1, the

Council may revoke the Access Point Provider's Accreditation to participate under the Framework.

9 Costs and Charges

(a) The Access Point Provider must;

(i) pay the Accreditation Fee specified in clause 3.1 (d);

(ii) bear its own development and operation costs relating to its own data systems and procedures as required to fulfil its obligations under this Agreement;

(iii) not charge the Council for any service whatsoever, unless specifically agreed in a separate agreement; and

(iv) not charge for exchanging Business Documents between Access Points.

(b) The Access Point Provider may freely and independently determine the pricing it charges to its Clients for the services it provides to a Client.

10 Goods and Services Tax (GST)

10.1 Recovery of GST

If one Party (**Supplying Party**) makes a taxable supply and the consideration for that supply does not expressly include GST, the Party that is liable to provide the GST-exclusive consideration (**Receiving Party**) must also pay an amount (**GST amount**) equal to the GST payable in respect of that supply.

10.2 Time for payment of GST amount

Subject to first receiving a tax invoice or adjustment note as appropriate, the Receiving Party must pay the GST amount when it is liable to provide the GST-exclusive consideration.

10.3 Indemnity and reimbursement payments

If one Party must indemnify or reimburse another Party (**Payee**) for any loss or expense incurred by the Payee, the required payment does not include any amount which the Payee (or an entity that is in the same GST group as the Payee) is entitled to claim as an input tax credit or would have been entitled to claim as an input tax credit had the other Party registered for GST if it was required or entitled to do so, but will be increased under clause 10.1 if the payment is consideration for a taxable supply.

10.4 Adjustment events

If an adjustment event arises in respect of a taxable supply made by a Supplying Party, the GST amount payable by the Receiving Party under clause 10.1 will be recalculated to reflect the adjustment event and a payment will be made by the Receiving Party to the Supplying Party, or by the Supplying Party to the Receiving Party, as the case requires.

10.5 Time limit on payment of the GST amount

A Receiving Party is not required to pay the GST amount referred to in clause 10.1 unless it has received a tax invoice in respect of the supply (or, if section 156-5(1) of the GST

Act applies to the supply, the periodic or progressive component of the supply) from the Supplying Party within three years and 11 months after the end of:

(a) the first calendar month in which any of the GST-exclusive consideration for the supply (or the periodic or progressive component of the supply) is provided; or

(b) if an invoice is issued prior to the provision of any of the GST-exclusive consideration for the supply (or the periodic or progressive component of the supply), the calendar month in which the invoice is issued.

11 Subcontracting

The Access Point Provider remains responsible for any Access Point services subcontracted by it.

12 Data Ownership

12.1 Message data owned by Client

The Parties acknowledge that the content of the Messages and their associated metadata is owned by the Client.

12.2 Client's permission to publish metadata

The Access Point Provider must ensure that the Client has given its acceptance to publish the Client's metadata to both the Digital Capability Publisher Provider and the Digital Capability Locator. If the registration is done by a third party and not the Access Point Provider who has the commercial arrangement with the Client, the Access Point Provider must ensure it is able to provide evidence of any transfer of responsibility.

12.3 Updates of metadata

If a Client's or a Participant's metadata is updated, the third party requesting the update must maintain an audit trail pertaining to the authorisation by the Client or Participant to carry out the update. The authorisation may be obtained by email.

13 Confidentiality and Privacy

13.1 Confidentiality Obligations

The Parties:

(a) must keep confidential any data, documents or other material that they have received from the other Party or otherwise in relation to the execution of their responsibilities and services under this Agreement which are Confidential Information;

(b) must only use or reproduce the other Party's Confidential Information for the purposes of this Agreement; and

(c) must take all steps reasonably necessary to:

(i) maintain the confidentiality of the other Party's Confidential Information;

(ii) ensure that any person who has access to Confidential Information of the other Party through it or on its behalf does not use, reproduce or

disclose that Confidential Information other than in accordance with this Agreement; and

(iii) enforce the confidentiality obligations imposed or required to be imposed by this Agreement, including diligently prosecuting at its cost any breach or threatened breach of such confidentiality obligations by a person to whom it has disclosed Confidential Information of another Party.

13.2 Disclosure of Confidential Information

Each Party who receives Confidential Information of the other Party may not disclose that Confidential Information to any person except:

(a) to its Personnel who need to know the Confidential Information for the purposes of this Agreement and subject to the receiving Party taking reasonable steps to ensure that any such Personnel are fully aware of the confidential nature of the Confidential Information of the disclosing Party before the disclosure is made;

(b) as required to be disclosed by Law or the listing rules of any stock exchange where the receiving Party's securities are listed or quoted;

(c) if the disclosing Party has given its consent to the disclosure or use; or

(d) as expressly permitted by this Agreement.

13.3 A Party may Disclose the existence of service contracts

For the avoidance of doubt, a Party may disclose information related to the existence of Access Point service contracts within their Domain of Responsibility.

13.4 Injunctive relief

In addition to other remedies, a Party may seek injunctive relief for breach or threatened breach of the other Party's obligations of confidentiality under this Agreement.

13.5 Privacy

The Parties must protect the personal data they receive, collect and process according to the requirements of the Privacy Laws and any guidelines issued by the Council.

13.6 Survival

The obligations of confidentiality and privacy in this clause 13 survive termination of this Agreement.

14 Logging

14.1 Requirement to keep logs

The Access Point Provider must log all Message activity handled by its Access Point for reporting requirements to the Council. These logs must be kept for at least two (2) years or for the period of time prescribed by any applicable Law.

14.2 Requirement to give Council access to logs

The Access Point Provider must, on request from the Council, give access to relevant data from the logs to the Council, provided the data is not subject to a duty of

confidentiality, in which case the prior written consent of the Client or other data owner must be obtained.

15 Suspension and Revocation of Services

15.1 Council may issue Warning Note

If the Access Point Provider does not fulfil its responsibilities and obligations under this Agreement (including the Framework, Implementation Guide, Schedules and Binding Implementation Note) or if fraud, spam or other misconduct by the Access Point Provider are identified, the Council may issue a Warning Note to the Access Point Provider specifying the nature of the problem or issue, the actions required to rectify the issue, the timeframe in which the Access Point Provider is to rectify the problem or issue, and the consequences of not rectifying the issue within the timeframe indicated.

15.2 Suspension

If the problem or issue is not rectified by the Access Point Provider within the timeframe and in accordance with the requirements specified in the Warning Notice the Council may suspend the Access Point Provider from participation under the Framework.

15.3 Revocation

If the problem or issue is serious or persistent and it is not rectified by the Access Point Provider within the timeframe and in accordance with the requirements specified in the Warning Notice the Council may take action under clause 20.2.

16 Liability

16.1 Mutual indemnities

Each Party (**Indemnifying Party**) indemnifies the other Party (**Indemnified Party**) and its Personnel (together **Indemnified Persons**) against all Loss suffered or incurred by the Indemnified Persons arising in connection with:

(a) any fraudulent or unlawful act or omission of the Indemnifying Party or its Personnel;

(b) any damage to real or personal property caused or contributed to by any act or omission of the Indemnifying Party or its Personnel;

(c) any breach of confidentiality and privacy obligations by the Indemnifying Party or its Personnel; or

(d) any Claim by a third Party that use of any material accordance with this Agreement infringes the Intellectual Property Rights of that third Party;

except to the extent that the Loss is directly attributable to the negligence or wrongful act or omission of the Indemnified Person.

16.2 Exclusion of Consequential Loss

(a) Subject to subclause 16.3 a Party is not liable for any Loss suffered or incurred by the other Party in connection with a breach of this Agreement by the first Party that does not arise naturally (that is, according to the usual course of

things) from that breach including loss of opportunity, income or profits (**Consequential Loss**).

(b) The Parties acknowledge that the following are not Consequential Loss:

(i) costs of assessing or remedying a Defect or a breach of this Agreement;

(ii) costs of undertaking workarounds or other steps to mitigate the effects of a Defect or breach of this Agreement;

(iii) costs of notifying, communicating or compensating Clients or other third parties affected by a Defect or a breach of this Agreement;

(iv) costs of recovering or recreating data or records which have been lost, destroyed, deleted or corrupted as a result of a Defect or breach of this Agreement; or

(v) fines or penalties resulting from any breach of Law as a result of a breach of this Agreement by the Access Point Provider.

16.3 Exceptions

The limitations and exclusions in clause 16.22 do not apply to a Party's liability for Loss suffered or incurred by the other Party in respect of:

(a) fraud or other unlawful acts;

(b) damage to real or personal property;

(c) breach of an obligation of confidentiality under this Agreement; and

(d) breach of an obligation of privacy under this Agreement.

17 Audit

On the Council's written request, the Access Point Provider must allow the Council or an independent third Party nominated by the Access Point Provider and approved by the Council (each an **Auditor**) to verify the Access Point Provider's compliance with the requirements of clauses 3, 5, 6, 7,and 8 of this Agreement in order to verify and if necessary audit the Access Point Provider's compliance with this Agreement. In relation to those audits:

(a) the Council may request audits at its discretion;

(b) the Council will not request an audit more than once in any 12 month period, unless an audit occurring in the preceding 12 month period identified a material non-conformance;

(c) the Council will give at least ten (10) Business Days' notice of any audit unless it reasonably suspects there is a serious non-compliance in which case it may require an audit on one (1) Business Day notice;

(d) where there is demonstrable cause for the audit, the Access Point Provider must reimburse the Council's reasonable costs of the audit;

(e) the Access Point Provider must provide, and must ensure that its Personnel provide, the Auditor the full records relating to the subject matter of the audit;

(f) the Access Point Provider is not required to disclose any information that:

(i) if disclosed, would result in the Access Point Provider being in breach of its confidentiality obligations to any person; or

(ii) relates to the Access Point Provider's profit margins;

(g) the Access Point Provider must provide reasonable co-operation, information and assistance to the Auditor in connection with an audit; and

(h) if a subcontractor or Related Body Corporate of the Access Point Provider is involved in the provision of the Access Point services or the performance of the Access Point Provider's other obligations under this Agreement or under the Framework, then the Access Point Provider must require that person to provide access to its applicable information consistent with this clause 17.

18 Force Majeure

(a) A Party will not be liable for any failure or delay in the performance of its obligations under this Agreement (other than any obligations in relation to business continuity, back-up or disaster recovery) to the extent that the failure or delay is caused, directly or indirectly, by a Force Majeure Event, provided:

(i) the failure or delay could not have been prevented by reasonable precautions, or could not have reasonably been circumvented by that Party by means of alternate sources, workarounds or other means;

(ii) that Party promptly advises the other Party of the details of the Force Majeure Event, and its likely effect on its obligations under this Agreement; and

(iii) that Party takes all steps reasonably necessary to recommence performance and minimise the delay caused by the Force Majeure Event.

(b) If any Force Majeure Event has the result that the Access Point Provider is not able to provide Access Point services, no fees or charges will be payable in respect of those services.

(c) If the Force Majeure Event continues for thirty (30) Business Days, the Party not affected may terminate this Agreement by giving ten (10) Business Days written notice to other Party.

19 Dispute Resolution

19.1 Dispute Notice required

If either Party considers that a dispute has arisen in connection with this Agreement (**Dispute**), it may issue a notice to the other Party, setting out reasonable details of the Dispute (**Dispute Notice**).

19.2 Good Faith First Level Discussions

After a Dispute Notice has been issued:

(a) the Parties must promptly hold good faith discussions between the Access Point Provider representative (or its nominee) and the Council representative (or its nominee), to attempt to resolve the Dispute (**First Level Discussions**); and

(b) each Party must provide the other Party with information relating to the Dispute which is appropriate in connection with its resolution.

19.3 Good Faith Second Level Discussions

If the Dispute has not been resolved within twenty (20) Business Days after the First Level Discussions started, the Parties must each nominate a senior representative who must hold good faith discussions to attempt to resolve the Dispute (**Second Level Discussions**).

19.4 Mediation

If the Dispute has not been resolved within (20) Business Days after the Second Level Discussions started (**Second Level Discussions Period**) the Dispute is by this clause submitted to mediation. The mediation must be conducted at Canberra in the Australian Capital Territory. The Institute of Arbitrators and Mediators Australia Mediation and Conciliation Rules (at the date of this Agreement) as amended by this clause 19 apply to the mediation, except where they conflict with this clause 19.

19.5 Failure to agree Mediator or Mediator's remuneration

If the Parties have not agreed upon the mediator and the mediator's remuneration within (5) Business Days after the end of the Second Level Discussions Period:

(a) the mediator is the person appointed by; and

(b) the remuneration of the mediator is the amount or rate determined by;

the Chair of the Australian Capital Territory Chapter of the Institute of Arbitrators and Mediators Australia (**Principal Appointor**) or the Principal Appointor's nominee, acting on the request of any Party to the Dispute.

19.6 Costs of Mediation

The Parties must pay the mediator's remuneration in equal shares. Each Party must pay its own costs of the mediation.

19.7 Requirement to continue to fulfil obligations

Until resolution of a Dispute, the parties will continue to perform their respective obligations under this Agreement.

19.8 Legal Proceedings not to be commenced

A Party must not commence legal proceedings other than for urgent injunctive or declaratory relief in relation to any Dispute unless the dispute resolution procedures set out in this clause 19 have been followed.

20 Termination

20.1 Termination by three month notice

This Agreement continues in force until terminated by one of the Parties giving the other Party three (3) months written notice.

20.2 Termination for Cause

(a) A Party may terminate this Agreement immediately by written notice if the other Party:

(i) commits a material breach of any of the following provisions of this Agreement that is capable of remedy, which is not remedied within twenty (20) Business Days after receipt of written notice of the breach:

(A) clause 3 (Eligibility);

(B) clause 5 (Testing);

(C) clause 6 (Access Point Provider's Obligations);

(D) clause 7 (Access Point Interoperability);

(E) clause 8 (Disconnections);

(F) clause 9 (Costs and Charges);

(G) clause 13 (Confidentiality and Privacy);

(H) clause 14 (Logging);

(I) clause 15 (Suspension and Revocation of Services);

(J) clause 16 (Liability); and

(K) clause 17 (Audit);

(ii) commits a material breach of any of the clauses set out in clause 20.2(a)(i) of this Agreement that is not capable of remedy; or

(iii) suffers an Insolvency Event;

20.3 Consequences of Termination

(a) The Parties are obliged to inform third parties that are affected by the termination of this Agreement that this Agreement has been terminated by the giving of a written notice.

(b) The Access Point Provider will immediately cease use of the Council's logo and name.

(c) If a termination notice is given, the Parties must amicably negotiate in good faith on the procedures relating to the ending of the cooperation under this Agreement, in order to avoid any unnecessary disturbances in Client relationships.

21 Notices

21.1 Form of Notice

Any demand, notice, consent, approval or other communication under this Agreement may be made or given by a Party or the solicitor for that Party provided that it:

(a) is in legible writing, in English and addressed to the intended recipient; and

(b) is signed by the sender (if an individual) or by an authorised representative of the sender; and

(c) is given to the addressee by:

(i) delivery in person; or

(ii) post to, or leaving at, that Party's address for service; or

(iii) sending by email to the Party's email address; and

(d) is regarded as being given by the sender and received by the addressee:

(i) if by delivery in person or by being left at the Party's address for service, upon delivery;

(ii) if by post, three (3) Business Days from and including the date of posting by ordinary prepaid post in respect of an address for service within the Commonwealth of Australia and twenty one (21) Business Days in respect of other any address; or

(iii) if by email, when legibly received by the addressee, with receipt being evidenced by sending;

but if the delivery or receipt occurs on a day which is not a Business Day or at a time after 5.00 pm (both the day and time being in the place of receipt) it is regarded as having been received at 9.00am on the next following Business Day.

21.2 Address for service

(a) For the purposes of this clause 21, a Party's address for service shall be:

(i) if subclause (b) does not apply, the Party's postal address, fax number or email address (if any) set out at the start of this Agreement; or

(ii) if that Party has notified the sender of a change of postal address, or changed email address, the address or email address last so notified.

(b) If the Party is a company, it shall also include its registered office.

22 Assignment

The Access Point Provider must not assign, novate or otherwise transfer any of its rights or obligations arising out of or under this Agreement to another person without the Council's prior written approval (which will not be unreasonably withheld).

23 Amendment

Any amendments to this Agreement must be in writing and will have no effect unless signed by the duly authorised representatives of the Parties.

24 Relationship of the Parties

(a) The Parties must not represent themselves, and must ensure that their officers, employees, agents and subcontractors do not represent themselves, as being an officer, employee, partner or agent of the other Party, or as otherwise able to bind or represent the other Party.

(b) This Agreement does not create a relationship of employment, agency or partnership between the Parties.

25 Governing Law and Jurisdiction

25.1 Governing Law

This Agreement will be interpreted under and is governed by the Laws of the Australian Capital Territory.

25.2 Jurisdiction

Each Party irrevocably submits to the non-exclusive jurisdiction of the courts exercising jurisdiction in the Australian Capital Territory and courts of appeal from them in respect of any proceedings arising in connection with this Agreement.

26 Counterparts

This Agreement may be executed in any number of counterparts which, when taken together, constitute one instrument.

Execution Page

EXECUTED as an Agreement on the day of 2016

EXECUTED by [Digital Business Council] in accordance with section 127(1) of the Corporations Act 2001

Signature of Director

Signature of Director / Company Secretary
(delete as applicable)

Name of Director
(Please print)

Name of Director / Company Secretary
(Please print)

EXECUTED by Party 2 - Company Name in accordance with section 127(1) of the Corporations Act 2001

Signature of Director

Signature of Director / Company Secretary
(delete as applicable)

Name of Director
(Please print)

Name of Director / Company Secretary
(Please print)

EXECUTED by Party 2 - Name of Sole Trader
trading as Party 2 - Trading Name of Sole Trader **ABN** ABN

Signature	Signature of Witness
Name (Please print)	Name of Witness

EXECUTED by the Party 2 - Partnership Name
by its partners Party 2 - Names of All Partners

Signature of Partner	Signature of Witness
Name of Partner (Please print)	Name of Witness
Signature of Partner	Signature of Witness
Name of Partner (Please print)	Name of Witness
Signature of Partner	Signature of Witness
Name of Partner (Please print)	Name of Witness

Schedule 1: Access Point Provider Accreditation Process

Described below are the steps a candidate Service Provider must follow to obtain the Digital Business Council's (Council) accreditation. It should be noted that the testing required for this process is essentially a 'self-testing' exercise that is expected to be conducted by the candidate Service Provider. The candidate Service Provider is expected to store and upload the test results to the Council's website for review and assessment. Outlined below is a detailed description of each step a potential Service Provider needs to perform/undergo to be accredited by the Council.

Step 1 - Download the testing resources from the Council's website.

The candidate Service Provider must download all the relevant testing resources published on the Council's website. These documents will outline the testing requirements and instructions for recording the test results.

Step 2 - Test the solution against the testing requirements and record test results.

The necessary test cases must be developed by the candidate Service Provider on the basis of the test assertions provided. The candidate Service Provider is expected to 'self-test' their solution thoroughly against the test assertions. The candidate Service Provider will be expected to conduct testing exercises with testing partners (i.e. other Service Providers) and these testing partners will be determined by the Council (based on a roster).

Step 3 - Upload the test results, fit and proper person's declaration and the agreement(s) to the Council's website.

Upon the completion of the 'self-testing' exercise of its solution and recording the test results in the required format, the candidate Service Provider is required to upload the test results to the Council's website (as per the instructions provided on the website). The candidate Service Provider must also sign and upload the relevant agreement(s) and the fit and proper person's declaration (as required by the relevant clause(s) in the Service Provider agreement(s)).

Step 4 - Notification by the Council.

The Council will provide a notification to the candidate Service Provider with either a confirmation of successful accreditation or a request for more information following its assessment of the candidate Service Provider's application.

Schedule 2: Service Level Agreements

Providers are encouraged to indicate their service levels for information purposes. Providers can choose to provide from one of the three levels service i.e. Bronze, Silver, or Gold. The following tables outline the examples of service level requirements within each tier of service.

No.	Service Level	Description	Bronze Standard	Silver Standard	Gold Standard
1.	Availability.	AP Availability.	98.5% (06:00 to 21:00) 94.0% (remaining period)	98.5% (all day) 94.0% (remaining period)	99.95% (7 days per week)
2.	Response Times.	Maximum AP message processing response time.	(120) seconds	(20) seconds	(4) seconds
3.	AP Provider Reporting of down time to Council.	Minimum down time required to be reported to Council (in aggregated monthly report).	(4) hours	(1) hour	(5) minutes
4.	Incident Response.	Response time for incidents.	(3) business days	(1) working day	(1) hour (at any time of day)
5.	Incident resolution time	Monthly report of resolution time of	n/a	n/a	(1) report per

No.	Service Level	Description	Bronze Standard	Silver Standard	Gold Standard
	reporting.	incidents (open and closed).			month
6.	Critical resolution time.	Maximum threshold for incident resolution.	(60) business days	(30) business days	(2) working days
7.	Additional service levels	Adherence to the recommended service levels.	None	None	All additional service levels.

The Access Point Provider can choose to provide from one of the three levels service i.e. Bronze, Silver, or Gold.

The following tables outline the service level requirements within each tier of service.

Access Point Service Levels (Bronze Standard)

No	Service	Description	Clause	Requirement	Notes
1.	Availability.	AP Availability.	7.2(a)	1. APs exposed to other APs must be available on average: • 98.5% of the time from Monday to Friday from 06:00 to 21:00 (AEST/AEDST); and • 94.0% of the remaining period.	
2.	Response Times.	AP Response Time.	7.2 (c) 7.5 (b)	A receiving AP must send a receipt of acknowledgement to the sending AP within a maximum of one hundred and twenty (120) seconds after having received the message.	
3.	Reporting.	AP Provider Reporting.	n/a	1. In the case of a major system failure causing a more than four (4) hour down time, the Council must be notified by the AP Provider. 2. AP Providers are required to provide documentation on service levels on a monthly basis to the Council.	
4.	Incident. Response.	Response time for reported incidents.	n/a	1. Any incident reported to the AP Provider Contact must be responded to within three (3) Business Days. 2. AP Provider must maintain a mailing list for subscription to the service messages (e.g. service windows).	

No	Service	Description	Clause	Requirement	Notes
5.	Incident resolution time reporting.	To ensure the capability of the provider is mature.	n/a	The Council must be provided with a list of open and closed incidents that impact service operation and the number of days each incident has been open or, where closed, the number of days taken to resolve it. Data must be aggregated and/or anonymous so as not to identify a particular client or customer.	This would be only to check the below requirement.
6.	Incident resolution time.	Maximum threshold for incident resolution to maintain status.	n/a	An incident's resolution time must not exceed (50) business days in the Incident resolution time report or Bronze status will be revoked by the Council and the provider have accreditation revoked.	This check could be automated in an upload of this data.

Exceptions

An AP Provider does not have to fulfil the service levels (Bronze Standard) in the following situations:

1. The AP Provider is under a denial of service (DoS) attack; or

2. Special conditions apply and the Council has approved lowering the service levels for a specific time period and under specific conditions.

Regardless of the situation, the AP Provider must always document the reasons for not fulfilling the service levels.

Access Point Service Levels (Silver Standard)

No.	Service	Description	Clause	Requirement	Notes
1.	Availability	AP Availability	7.2(a)	1. APs exposed to other APs must be available on average: • 98.5% of the time from Monday to Friday; and • 94.0% of the remaining period.	The figures used in the requirement for this service are for illustration purposes only.
2.	Response Times	AP Response Time.	7.2 (c) 7.5 (b)	1. A receiving AP must send a receipt of acknowledgement to the sending AP within a maximum of twenty (20) seconds after having received the message.	The figures used in the requirement for this service are for illustration purposes only.
3.	Reporting	AP Provider Reporting.	n/a	1. In the case of a major system failure causing a more than one (1) hour down time, the Council must be notified by the AP Provider. 2. AP Providers are required to provide documentation on service levels on a monthly basis to the Council.	
4.	Incident Response	Response time for reported incidents.	n/a	1. Any incident reported to the AP Provider Contact must be responded to within one (1) working day. 2. AP Provider must maintain a mailing list for subscription to the service messages (e.g. service windows)	The figures used in the minimum requirement for this service are for illustration purposes only.

No.	Service	Description	Clause	Requirement	Notes
5.	Incident resolution time reporting.	To ensure the capability of the provider is mature.	n/a	The Council must be provided with a list of open and closed incidents that impact service operation and the number of days each incident has been open or, where closed, the number of days taken to resolve it. Data must be aggregated and/or anonymous so as not to identify a particular client or customer.	This would be only to check the below requirement.
6.	Incident resolution time.	Maximum threshold for incident resolution to maintain status.	n/a	An incident's resolution time must not exceed 30 business days in the Incident resolution time report or Silver status will be revoked by the Council and the provider downgraded to Bronze status.	This check could be automated in an upload of this data.

Exceptions

An AP Provider does not have to fulfil the service levels (Silver Standard) in the following situations:

1. The AP Provider is under a denial of service (DoS) attack; or

2. Special conditions apply and the Council has approved lowering the service levels for a specific time period and under specific conditions.

Regardless of the situation, the AP Provider must always document the reasons for not fulfilling the service levels.

Access Point Service Levels (Gold Standard)

No.	Service	Description	Clause	Requirement	Notes
1.	Availability	AP Availability	7.2(a)	1. APs exposed to other APs must be available on average: • 99.95% of the time (7 days per week).	The figures used in the requirement for this service are for illustration purposes only.
2.	Response Times	AP Response Time	7.2 (c) 7.5 (b)	1. A receiving AP must send a receipt of acknowledgement to the sending AP within a maximum of four (4) seconds after having received the message.	The figures used in the requirement for this service are for illustration purposes only.
3.	Reporting	AP Provider Reporting	n/a	1. In the case of a major system failure causing a more than five (5) minutes down time, the Council must be notified by the AP Provider. 2. AP Providers are required to provide documentation on service levels on a monthly basis to the Council.	
4.	Incident Response	Response time for reported incidents	n/a	1. Any incident reported to the AP Provider Contact must be responded to within fifteen (15) minutes. 2. AP Provider must maintain a mailing list	The figures used in the minimum requirement for this service are for illustration purposes only.

No.	Service	Description	Clause	Requirement	Notes
				for subscription to the service messages (e.g. service windows).	
5.	Additional Service Levels.	Mandatory requirements for Gold.	n/a	All recommended Access Point additional service levels must be implemented.	
6.	Incident resolution time reporting.	To ensure the capability of the provider is mature.	n/a	The Council must be provided with a list of open and closed incidents that impact service operation and the number of days each incident has been open or, where closed, the number of days taken to resolve it. Data must be aggregated and/or anonymous so as not to identify a particular client or customer.	This would be only to check the below requirement.
7.	Incident resolution time.	Maximum threshold for incident resolution to maintain status.	n/a	An incident's resolution time must not exceed 2 working days in the Incident resolution time report or Gold status will be revoked by the Council and the provider downgraded to Silver status.	This check could be automated in an upload of this data.

Exceptions

An AP Provider does not have to fulfil the service levels (Gold Standard) in the following situations:

1. The AP Provider is under a denial of service (DoS) attack; or

2. Special conditions apply and the Council has approved lowering the service levels for a specific time period and under specific conditions.

Regardless of the situation, the AP Provider must always document the reasons for not fulfilling the service levels.

Access Point Additional Services

This is a list of additional services that an Access Point (AP) Provider could provide in additional to the services it offers. These should appear on the AP Provider's 'profile page/section' on the Council's website.

No.	Service	Description	Clause	Requirement	Notes
1.	BCP	Business Continuity Plan.	n/a	There should be an option for the AP Provider to list its ability of providing a Business Continuity Plan whilst creating/updating their profile on the Council's website.	This is an additional service that an AP Provider can choose to deliver and hence should be able to be displayed on the Provider's profile on the Council's website.
2.	DRP	Disaster Recovery Plan.	n/a	There should be an option for the DCP Provider to list its ability of providing a 'Disaster Recovery Plan' whilst creating/updating their profile on the Council's website.	This is an additional service that an AP Provider can choose to deliver and hence should be able to be displayed on the Provider's profile on the Council's website.
3.	Disconnections Notice.	This is a disconnection notice provided to the Council.	8	There should be an option for the AP Provider to list its ability to provide a 'disconnection notice' on its	Disconnection notice is the timeframe given by an AP Provider to its Client prior to disconnecting its services. E.g.

No.	Service	Description	Clause	Requirement	Notes
				profile on the Council's website.	'Disconnection notice = 20 business days'.
4.	Known Error Database.	A database containing all incidents or problems documenting the root cause and possible workaround(s) available to its clients.	n/a	There should be an option for an AP Provider to list its ability of providing a Known Error Database (that also contains a list of workarounds) whilst creating/updating their profile on the Council's website.	It is not envisaged this would be available publicly, but only to the clients of the Service Provider.
5.	Incident/Problem Database.	A database containing all incidents and/or problems available to its clients.	n/a	There should be an option for the AP Provider to list its ability of providing a Problem/Incident database whilst creating/updating their profile on the Council's website.	It is not envisaged that this would be available publicly, but only to the clients of the Service Provider.
6.	Performance Dashboard.	A public facing web page containing performance of the service against the Council's service levels.	n/a	There should be an option for the AP Provider to list its ability of providing a performance dashboard	

No.	Service	Description	Clause	Requirement	Notes
				whilst creating/updating its profile on the Council's website.	
7.	User Acceptance Test (UAT) environment.	An environment where dummy message exchanges can be simulated by a client's software or for use by another access point.	n/a	There should be an option for the DCP Provider to list its ability of providing a UAT environment whilst creating/updating their profile on the Council's website.	

Schedule 3: Access Point Test Assertions

This schedule describes the test assertions for the Digital Business Council's (Council) AS4 profile that has been adopted for use by Access Points acting as service providers under the Council's Interoperability Framework.

More specifically, the AS4 profile is the AS4 usage profile defined by the Technical Working Group based on the AS4 Profile of ebMS 3.0 Version 1.0 OASIS Standard. AS4 itself is based on other standards, in particular on OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features OASIS Standard, which in turn is based on various Web Services specifications. The purpose of these test assertions is to focus on what is expected from the implementation.

The key terms used in this test assertion description are taken from the respective implementation guides. The intended audience are Access Point service providers engaged in verifying conformance to the Council's ebXML Messaging Services v3.0 AS4 Profile.

Entity	Description
Message Service Handler (MSH)	An entity that is able to generate and/or process Council's AS4 messages.
Producer	An entity (e.g. application) that interacts with a sending MSH to initiate the sending of a User Message.
Consumer	An entity that interacts with a receiving MSH to consume data from a received User Message.

Messaging Model

Business applications or middleware, acting as a Producer, submit message content and metadata to the sending MSH, which packages this content and sends it to the receiving MSH of the business partner, which in turn delivers the User Message to another business applications or middleware that consumes the User Message content and metadata.

Definitions

Term	Description
User Message	A message that contains a User Message unit. It allows transmitting data interpreted by a Consumer.
Signal Message	A message that contains a Signal Message unit. It allows transmitting data interpreted by a MSH (as a signal).
MEP (Message Exchange Pattern)	An agreement between sending and receiving MSHs. Some aspects of MEPs supported in the messaging layer include: ➢ Specifying the correlation between messages sent and received in the message header. ➢ Message binding to the underlying transfer protocol. One MEP is defined in this specification, not exclusive of others: ➢ The One-Way MEP, which governs the exchange of a single, User Message Unit unrelated to other User Messages. Its label is 'oneway'.
PMode (Processing Mode)	The contextual information that governs the processing of a particular message (thus is basically a set of configuration parameters).

Abbreviations

Abbreviation	Description
SMSH	A MSH in the sending role.
RMSH	A MSH in the receiving role.

Notes

- Test assertions not related to the AS4 protocol and those relating to the Digital Capability Publisher, are published in separate documents.
- For details on MSH's configuration, please refer to the Access Point Implementation Guide which is available on the Council's website. When used, configurations are described in the following test assertions as:

Configuration	PMode parameters
SMSH and RMSH are configured to exchange AS4 messages according to the Council's AS4 profile.	PModes are set according to the Access Point Implementation Guide.
SMSH and RMSH are configured to exchange AS4 messages: One-Way/Push MEP.	➢ PMode[1].MEP: set to One-way ➢ PMODE[1].MEPBinding: set to Push

- In order to test some requirements, MSHs are sometimes 'misconfigured' or 'simulated' to produce AS4 messages that do not conform to the Council's AS4 profile. This can also be achieved by intercepting the messages and altering them before they reach their destination (e.g. by using SOAP UI). More information can be found in the following sources:

Council's AS4 Profile Implementation Guide	http://digitalbusinesscouncil.com.au/software-and-service-providers
Council's eInvoicing Implementation Guide	http://digitalbusinesscouncil.com.au/software-and-service-providers
[EBMS v3.0]	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf
[AS4]	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf
[XML 1.0] specification	http://www.w3.org/TR/xml

Access Point Test Assertions

TA Id	DBC_TA01
Requirement	The AS4 ebHandler Conformance Profile is the AS4 conformance profile that provides support for sending and receiving roles using Push channel bindings. Support is required for the following Message Exchange Patterns: ➢ One-Way/Push ➢ PMode.MEP: support required
Target	One-Way/Push MEP
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the Council's AS4 profile: One-Way/Push MEP. ➢ SMSH sends an AS4 User Message to the RMSH.
Expected Result	The RMSH returns an eb:Receipt. For further information please refer to sections 7.2.1, 10.3 and 10.3.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink will be inserted before this document is published>>
Prescription Level	Mandatory
Tag	Message exchange Pattern, One-Way/Push.
Variable	N/A

TA Id	DBC_TA02
Requirement	Both UserMessage/PartyInfo/From and UserMessage/PartyInfo/To must NOT include more than one PartyId element.
Target	User Message single exchange parties.
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ SMSH and RMSH exchange several AS4 user messages.
Expected Result	Each exchanged AS4 message contains single ORIGIN and DESTINATION PartyId element. For further information please refer to sections 10.2 and 10.2.1 in the Access

TA Id	DBC_TA02
	Point Implementation Guide published on the Council's website. <<relevant hyperlink will be inserted before this document is published>>
Prescription Level	Mandatory
Tag	User Message, party info
Variable	ORIGIN: XML element Messaging/UserMessage/PartyInfo/From DESTINATION: XML element Messaging/UserMessage/PartyInfo/To

TA Id	DBC_TA03
Requirement	Note: This test assertion is created to verify that non compressed payloads (in case it happens) are also processed and delivered to the Consumer. Due to the mandatory use of AS4 compression, XML Payloads are exchanged as compressed binary data.
Target	Payload compression
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ SMSH is simulated to produce 'uncompressed' payloads. ➢ SMSH sends the AS4 message with 'uncompressed' payload to the RMSH.
Expected Result	The RMSH returns an eb:Receipt and delivers the message to the Consumer. For further information please refer to sections 10.3 and 10.3.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink will be inserted before this document is published>>
Prescription Level	Mandatory
Tag	Payload, compression
Variable	N/A

TA Id	DBC_TA04
Requirement	Due to the mandatory use of AS4 compression, XML Payloads are exchanged

TA Id	DBC_TA04
	as compressed binary data, which is carried in separate MIME parts and not in the SOAP body. Therefore, AS4 messages based on this profile always have an empty SOAP Body.
Target	Payload location
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ Producer submits a message with metadata information and an XML payload to the SMSH. ➢ SMSH generates the AS4 message to send to the RMSH.
Expected Result	In the AS4 message created by the SMSH, the compressed payload is carried in a separate MIME part and the SOAP body is empty. For further information please refer to section 7.2.3 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>> and section 5.1.1 in: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf
Prescription Level	Mandatory
Tag	Payload packaging
Variable	N/A

TA Id	DBC_TA05
Requirement	Due to the mandatory use of AS4 compression, XML Payloads are exchanged as compressed binary data, which is carried in separate MIME parts and not in the SOAP body. Therefore, AS4 messages based on this profile always have an empty SOAP Body. and; A single AS4 UserMessage MUST reference, via the PayloadInfo header, a single structured business document and may reference one or more other

TA Id	DBC_TA05
	(structured or unstructured) payload parts. The business document is considered the 'leading' payload part for business processing.
Target	Payload location
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile (One-Way/Push MEP). ➢ Producer submits a message to the SMSH with metadata information, an XML payload (leading business document) and other payloads (XML and non XML).
Expected Result	In the AS4 message created by the SMSH, the compressed payloads are carried in separate MIME parts and the SOAP body is empty. For further information please refer to sections 7.2.3, 10.2 and 10.2.1 the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>> and section 5.1.1 in: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf
Prescription Level	Mandatory
Tag	Payload packaging
Variable	N/A

TA Id	DBC_TA06
Requirement	A single AS4 UserMessage must reference via the PayloadInfo header, a single structured business document and may reference one or more other (structured or unstructured) payload parts. The business document is considered the 'leading' payload part for business processing. Any payload parts other than the business document are not to be processed in isolation but only as adjuncts to the business document.
Target	Payload processing
Prerequisite	➢ DBC_TA05

TA Id	DBC_TA06
	➢ SMSH sends the AS4 message to the RMSH
Expected Result	The RMSH successfully processes the AS4 message and sends an eb:Receipt to the SMSH. For further information please refer to sections 7.2.3, 10.3 and 10.3.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>> and section 5.1.1 in: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf
Prescription Level	Mandatory
Tag	Payload packaging
Variable	N/A

TA Id	DBC_TA07
Requirement	A single AS4 UserMessage must reference via the PayloadInfo header, a single structured business document and may reference one or more other (structured or unstructured) payload parts. The business document is considered the 'leading' payload part for business processing. Any payload parts other than the business document are not to be processed in isolation but only as adjuncts to the business document.
Target	Payload processing
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ SMSH is simulated to send an AS4 message to the RMSH with non XML payloads and without a leading business document payload. ➢ The SMSH sends the AS4 UserMessage to the RMSH.
Expected Result	The RMSH sends back a synchronous eb:Error response. For further information please refer to sections 7.2.3, 10.4 and 10.4.1 in the

TA Id	DBC_TA07
	Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>> and section 5.1.1 in: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf
Prescription Level	Mandatory
Tag	Payload packaging
Variable	N/A

TA Id	DBC_TA08
Requirement	The ebMS3 mechanism of supporting 'external' payloads via hyperlink references (as mentioned in section 5.2.2.12 of the ebMS3 Core Specification) must not be used. For further information please refer to the ebMS v3.0 core specification: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf
Target	Payload location
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push ➢ SMSH is simulated to send an AS4 UserMessage with a payload hyperlink reference.
Expected Result	The RMSH sends back a synchronous eb:Error response. For further information please refer to sections 10.4 and 10.4.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription Level	Mandatory
Tag	Payload reference
Variable	N/A

TA Id	DBC_TA09
Requirement	This profile requires the use of the AS4 Reception Awareness feature. This feature provides a built-in Retry mechanism that can help overcome temporary network or other issues and detection of messages duplicates. ➢ The parameter PMode[1].ReceptionAwareness must be set to true. ➢ The parameter PMode[1].ReceptionAwareness.Retry must be set to true. ➢ The parameter PMode[1]ReceptionAwareness.DuplicateDetection must be set to true. Note: The parameters PMode[1].ReceptionAwareness.Retry.Parameters and related PMode[1].ReceptionAwareness.DuplicateDetection.Parameters are set of parameters for configuring retries and duplication detection.
Target	Message integrity
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ Simulate the RMSH to not send receipts (can be done my intercepting the receipts e.g. using SOAP UI). ➢ SMSH attempts to resend the AS4 UserMessage to the RMSH.
Expected Result	The SMSH tries to resend the AS4 UserMessage to the RMSH. For further information please refer to the Access Point Implementation Guide (Appendix A: PMode Parameters) published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription Level	Mandatory
Tag	Reception Awareness
Variable	N/A

TA Id	DBC_TA10
Requirement	This profile requires the use of the AS4 Reception Awareness feature. This feature provides a built-in Retry mechanism that can help overcome

TA Id	DBC_TA10
	temporary network or other issues and detection of message duplicates. The parameters PMode[1].ReceptionAwareness.Retry.Parameters and related PMode[1].ReceptionAwareness.DuplicateDetection.Parameters are set of parameters used in configuring retries and duplicate detection. **Detection duplicate parameters are:** maxsize=10Mb; checkwindow=7D Maximum log size is 10Mb for checking. Duplicate check window is guaranteed of seven (7) days minimum. **Retry parameters are:** maxretries=3; period=120000 Period is two (2) minutes which corresponds to the lowest tier (bronze) SLA value for response.
Target	Message reliability
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ Simulate the RMSH to not send receipts (can be done my intercepting the receipts using SOAP UI). ➢ SMSH tries to resend (retry) the AS4 UserMessage to the RMSH. ➢ Before a TIME_OUT is reached the network connection is restored (i.e. RMSH is able to send a receipt).
Expected Result	The RMSH sends back an eb:Receipt to the SMSH and delivers only one user message to the Consumer and the SMSH stops resending the original AS4 UserMessage. For further information please refer to appendix A: PMode Parameters and sections 10.3 and 10.3.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription	Mandatory

TA Id	DBC_TA10
Level	
Tag	Reception Awareness
Variable	TIME_OUT: deadline (in terms of time or number of retries) allocated for resending messages.

TA Id	DBC_TA11
Requirement	The parameter PMode[1].ErrorHandling.Report.SenderErrorsTo MUST NOT be set.
Target	Message reliability
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push
Expected Result	PMode parameter 'PMode[1].ErrorHandling.Report.SenderErrorsTo' is not set. For further information please refer to section 2.1.3.4 in the following specification: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf and; Access Point Implementation Guide (Appendix A: PMode Parameters) published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription Level	Mandatory
Tag	Error report
Variable	N/A

TA Id	DBC_TA12
Requirement	Reception awareness errors generated by the Sender MUST be reported to the submitting application. ➢ The parameter

TA Id	DBC_TA12
	PMode[1].Errorhandling.Report.MissingReceiptNotifyProducer must be set to true.
Target	Message reliability
Prerequisite	➢ DBC_TA09 ➢ TIME_OUT for resending the messages is reached.
Expected Result	The SMSH reports an error (message delivery failure) to the message Producer. For further information please refer to Appendix A: PMode Parameters and section 10 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>> and; sections 2.1.3.4 and 5.2.2 in the following specification; http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf
Prescription Level	Mandatory
Tag	Reception Awareness
Variable	TIME_OUT: deadline (in terms of time or number of retries) allocated for resending messages.

TA Id	DBC_TA13
Requirement	Appendix F (F.2.5.3) in the core ebMS v3.0 specification defines a server test feature that allows an organization to 'Ping' a communication partner. The feature is based on messages with the values of: UserMessage/CollaborationInfo/Service set to http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service UserMessage/CollaborationInfo/Action set to http://docs.oasis-

TA Id	DBC_TA13
	open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test This feature must be supported so that the business partners can perform a basic test of the communication configuration (including security at network, transport and message layer, and reliability) in any environment, including the production environment. This functionality may be supported as a built-in feature of the AS4 product. If not, a PMode MUST be configured with these values.
Target	Test service
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ Producer submits a 'ping' message with metadata information to the SMSH (to 'ping' the Consumer).
Expected Result	The SMSH generates an AS4 message with values and sends it to the RMSH: UserMessage/CollaborationInfo/Service set to http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service UserMessage/CollaborationInfo/Action set to http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test
Prescription Level	Mandatory
Tag	Ping message
Variable	N/A

TA Id	DBC_TA13
Requirement	The AS4 product must be configured so that messages with these values (Service/Test) are not delivered to any business application.
Target	Test service
Prerequisite	➢ DBC_TA12 ➢ The Consumer is reachable.
Expected Result	The RMSH sends back a receipt within a HTTP response with status code 204 and the Consumer does not receive any message.

TA Id	DBC_TA13
Prescription Level	Mandatory
Tag	Ping message
Variable	N/A

TA Id	DBC_TA14
Requirement	The value for this element must be copied from the Digital Capability Publisher values when using dynamic discovery. PMode[1].BusinessInfo.Service
Target	Business Discovery
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ SMSH performs dynamic discovery to connect and send a user message to the RMSH.
Expected Result	The value for PMode[1].BusinessInfo.Service is copied from the Digital Capability Publisher. For further information please refer to section 7.2.10.3 and Appendix A: PMode Parameters in the Access Point Implementation Guide on the Council's website. <<relevant hyperlink(s) to be inserted before this document is published>>
Prescription Level	Mandatory
Tag	Business Info
Variable	N/A

TA Id	DBC_TA15
Requirement	The value for this element is copied from the Digital Capability Publisher values when using dynamic discovery. PMode[1].BusinessInfo.Action
Target	Business Discovery
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages

TA Id	DBC_TA15
	according to the DBC AS4 profile: One-Way/Push. ➢ SMSH performs dynamic discovery to connect and send a user message to the RMSH.
Expected Result	The value for PMode[1].BusinessInfo.Action is copied from the Digital Capability Publisher. For further information please refer to section 7.2.10.3 and Appendix A: PMode Parameters in the Access Point Implementation Guide on the Council's website. <<relevant hyperlink(s) to be inserted before this document is published>>
Prescription Level	Mandatory
Tag	Business Info
Variable	N/A

TA Id	DBC_ TA16
Requirement	A compliant product MUST allow the Producer, when submitting messages, to set values for MessageID, RefToMessageID and ConversationId (to support correlation).
Target	User Message exchange parameters
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ Producer submits a Message including metadata information and payload to the SMSH with setting message parameters: MessageId, RefToMessageId and ConversationId.
Expected Result	The SMSH returns a successful submission notification and the AS4 Message generated by the SMSH contains the same parameter values set by the producer. For further information please refer to sections 7.2.1 and 10.2.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>

TA Id	DBC_ TA16
Prescription Level	Mandatory
Tag	User Message
Variable	MessageId: XML element Messaging/UserMessage/MessageInfo/MessageId RefToMessageId: XML element Messaging/UserMessage/MessageInfo/RefToMessageId ConversationId: XML element Messaging/UserMessage/CollaborationInfo/ConversationId

TA Id	DBC_TA17
Requirement	Section 5.1.1 of the ebMS3 Core Specification: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf requires implementations to process both non-multipart (simple SOAP) messages and multipart (SOAP-with-attachments) messages. This is a requirement for the AS4 ebHandler Conformance Profile.
Target	AS4 Message Format
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ SMSH sends an AS4 message (UserMessage with payload) to the RMSH.
Expected Result	The RMSH sends an eb:Receipt to the SMSH. For further information please refer to section 10.3.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription Level	Mandatory

TA Id	DBC_TA17
Tag	Message format, Message packaging, SOAP-with-attachments
Variable	N/A

TA Id	DBC_TA18
Requirement	Section 5.1.1 of the ebMS3 Core Specification: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf requires implementations to process both non-multipart (simple SOAP) messages and multipart (SOAP-with-attachments) messages. This is a requirement for the AS4 ebHandler Conformance Profile.
Target	AS4 Message Format
Prerequisite	➢ DBC_TA17
Expected Result	The SMSH sends a success notification to the Producer
Prescription Level	Mandatory
Tag	Message format, simple SOAP
Variable	N/A

TA Id	DBC_TA19
Requirement	Due to the mandatory use of AS4 compression, XML Payloads are exchanged as compressed binary data.
Target	Payload compression
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ Producer submits a Message with metadata information and XML payload to the SMSH.
Expected Result	This generates an AS4 message with a gzip compressed payload. For further information please refer to section 10.2.1 the Access Point

TA Id	DBC_TA19
	Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>> and section 3.1 in: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf
Prescription Level	Mandatory
Tag	Payload compression
Variable	N/A

TA Id	DBC_TA20
Requirement	The PartInfo element in the message header that relates to the compressed message part, must have a Property element with @name = 'CompressionType'. The content type of the compressed attachment must be 'application/gzip'.
Target	Payload compression
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ Producer submits a Message with metadata information and payload to the SMSH.
Expected Result	In the AS4 message generated by the SMSH, a property element with name 'CompressionType' and value set to 'application/gzip' is present. For further information please refer to section 10.2.1 the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>> and section 3.1 in: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf
Prescription	Mandatory

TA Id	DBC_TA20
Level	
Tag	Payload compression, compression type
Variable	N/A

TA Id	DBC_TA21
Requirement	Packaging requirement: ➢ A PartInfo/PartProperties/Property/@name = 'MimeType' value is required to identify the MIME type of the payload before compression was applied.
Target	Payload compression
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ Producer submits a message to the SMSH with payload (ex: XML document) and metadata information including a property element with name 'MimeType' and value (application/xml).
Expected Result	The SMSH generates an AS4 message with the property 'MimeType' present and set to the value specified by the producer (application/xml). For further information please refer to section 10.2.1 the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>> and section 3.1 in: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf
Prescription Level	Mandatory
Tag	Payload compression, Mime Type
Variable	N/A

TA Id	DBC_TA22

TA Id	DBC_TA22
Requirement	Packaging requirement: ➢ A PartInfo/PartProperties/Property/@name = 'MimeType' value is required to identify the MIME type of the payload before compression was applied.
Target	Payload compression
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ The SMSH is simulated to send an AS4 message **without** property 'MimeType' present to the RMSH.
Expected Result	The RMSH sends a synchronous ebMS error message. For further information please refer to sections 10.4 and 10.4.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>> and section 3.1 in: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf
Prescription Level	Mandatory
Tag	Payload compression, Mime Type
Variable	N/A

TA Id	DBC_TA23
Requirement	Packaging requirement: ➢ For XML payloads, a PartInfo/PartProperties/Property/@name = 'CharaterSet' value is recommended to identify the character set of the payload before compression was applied. The value of this property MUST conform to the values defined in section 4.3.3 of (XML 1.0) http://www.w3.org/TR/xml/
Target	Payload compression

TA Id	DBC_TA23
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ Producer submits a message to the SMSH with XML (UTF-16) payload and metadata information including payload CharacterSet info.
Expected Result	The SMSH generates an AS4 message with the property 'CharacterSet' present and set to the value 'UTF-16'. For further information please refer to section 3.1 in: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf and section 4.3.3 in: http://www.w3.org/TR/xml/#sec-references
Prescription Level	Mandatory
Tag	Payload compression, CharacterSet
Variable	N/A

TA Id	DBC_TA24
Requirement	Packaging requirement: ➢ For XML payloads, a PartInfo/PartProperties/Property/@name = 'CharaterSet' value is recommended to identify the character set of the payload before compression was applied. The value of this property MUST conform to the values defined in section 4.3.3 of (XML 1.0). http://www.w3.org/TR/xml/
Target	Payload compression
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ Producer submits a message to the SMSH with XML (UTF-8) payload and the metadata information including payload CharacterSet info.
Expected Result	The SMSH generates an AS4 message with the property 'CharacterSet' present and set to the value 'UTF-8'

TA Id	DBC_TA24
Prescription Level	Mandatory
Tag	Payload compression, CharacterSet
Variable	N/A

TA Id	DBC_TA25
Requirement	Packaging requirement: ➢ For XML payloads, a PartInfo/PartProperties/Property/@name = 'CharaterSet' value is recommended to identify the character set of the payload before compression was applied. The value of this property MUST conform to the values defined in section 4.3.3 of (XML 1.0). http://www.w3.org/TR/xml/ and; https://issues.oasis-open.org/browse/EBXMLMSG-87 and; https://issues.oasis-open.org/browse/EBXMLMSG-88
Target	Payload compression
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ SMSH is simulated to send an AS4 message with property element 'CharaterSet' set to value not conforming to section 4.3.3 of (XML 1.0) (example '!utf*'). ➢ The SMSH sends the AS4 message to the RMSH.
Predicate	The RMSH returns a synchronous ebMS error message. For further information please refer to sections 10.4 and 10.4.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription Level	Mandatory

TA Id	DBC_TA25
Tag	Payload compression, CharacterSet
Variable	N/A

TA Id	DBC_TA26
Requirement	In case of an error during decompression, the following error MUST be used: Code = EBMS:0303, short description = Decompression failure, Severity = Failure, Category = Communication Error Handling For the error handling this profile specifies that errors must be reported and transmitted synchronously to the Sender and should be reported to the Consumer. ➢ The parameter PMode[1].ErrorHandling.Report. AsResponse must be set to the value_true.
Target	Message compression
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ SMSH is simulated to send an AS4 User Message with compressed but damaged payloads. ➢ The SMSH sends the AS4 User Message to the RMSH.
Expected Result	The RMSH sends back a synchronous error response to the Consumer with error code: Code = ‘EBMS: 0303’, Short description = ‘DecompressionFailure’, Severity = ‘Failure’, Category = ‘Communication’. For further information please refer to sections 7.2.10.4, 10.4 and 10.4.1 in the Access Point Implementation Guide published on the Council’s website. <<relevant hyperlink to be inserted before this document is published>> And 5.2.2 in:

TA Id	DBC_TA26
	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf
Prescription Level	Mandatory
Tag	Payload compression, error handling
Variable	N/A

TA Id	DBC_TA27
Requirement	The RMSH must decompress any payload part(s) compressed by the SMSH before delivering the message.
Target	Payload reception
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push. ➢ SMSH sends an AS4 User Message with a compressed payload to the RMSH.
Expected Result	The RMSH delivers the message with decompressed payload to the Consumer.
Prescription Level	Mandatory
Tag	Payload delivery
Variable	N/A

TA Id	DBC_TA28
Requirement	➢ It must be possible to configure the accepted TLS versions(s) in the AS4 message handler. ➢ It must be possible to configure accepted TLS cipher suites in the AS4 message handler.
Target	Transport Layer Security
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the DBC AS4 profile: One-Way/Push.
Expected Result	Parameters to configure TLS version and cipher suites exist.

TA Id	DBC_TA28
	For further information please refer to section 7.2.7.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription Level	Mandatory
Tag	TLS
Variable	N/A

TA Id	DBC_TA29
Requirement	The ENISA and BSI reports state that TLS 1.0 and TLS 1.1 should not be used in new applications. Older versions such as SSL 2.0 (RFC6176) and SSL 3.0 MUST NOT be used. Products compliant with this profile SHOULD therefore support TLS 1.2 (RFC5246).
Target	Transport Layer Security
Prerequisite	➢ DBC_TA28 ➢ RMSH is configured with TLS v1.2 ➢ SMSH is configured with TLS v1.0 or TLS v1.1 ➢ SMSH tries to submit an AS4 message to the RMSH.
Expected Result	Connection is **not** established between the SMSH and the RMSH.
Prescription Level	Preferred For further information please refer to section 7.2.7.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Tag	TLS, Error
Variable	N/A

TA Id	DBC_TA30
Requirement	The ENISA and BSI reports state that TLS 1.0 and TLS 1.1 should not be used in new applications. Older versions such as SSL 2.0 (RFC6176) and SSL 3.0 MUST NOT be used. Products compliant with this profile SHOULD

TA Id	DBC_TA30
	therefor support TLS 1.2 (RFC5246).
Target	Transport Layer Security
Prerequisite	➢ DBC_TA28 ➢ RMSH is configured with TLS v1.2 ➢ SMSH is configured with SSL v2.0 or SSL v3.0 ➢ SMSH tries to submit an AS4 message to the RMSH.
Expected Result	Connection is **not** established between the SMSH and the RMSH. For further information please refer to the Access Point Implementation Guide (Section 7.2.7.1) published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription Level	Mandatory
Tag	TLS, Error
Variable	N/A

TA Id	DBC_TA31
Requirement	(Note: This test assertion is only valid when TLS is handled by the AS4 message handler) ➢ IANA publishes a list of TLS cipher suites (TLSSP), only a subset of which the ENISA Report considers future-proof. Products must support cipher suites included in this subset. Vendors must add support for newer, safer cipher suites, as and when such suites are published by IANA/IETF. ➢ Support for SSL 3.0 and for cipher suites that are not currently considered secure should be disabled by default. ➢ Perfect Forward Secrecy, which is required in (BSITLS), is supported by the TLS_ECDHE_* and TLS_DHE_* cipher suites, which are therefore preferred and should be supported.
Target	Transport Layer Security
Prerequisite	➢ DBC_TA28 ➢ RMSH is configured with TLS v1.2 and list_accepted_cipher_suites.

TA Id	DBC_TA31
	➢ SMSH is configured with TLS v1.2 and cipher_suites not in list_accepted_cipher_suites. ➢ SMSH submits an AS4 message to the RMSH.
Expected Result	Connection is **not** established between SMSH and RMSH. For further information please refer to the Access Point Implementation Guide (Section 7.2.7.1) published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription Level	Mandatory
Tag	TLS
Variable	List_accepted_cipher_suites: subset of list of TLS cipher suites (TLSSP) and TLS_ECDHE_* and TLS_DHE_* cipher suites.

TA Id	DBC_TA32
Requirement	➢ IANA publishes a list of TLS cipher suites (TLSSP), only a subset of which the ENISA Report considers future-proof Products must support cipher suites included in this subset. Vendors must add support for newer, safer cipher suites, as and when such suites are published by IANA/IETF. ➢ Support for SSL 3.0 and for cipher suites that are not currently considered secure should be disabled by default. ➢ Perfect Forward Secrecy, which is required in (BSITLS), is supported by the TLS_ECDHE_* and TLS_DHE_* cipher suites, which are therefore preferred and should be supported.
Target	Transport Layer Security
Prerequisite	➢ DBC_TA28 ➢ RMSH is configured with TLS v1.2 and list_accepted_cipher_suites. ➢ SMSH is configured with TLS v1.2 and cipher_suites in list_accepted_cipher_suites. ➢ SMSH submits an AS4 message to the RMSH.

TA Id	DBC_TA32
Expected Result	The RMSH returns an HTTP response code 2XX. (Success) For further information please refer to sections 10.3 and 10.3.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription Level	Mandatory
Tag	TLS
Variable	List_accepted_cipher_suites: subset of list of TLS cipher suites (TLSSP) and TLS_ECDHE_* and TLS_DHE_* cipher suites.

TA Id	DBC_TA33
Requirement	From/PartyId and To/PartyId SHALL MUST address the identifiers of Access Points.
Target	Message Reliability
Prerequisite	➢ SMSH and RSMH are configured to exchange AS4 messages according to the DBC AS4 Profile (One-Way/Push MEP). ➢ SMSH sends an AS4 UserMessage to the RMSH.
Expected Result	In the message, sender/receiver elements reference the Sending and Receiving MSHs and **not** the message Producer or Consumer. For further information please refer to sections 10.2 and 10.2.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>
Prescription Level	Mandatory
Tag	Addressing
Variable	Sender/Receiver: UserMessage/PartyInfo/{From/To}/PartyId elements.

TA Id	DBC_Semantic1
Requirement	The Service Provider's solution must ensure that it adheres to the Council's Semantic model and specification **prior** to sending out any business

TA Id	DBC_Semantic1
	documents (eInvoices).
Target	Semantic Conformance
Prerequisite	➢ SMSH is configured to send AS4 messages according to the Council's AS4 profile: One-Way/Push MEP. ➢ SMSH attempts to sends an AS4 User Message to the RMSH, where the payload (eInvoice) does **not** conform to the Council's semantic specification and model. For further information please refer to the eInvoicing Implementation Guide and the eInvoicing semantic model published on the Council's website. <<relevant hyperlink will be inserted before this document is published>>
Expected Result	The SMSH reports an error (message delivery failure) to the message Producer. For further information please refer to Appendix A: PMode Parameters and section 10 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>> and; sections 2.1.3.4 and 5.2.2 in the following specification; http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.pdf
Prescription Level	Mandatory
Tag	Semantic
Variable	N/A

TA Id	DBC_Semantic2
Requirement	The Service Provider's solution must ensure that it adheres to the Council's Semantic model and specification for sending business document(s) to other Council registered providers.
Target	Semantic Conformance
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the Council's AS4 profile: One-Way/Push MEP. ➢ SMSH sends an AS4 User Message to the RMSH, with a payload

TA Id	DBC_Semantic2
	(eInvoice) that conforms to the Council's semantic model and specification. For further information please refer to the eInvoicing Implementation Guide and the eInvoicing semantic model published on the Council's website. <<relevant hyperlink will be inserted before this document is published>>
Expected Result	The RMSH returns an eb:Receipt. For further information please refer to sections 7.2.1, 10.3 and 10.3.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink will be inserted before this document is published>>
Prescription Level	Mandatory
Tag	Semantic
Variable	N/A

TA Id	DBC_Semantic3
Requirement	The Service Provider's solution must ensure that it adheres to the Council's Semantic model and specification for sending business document(s) to other Council registered providers.
Target	Semantic Conformance
Prerequisite	➢ SMSH and RMSH are configured to exchange AS4 messages according to the Council's AS4 profile: One-Way/Push MEP. ➢ SMSH sends an AS4 User Message to the RMSH, with a payload (eInvoice) that **does not** conform to the Council's semantic model and specification. For further information please refer to the eInvoicing Implementation Guide and the eInvoicing semantic model published on the Council's website. <<relevant hyperlink will be inserted before this document is published>>
Expected Result	The RMSH sends back a synchronous eb:Error response. For further information please refer to sections 7.2.3, 10.4 and 10.4.1 in the Access Point Implementation Guide published on the Council's website. <<relevant hyperlink to be inserted before this document is published>>

TA Id	DBC_Semantic3
Prescription Level	Mandatory
Tag	Semantic
Variable	N/A