Transport Certification Australia

Intelligent Access Program (IAP)

Functional and Technical Specification
Version 3.02

January 2018

An *app* of the National Telematics Framework

Intelligent Access Program (IAP)
Functional & Technical Specification
TCA-S01-3.02

First published March 2006

Transport Certification Australia Ltd
T +61 3 8601 4600
F +61 3 8601 4611
E tca@tca.gov.au
W www.tca.gov.au

ABN 83 113 379 936

Document Details

Title	Intelligent Access Program Functional and Technical Specification
Document Number	TCA-S01
Version	3.02
Version Date	January 2018
Printing Instructions	Double sided, colour

Document History

Version	Date	Description
1.03	March 2006	Circulated for comment from interested parties.
2.00	November 2006	Final draft, inclusive of self-declaration function. Circulated for comment from interested parties.
2.01	December 2006	Included changes from review and comments from interested parties.
2.02	March 2007	Changes to Specification Version 2.01 include: • Removal of A.5.4 (no battery in TID) • Inclusion of B.16.7 (Interpretation of "No Load") • B.34.4,5,6,7 replace 'perpendicular' with 'at right-angles' • B.34.18 inserted 'NCR' prior to 'Position Record' • B.37.1 modified to permit all SD Records generated whilst non-compliant to be issued to jurisdictions • B.38.4b&c rewording to clarify records for the full period are required • B 38.9 modified to permit all relevant SD Records to be issued to jurisdictions • B.39.2 rewording of the 'Note' to make information clear • Table 2 'Vehicle Category Code' corrected to include two additional vehicle types • B.39.14b modified to include UTC date and time of last known position • General minor edits correcting referencing and typing errors only Appendix C (page C-5): • Added 'Last Known Position – UTC data/time' field to NCR SD Records Appendix H: • Updated 'Figure H-15' Appendix H: Annexes A & B: Modification to accommodate changes in B.39.14b, adding UTC date and time to last known position (as used by NCR SD records)
3.0	October 2017	Inclusion of Addenda 1 to 9, including: • 1.3.1 updated by Addendum 1 • 3.1.1 updated by Addendum 9 • A.2.3 updated by Addendum 6 • A.3.1 updated by Addendum 1 • A.8.1 updated by Addendum 9 • A.9.1 updated by Addendum 9 • A.13.1 updated by Addendum 9 • A.13.3 updated by Addendum 9 • A.14.7 updated by Addendum 6 • A.16.2 updated by Addendum 9 • A.17.2 updated by Addendum 9 • A.25.3 updated by Addendum 9 • A.26.1 updated by Addendum 9

- A.29.2 updated by Addendum 1
- A.30.3 updated by Addendum 1
- A.32.7 updated by Addendum 7
- A.32.8 updated by Addendum 4
- B.1 heading updated by Addendum 9
- B.4.7 updated by Addendum 7
- B.6 heading updated by Addendum 9
- B.7.1 updated by Addendum 1
- B.12.6 updated by Addendum 9
- B.12.7 inserted by Addendum 7
- B.14.1 updated by Addendum 3
- B.17.3 updated by Addendum 9
- B.17.16 updated by Addendum 4
- B.17.18 updated by Addendum 7
- B.17.19 inserted by Addendum 7
- B.17.20 inserted by Addendum 7
- B.17.21 renumbered Addendum 7 (previously B.17.19)
- B.17.22 renumbered Addendum 7 (previously B.17.20)
- B.17.23 renumbered Addendum 7 (previously B.17.21)
- B.18.2 updated by Addendum 7
- B.19.3 updated by Addendum 9
- B.21.2 updated by Addendum 9
- B.23.1 updated by Addendum 5
- B.23.2 updated by Addendum 5
- B.23.4 updated by Addendum 5
- B.23.5 updated by Addendum 5
- B.23.6 updated by Addendum 1
- B.24.6 updated by Addendum 9
- B.25.1 updated by Addendum 1
- B.31.7 updated by Addendum 1
- B.33.14 updated by Addendum 3
- B.34.4 updated by Addendum 9
- B.34.5 updated by Addendum 9
- B.34.6 updated by Addendum 9
- B.34.7 updated by Addendum 9
- B.34.13 updated by Addendum 9
- B.34.14 updated by Addendum 9
- B.34.18 updated by Addendum 9
- B.34.19 renumbered Addendum 9 (previously B.34.18)
- B.34.20 renumbered Addendum 9 (previously B.34.19)
- B.36.1 updated by Addendum 9
- B.36.2 updated by Addendum 9
- B.38.2 updated by Addendum 7
- Table 1 Alarm Code 52 updated Addendum 9
- Table 1 Alarm Code 85 updated Addendum 7
- Table 1 Alarm Code 86 inserted Addendum 7
- B.38.3 updated by Addendum 9
- B.38.4 updated by Addendum 7
- B.38.5 removed by Addendum 7
- B.38.7 updated by Addendum 9
- B.38.8 updated by Addendum 9
- B.38.11 updated by Addendum 4
- B.38.12 updated by Addendum 9
- B.39.3 updated by Addendum 9
- B.39.6 updated by Addendum 9
- B.39.10 updated by Addendum 9
- B.39.13 updated by Addendum 9
- B.39.14 updated by Addendum 9
- B.40.1 updated by Addendum 1
- B.41.10 inserted by Addendum 4
- B.42.7 updated by Addendum 4
- B.43.10 renumbered Addendum 7 (previously B.43.9)
- B.43.11 renumbered Addendum 7 (previously B.43.10)
- B.43.12 updated by Addendum 9
- B.44.1 updated by Addendum 9
- B.46.1 updated by Addendum 6
- B.46.3 updated by Addendum 7
- B.47.5 updated by Addendum 1
- B.52.2 updated by Addendum 4
- C.2.1 updated by Addendum 9
- C.4.4 inserted by Addendum 9
- C.4.5 inserted by Addendum 9
- C.4.6 inserted by Addendum 9
- C.4.7 inserted by Addendum 9
- C.4.8 inserted by Addendum 9
- C.4.9 inserted by Addendum 9
- C.4.10 inserted by Addendum 9
- C.4.11 inserted by Addendum 9
- C.5.1 updated by Addendum 9
- C.6.1 updated by Addendum 9

		• Appendix B note updated by Addendum 4 • E.2.1 updated by Addendum 9 • F.4 updated by Addendum 1 • F.6 updated by Addendum 9 • G.2.3.5 updated by Addendum 9 • Table G-1 note updated by Addendum 4 • Table G-5 note updated by Addendum 9 • H.3.2.2 updated by Addendum 9 • H.3.2.3 updated by Addendum 9 • H.4.1.2 updated by Addendum 9 • H.4.2.2 updated by Addendum 7 • H.4.2.5 updated by Addendum 9 • H.4.3.1 updated by Addendum 9 • Section H.4.9 inserted by Addendum 1 • H.4.9.1 updated by Addendum 9 • H.4.9.3 updated by Addendum 9 • Section H.4.10 inserted by Addendum 2 • H.4.10.4 updated by Addendum 9 • Figure H–16 moved by Addendum 9 • Table 2 Row 3 updated by Addendum 7 • Table 2 Row 4 updated by Addendum 7 • Table 2 Row 28 inserted by Addendum 9 • Table 2 Row 29 inserted by Addendum 9 • Appendix A HDOP definition updated by Addendum 9 • Appendix A IAP-SP/TO Agreement definition updated by Addendum 2 • Appendix A SD Record definition updated by Addendum 3 • Appendix A TCA Reference System definition updated by Addendum 9 (previously GPS Reference System) • Appendix A Transform definition inserted by Addendum 4 • Appendix B IAC Form Permitted Vehicle Types table updated by Addendum 9 • Appendix B IAC Form Prime Mover / Rigid Truck Details table updated by Addendum 5 • Appendix C NCR Form Transport Operator note updated by Addendum 5 • Appendix C NCR Form Transport Operator table updated by Addendum 5 • Appendix C NCR Form Prime Mover / Rigid Truck Details table updated by Addendum 5 • Appendix C NCR Form Trailer Details note updated by Addendum 5 • Appendix C NCR Form Trailer Details table updated by Addendum 5 • Appendix D PR Form IAP-SP Details table updated by Addendum 9 • Appendix D Vehicle Details note updated by Addendum 5 • Appendix D Vehicle Details table updated by Addendum 5 • Table G–5 updated by Addendum 1
3.01	November 2017	Changes to clarify distinction of roles for the Jurisdiction and the IAC-issuing Jurisdiction, including: • 1.1.2, 2.2.6, 2.2.7, 2.3.5, 2.3.8 • B.18, B.19, B.20, B.21, B.22, B.23, B.24, B.25, B.26, B.28, B.31, B.32 • B.33, B.34, B.35, B.38, B.39, B.41, B.42, B.43, Table 2, B.45 • Appendices A, B, C, D, F, G, Table G-6 • H.1, H.2, H.3, H.4 Changes to clarify Jurisdiction local date and time, including: • B.27.3, B.40.1, B.41.3, Appendix A
3.02	January 2018	Changes to allow IAP Speed Thresholds (within Speed Conditions) to apply per Jurisdiction, associated adjustments to A.13.3 and A.17, and minor editorial corrections

Contents

FIGURES

TABLES

APPENDICES

1 INTRODUCTION

1.1 Purpose of this document

1.1.1 This document serves to describe the functional and technical requirements of:

a) In-Vehicle Units (IVUs), plus Trailer Identification Devices (TIDs);

b) IAP-Service Providers (IAP-SPs); and

c) Self Declaration Input Devices (SDIDs)

operating within the Intelligent Access Program (IAP).

1.1.2 This document also serves to detail various obligations of other parties to the IAP (specifically Transport Certification Australia Limited (TCA) and Intelligent Access Condition (IAC)-issuing Jurisdictions), particularly where these obligations relate to interacting with the IAP-SP.

1.2 Scope

1.2.1 This document describes the following IAP requirements:

a) Requirements for IVU and TID Type-Approval: these are requirements that shall be met by Applicants intending to provide a type-approved IVU and if implemented, the optional capability provided through TIDs, for usage within the IAP. TCA is the organisation that will grant IVU and TID type- approval;

b) Requirements for IAP-SPs: these are requirements that shall be met by an IAP-SP in fulfilling the IAP functional and technical requirements of an IAP-SP under the IAP. TCA is the organisation that will certify IAP-SPs; and

c) Requirements for SDIDs: these are requirements that shall be met in the provision of SDIDs.

1.3 Document overview

1.3.1 The philosophy guiding the creation of the IAP Functional & Technical Specification has been that it focuses on required outcomes, without being overly prescriptive or solution oriented.

That is, Applicants for certification and, in an ongoing context IAP Service Providers, are both encouraged to develop innovative ways of meeting the various functional and technical requirements of the IAP Functional & Technical Specification and to submit them to TCA for approval. This will enable the IAP to draw upon the best in available technology as it develops from time to time, and indeed to encourage its development, rather than simply availing itself of the technology which was available at a particular point in time. TCA will of course take due care to ensure that the intellectual property rights of individual Applicants and IAP Service Providers are protected in this approval process.

1.3.2 The Specification commences with this Introduction (Section 1), followed by Background concerning the IAP (Section 2).

1.3.3 References applicable to this Specification are listed at Section 3.

1.3.4 Sections 4, 5 and 6 describe the requirements for:

a) IVU and TID Type-Approval;

b) IAP-SPs; and

c) SDIDs.

1.3.5 IVUs and TIDs are to be type-approved. The *Requirements for IVU and TID Type-Approval* describe the requirements for IVUs and TIDs under the IAP. Requirements in this section are prefixed by an 'A' (e.g. A.5.2).

1.3.6 The performance of individual, installed IVUs will be monitored during operation in accordance with the *Requirements for IAP-SPs*. Requirements in this section are prefixed by a 'B' (e.g. B.12.5). The operation of an IVU, its transfer of data and the subsequent reporting of Non-Compliance Reports (NCRs) and Participants Reports (PRs) is dependent on a number of factors, such as installation, communication coverage, Global Positioning System (GPS) usage as well as the IAP-SP System's capabilities. The *Requirements for IAP-SPs* also describe the responsibilities and outputs expected of the IAP-SP, including data interchange requirements between the various parties taking part in the IAP.

1.3.7 The requirements for SDIDs are prefixed by a 'C' (e.g. C.1.1).

1.3.8 The Specification includes the following appendices:

- Appendix A: Acronyms and Definitions;
- Appendix B: Intelligent Access Condition Form;
- Appendix C: Non-Compliance Report Form;
- Appendix D: Participants Report Form;
- Appendix E: Requirements for the Provision of IVUs, TIDs and SDIDs to TCA;
- Appendix F: Requirements for Speed Record Processing;
- Appendix G: Data Requirements Specification for TCA Audit System (TAS); and
- Appendix H: Business to Business Interface Specification.

1.3.9 It is important to note that the Form representations provided at Appendices B, C and D are included only as aids to the reader of this Specification. The IAC, NCR and PR are detailed in Appendix H, which specifies the exact data formats through XML schema. The reader should ultimately defer to Appendix H when determining IAC, NCR and PR data requirements.

1.4 Nomenclature

1.4.1 In this document:

a) all references to Global Positioning System (GPS) include all TCA approved Global Navigation Satellite Systems (GNSS);

b) all references to software include software in any form or medium, including firmware, unless otherwise qualified; and

c) where the context so requires it, references to the 'IAP-SP' shall, before the IAP-SP has been certified by TCA, be a reference to that party as an Applicant for certification.

1.4.2 Requirements clauses within this document that are denoted by:

a) '*shall*' are requirements that must be met;

b) '*should*' are requirements that should desirably be met; and

c) '*will*' are obligations that will be met by other parties.

1.4.3 Notes are included by way of clarification and apply to the immediately preceding clause.

1.4.4 Acronyms and terms defined for the purposes of this Specification may be found within Appendix A, Acronyms and Definitions.

2 BACKGROUND

2.1 Intelligent Access Program

2.1.1 The IAP is a voluntary program which provides to the operators of heavy vehicles, access, or improved access, to the Australian road network in return for the monitoring of their compliance with specific access conditions by vehicle telematics solutions.

2.1.2 Vehicle monitoring is on the basis of three parameters:

a) vehicle position (for spatial compliance);

b) vehicle time (for temporal compliance); and

c) vehicle speed (for speed compliance).

2.1.3 Additionally, the IAP allows for a Transport Operator (TO) and/or its nominated representative to self declare data. At this stage the self declaration (SD) function supports Vehicle Type (Vehicle Category and Number of Axles), Total Combination Mass (TCM) and Comments.

2.1.4 All vehicles participating in the IAP will require an In-Vehicle Unit (IVU) to be installed. The operation of the IVU and the reporting of data received from it is the responsibility of the IAP-SP.

2.2 Operation of the IAP

2.2.1 Jurisdictions may develop and make available schemes, permits, applications, notices, concessions, exemptions or gazettals (variously named in accordance with individual Jurisdictional practice) which provide improved access to the road network and utilise the IAP as a compliance solution.

2.2.2 The schemes, permits, applications, notices, concessions, exemptions and gazettals referred to in 2.2.1 are known as IAP Applications.

2.2.3 IAP remotely monitors vehicles using in-vehicle systems that utilise sensors to monitor parameters of interest (such as position and time). Wireless communications networks are used to transmit data to IAP-SPs.

2.2.4 A TO may apply to be part of such IAP Applications, or it may approach a Jurisdiction for a unique IAP Application which better suits its particular needs.

2.2.5 The Jurisdiction examines both the proposed vehicle and the requested access to determine what effect, if any, the proposal may have on safety, infrastructure and the environment. The Jurisdiction may then:

a) approve the request by way of granting an IAP Application; or

b) deny access to the network under the proposed conditions, should the proposal be unacceptable.

2.2.6 In summary, the IAP operates as follows:

a) The TO applies to join a particular IAP Application through an IAC-issuing Jurisdiction in order to gain improved access to the road network. This IAP Application includes a set of IAP Conditions, designed by the IAC-issuing Jurisdiction, with which the applying vehicle combinations must comply.

b) The TO then engages an IAP-SP to:

i) install an IVU to enable monitoring of the vehicle parameters, and, if applicable, TID(s) and SDID; and

ii) provide IAP Services on a fee-for-service basis.

c) Details of the TO's application to join an IAP Application are contained in an Intelligent Access Condition (IAC). The IAC specifies details about the Jurisdiction, the IAC-issuing Jurisdiction, the IAP Conditions, the TO and its vehicle combination, the IAP-SP and the installed in-vehicle equipment.

d) A vehicle may operate under one or more IAP Application. A vehicle may have more than one IAC.

e) The IAP-SP commences provision of IAP Services.

f) The IAP-SP notifies the IAC-issuing Jurisdiction in a Non-Compliance Report (NCR) whenever the TO is non-compliant with the IAP Conditions according to the following:

i) Spatial and Temporal non-compliance is assessed against each applicable IAC issued to the vehicle independently; and

ii) other non-compliance is assessed against the set of applicable IACs issued to the vehicle;

g) The IAP-SP provides a monthly Participants Report (PR) for each Jurisdiction aggregating the number of NCRs for each vehicle.

h) Transport Certification Australia Limited (TCA) serves its members and the community by ensuring that IAP-SPs are certified and audited.

2.2.7 The participants, or key players in the IAP operating model, as shown in *Figure 1* along with their broad interactions, are:

a) TCA – The body responsible for the certification and auditing of IAP-SPs and administering the IAP;

b) Jurisdictions – Entities that establish schemes with an IAP compliance solution. An IAC-issuing Jurisdiction may have the authority to issue IACs on behalf of one or more Jurisdictions, to achieve the monitoring, compliance and enforcement activities necessary to realise the IAP Applications for those respective Jurisdictional road network(s);

c) IAP-SPs – Private sector monitoring companies that provide telematics services (i.e. hardware, software and associated processes) and are certified and audited by TCA for participation in the IAP;

d) TOs – Operators of one or more vehicles eligible to voluntarily enter a scheme requiring an IAP compliance solution; and

e) IAP Auditors – Companies or individuals that assist TCA in auditing parties who have applied for certification as an IAP-SP (Applicants) and in ongoing auditing and review of IAP-SPs.

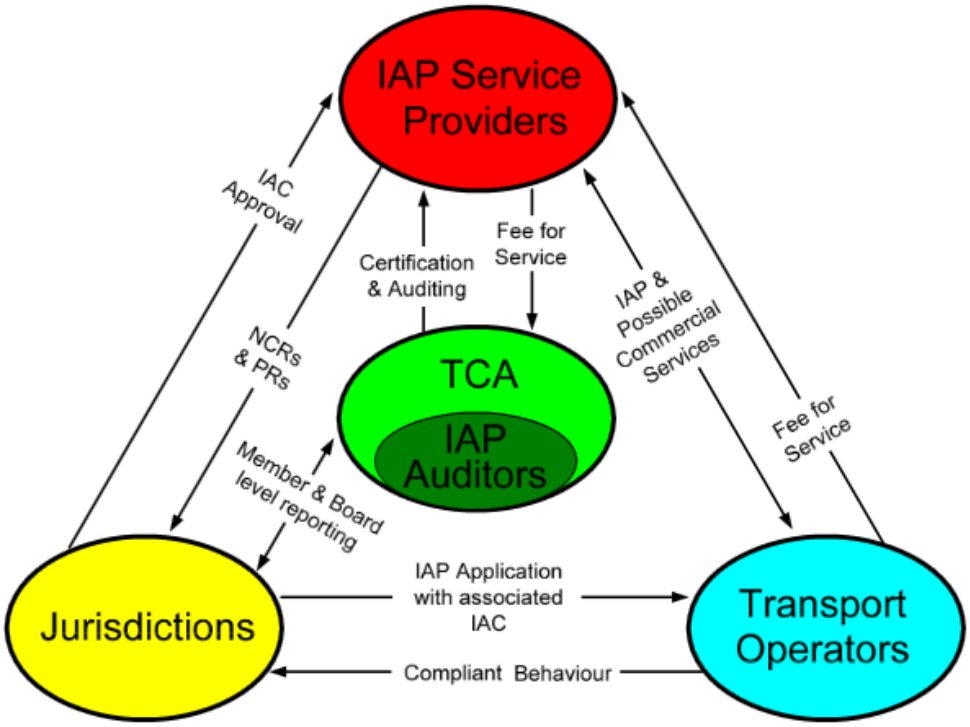


Figure 1: IAP Key Players

Note: An IAC-issuing Jurisdiction may have the authority to issue IACs on behalf of one or more Jurisdictions, to achieve the monitoring, compliance and enforcement activities necessary to realise the IAP Applications for those respective Jurisdictional road network(s).

2.3 Physical reference architecture

2.3.1 *Figure 2* depicts the main components in the physical reference architecture of the IAP. The IVU will be supported via an external power supply (envisaged to be the vehicle's power supply) and will collect data from a number of sources and sensors, generate IVU Data Records and transmit those records to the IAP-SP System for further processing. Such system processing is carried out by the IAP-SP using its Information Technology (IT) processing facilities. This activity is performed completely independently of the TO.

2.3.2 Data processed by the IAP-SP will be assessed against the one or more IACs that may pertain to the vehicle being monitored, subject to jurisdictional boundaries.

2.3.3 In the event that a non-compliant activity within a Jurisdiction is identified, an NCR is generated by the IAP-SP and electronically transmitted to the relevant IAC-issuing Jurisdiction.

2.3.4 In addition to the generation of NCRs, the IAP-SP is required, on a periodic basis, to generate a PR, for each Jurisdiction.

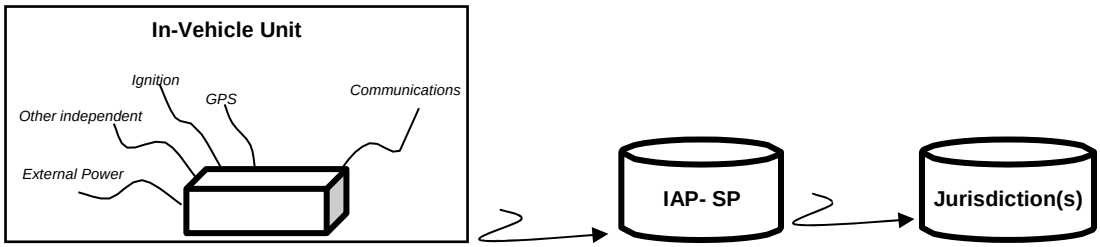


Figure 2: Physical Reference Architecture

2.3.5 The data specified within the IAP physical reference architecture is in various locations as shown in *Figure 2* through the phases of:

a) Data collection. The Specification details the data to be collected and the records to be generated and stored by the IVU prior to data transfer. Such data is specified in order to produce as output, prescribed evidentiary level data that will be assessed against the IAC for compliance.

b) Data transfer. The Specification details what IVU Data Records are to be transmitted from the IVU to the IAP-SP System, dealing with issues such as frequency, storage, security and access to communication links.

c) Data processing. The Specification relating to data analysis and processing addresses the requirements to identify non-compliant activities and deliver NCRs and PRs as outputs to the IAC-issuing Jurisdictions (with data transfer via the Internet).

2.3.6 While the data to be collected by the IVU is specified, it is left to the IAP-SP to determine how that data is collected.

2.3.7 The performance of IVUs is monitored to ensure that they are performing in accordance with this Specification.

2.3.8 Data forming the actual IACs, NCRs and PRs will be securely transmitted electronically between the relevant IAP-SPs and IAC-issuing Jurisdictions using a Business to Business (B2B) electronic data interchange capability over the Internet, with transmissions electronically signed.

3 REFERENCES

3.1.1 Documents referenced in the Specification are listed below:

a) Australian Design Rule 42/04 General Safety Requirements, Section 18;

b) Degrees of protection provided by enclosures (IP code), AS 60529-2004, Standards Australia;

c) Electromagnetic compatibility (EMC) – Part 4-3:Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test, AS/NZS IEC 61000.4.3:2013, Standards Australia;

d) Electromagnetic compatibility (EMC) – Testing and measurement techniques – Electrostatic discharge immunity test, AS/NZS IEC 61000.4.2:2013, Standards Australia;

e) Information Technology – Code of practice for information security management, ISO/IEC 27002-2005;

f) *Quality Management Systems – Requirements*, AS/NZS ISO 9001:2000, Standards Australia;

g) Radiocommunications (Radionavigation – Satellite Service) Class Licence 2015, Australian Communications and Media Authority;

h) Regulation No 10 of the Economic Commission for Europe of the United Nations (UNECE) – Uniform provisions concerning the approval of vehicles with regard to electromagnetic compatibility, Rev.5, 16 October 2014 (UNECE Regulation No10);

i) Road Vehicles – Electrical disturbances from conduction and coupling, Part 3: Electrical transient transmission by capacitive and inductive coupling via lines other than supply Lines, ISO 7637-3:2016, ISO 2016;

j) *Security seals – Classification*, AS/NZS 4255.1:1994, Standards Australia; and

k) *Vehicle immobilizers*, AS/NZS 4601:1999, Standards Australia.

4 REQUIREMENTS FOR IVU AND TID TYPE-APPROVAL

4.1 Overview

4.1.1 This section contains the requirements for the type-approval of IVUs and TIDs. The section is divided into the following:

- Physical and environmental characteristics;
- Data collection and record generation;
- Data storage and transfer; and
- Provision of IVU and TID for type-approval.

4.2 Philosophy

4.2.1 Approval of an IVU or a TID is on the basis of type. TCA will perform type-approval of IVUs and TIDs on the basis of two IVUs, and, if applicable, two TIDs, being submitted to TCA for type-approval.

4.2.2 Only type-approved IVUs and TIDs may be used by an IAP-SP in providing IAP Services.

4.3 Requirements

PHYSICAL AND ENVIRONMENTAL CHARACTERISTICS

A.1 In-Vehicle Unit (IVU)

A.1.1 The IAP Service Provider (IAP-SP) shall provide an In-Vehicle Unit (IVU) that collects, monitors and stores Global Positioning System (GPS) and other data required to be collected under the Intelligent Access Program (IAP) and transfers that data via a communications device to the IAP-SP.

A.1.2 An IVU shall be inclusive of:

a) a GPS receiver connected to a GPS antenna via an antenna cable;

b) a communications device connected to a communications antenna via a communications cable;

c) all cabling, connections and fixings leading up to, but not including:

i) external power supply;

ii) ignition (*refer A.19.3*); and

iii) other independent movement sensor (*refer A.19.4*).

A.1.3 GPS is one form of Global Navigation Satellite System (GNSS). Other forms of GNSS can be proposed and adopted by an IAP-SP subject to the approval of TCA.

A.1.4 An IVU shall be robustly connected to the respective prime mover/rigid truck to be monitored under the IAP.

A.2 IVU identifier

A.2.1 Each IVU shall have a unique alphanumeric identifier (IVU ID) that will be used to identify:

a) the particular IVU; and

b) data from that IVU, when being processed or stored by the IAP-SP System.

Note: TCA will provide each IAP-SP with a unique, three character identifier which the IAP-SP shall use as a prefix in the IVU identifier (IVU ID).

A.2.2 The IVU ID shall be visibly etched or marked on the outside casing of the unit in a manner such that it cannot be modified or removed.

A.2.3 The IVU ID shall be stored in the non-volatile programmable read-only memory of the IVU.

Note: For instance, stored using EPROM, Flash, NV RAM (battery backed), etc.

Subject to the approval of TCA, the IAP-SP may utilise an alternate approach to the above which achieves the security outcomes sought; namely the uniqueness of the IVU identifier.

A.2.4 The IVU ID shall not be able to be set or altered by any person other than the IAP-SP, or otherwise tampered with.

A.3 Security seals

A.3.1 The IVU shall be protected by security seal(s) to ensure detection of any unauthorised removal or opening of the IVU in accordance with AS/NZS 4255.1:1994 Security Category 10, Grade A, or equivalent.

A.3.2 Removal or opening of the IVU shall be possible only by breaking the security seal(s) and the security seal(s) shall be such that if broken they cannot be reinstated.

A.3.3 The IVU shall be placed in a position that facilitates inspection of the integrity of the security seal(s).

A.3.4 The security seal(s) shall clearly display signs of any unauthorised access, either visually and/or physically.

A.4 Level 1 and Level 2 Type-approved IVUs

A.4.1 There are two categories of IVU:

a) Level 1 Type-approved; and

b) Level 2 Type-approved.

A.4.2 Level 1 Type-approved IVUs shall monitor only a prime mover/rigid truck. For Level 1 Type-approved IVUs there is no requirement to identify any trailer(s) connected to a prime mover/rigid truck.

A.4.3 Level 2 Type-approved IVUs shall, in addition to monitoring a prime mover/rigid truck, automatically identify and record trailer identification information:

a) from each Trailer Identification Device (TID) (refer A.5);

b) for each trailer connected to the prime mover/rigid truck; and

c) for one to ten connected trailers.

Note: 'Connected' means that the trailer(s) are connected to the prime mover/rigid truck such that the trailer(s) move automatically in unison with the prime mover/rigid truck in a manner complying with all applicable laws, regulations and standards.

A.5 Trailer Identification Device (TID)

A.5.1 If supporting Level 2 Type-approved IVUs, the IAP-SP shall provide Trailer Identification Devices (TIDs) to facilitate automatic identification and recording of fitted trailers by the IVU.

Note: See also A.18.

A.5.2 A TID shall be robustly connected to each trailer to be monitored by the IAP-SP and shall be inclusive of the hardware, software and cabling and connections leading up to, but not including the IVU.

A.5.3 A TID shall automatically become permanently inoperable upon opening and/or removal from the trailer.

A.5.4 When the trailer(s) are attached to the prime mover/rigid truck, the TID(s) shall be identified and recorded automatically by the Level 2 Type-approved IVU without the need for additional electrical connection to the TID(s) and without manual confirmation being required.

A.5.5 When the trailer(s) are detached from the prime mover/rigid truck, trailer identification details of the remaining attached trailers (if any) shall be similarly automatically recorded by the Level 2 Type-approved IVU.

A.5.6 The Level 2 Type-approved IVU shall only identify physically connected trailers.

A.6 Trailer Identifier

A.6.1 Each TID shall have a unique identifier (Trailer ID) that will be used to uniquely identify:

a) the trailer; and

b) data pertaining to the connection of the trailer to the prime mover/rigid truck, when being processed or stored by the IAP-SP System.

Note: TCA will provide each IAP-SP with a unique, three character identifier which the IAP-SP shall use as a prefix in the Trailer ID.

A.6.2 The Trailer ID shall be visibly etched or marked on the outside casing of the unit in a manner such that the Trailer ID marking cannot be modified or removed.

A.6.3 The Trailer ID shall be stored in non-volatile programmable read-only memory of the TID.

A.6.4 It shall not be possible to alter the Trailer ID in non-volatile programmable read- only memory without making the TID permanently inoperable.

A.7 Self Declaration capability

A.7.1 The IVU shall be capable of accepting input from a Self Declaration Input Device (SDID) installed by the IAP-SP.

Note: See also B.14.1.

A.8 Suitability for use in vehicles

A.8.1 The IAP-SP shall provide to TCA, evidence of compliance from an appropriate body, with the following, or equivalent(s) as approved by TCA in relation to the IVU and TID (if applicable):

a) the vibration requirements specified in AS/NZS 4601:1999 Type 1 paragraph 3.3.4;

b) the impact requirements specified in AS/NZS 4601:1999 paragraph 3.3.5;

c) the temperature and humidity requirements specified in AS/NZS 4601:1999 paragraphs 2.2.5.2 and 3.3.2;

d) for components exposed to the elements, the dust and water ingress protection requirements of IP66, Table 7, Item 6 and Clause 13.4 and Table 8, Item 6 and Clause 14.2.6 as defined in AS 60529-2004 (IEC 60529 Ed 2.1:2001);

e) for components mounted in the cabin, the dust and water ingress protection requirements of IP44, Table 7, Item 4 Clause 13.4 and Table 8, Item 4 and Clause 14.2.4 as defined in AS 60529-2004 (IEC 60529 Ed 2.1:2001);

f) for radiated immunity, AS/NZS IEC 61000.4.3:2013, paragraph 5, Table 1 where the test field strength is 50 V/m over a frequency range of 80 MHz to 1000 MHz and the test is conducted for set and unset states such that the IVU and/or TID shall remain in a state where all functions perform as designed during and after exposure;

g) for radiated emissions, UNECE Regulation No.10, Rev. 5, sections 6.5 and 6.6;

h) for conducted immunity for conducted disturbances along supply lines, UNECE Regulation No.10, Rev. 5, section 6.9 with functional status “A”, Table 2;

i) for conducted immunity for conducted disturbances on signal lines, ISO 7637-3:2016, the test pulses a through b shall be applied at a severity level III for either Table B.1 12V or Table B.2 24V powered IVUs and/or TIDs or both, as appropriate, in both the set and unset states with the test duration 5 min, such that the IVU and/or TID shall remain in a state where all functions perform as designed during and after exposure;

j) for conducted emissions, UNECE Regulation No.10, Rev. 5, section 6.7, Table 1 using the pulse amplitude level for both 12V and 24V systems, as appropriate; and

k) for electrostatic discharge, AS/NZS IEC 61000.4.2:2013, severity level 3 for air discharge, where the test is conducted for set and unset states and the IVU and/or TID is allowed a functional status of Class C whereby a function of the IVU and/or TID does not perform as designed during exposure but returns automatically to normal operation after exposure is removed.

Note: For the avoidance of doubt, an IVU and/or TID meeting the requirements of A.8.1 at the time of its type-approval does not require retesting in the event of updates to standards referenced in A.8.1 that are considered equivalent by TCA.

Significant changes to the hardware of a type-approved IVU and/or TID may however require retesting as deemed relevant by TCA.

A.8.2 Security seals (*refer A.3*) shall remain intact when exposed to the vibration and impact as specified in A.8.1a and A.8.1b.

A.9 IVU GPS capability

A.9.1 The IVU GPS receiver and GPS antenna shall comply with the Radiocommunications (Radionavigation – Satellite Service) Class Licence 2015 – the Australian Communications and Media Authority.

The IVU GPS antenna shall be mounted in an elevated position that meets the manufacturer's specification for the vehicle combination and such that it optimises signal strength from the GPS satellites.

A.10 Non-IAP functionality in IVU

A.10.1 It shall be permissible, subject to the approval of TCA from the perspective of preservation of the integrity of the IAP, for non-IAP functionality to be accommodated within the IVU.

A.10.2 The IAP-SP shall document, to the satisfaction of TCA, any non-IAP functionality to be provided by the IVU.

A.10.3 The IAP functionality shall be isolated from any non-IAP functionality that may be provided by the IVU such that the performance of the IVU for IAP purposes is not hindered or degraded below the requirements in this Specification, and such that the IAP is not compromised.

A.10.4 The IAP-SP shall document, to the satisfaction of TCA, the design features of the IVU which isolate and protect IAP functionality from any non-IAP functionality.

A.11 Documentation

A.11.1 The IAP-SP shall document, to the satisfaction of TCA, the IVU and, if applicable, TID and all components, cabling and their interfaces.

DATA COLLECTION AND RECORD GENERATION

A.12 Data

A.12.1 The IVU shall collect the following data:

a) GPS quality data (*refer A.13*);

b) date and time data (*refer A.14*);

c) vehicle position data (*refer A.15*);

d) vehicle direction of travel data (*refer A.16*);

e) vehicle speed data (*refer A.17*);

f) trailer identification data (if applicable) (*refer A.18*);

g) alarm status data (*refer A.19*); and

h) Self Declaration (SD) data (if applicable) (*refer A.20*).

A.12.2 The IVU shall process the collected data to produce the following IVU Data Records which are stored for later transmission:

a) Position Records (*refer A.21*);

b) Speed Records (*referA.22*);

c) Alarm Records (*referA.23*); and

d) SD Records (*refer A.24*).

A.13 GPS quality data

A.13.1 TCA will use the TCA Reference System for GPS quality comparison purposes, for IVU type-approval testing.

Note: Further information concerning the TCA Reference System may be obtained from TCA.

A.13.2 GPS quality shall be measured by the number of satellites used and the horizontal dilution of precision (HDOP).

Note: 'used' means the number of satellites whose signal is received and taken into account by the IVU in the determination of data.

A.13.3 The IVU GPS receiver shall demonstrate GPS quality to the level exhibited by the TCA Reference System, or better. Specifically:

a) the HDOP shall be no worse than plus 0.1 (+0.1) from that of the TCA Reference System for at least 95% of the observations when using:

i) at least four satellites; and

ii) the same number of satellites as the TCA Reference System; and

b) the number of satellites used by the IVU's GPS receiver shall be minus one (-1) or better than the total number used by the TCA Reference System for at least 95% of observations, at a fixed mask angle (selected according to manufacturer's recommendation) of between 10 and 20 degrees.

Note: The GPS quality comparison testing location and duration will be defined by TCA.

A.13.4 The HDOP from the IVU GPS receiver shall be measured and stored to a resolution of 0.1 or better.

A.14 Date and time data

A.14.1 The IVU shall collect and store date and time data in UTC format.

A.14.2 The date and time shall be stored with a resolution of 1 second.

A.14.3 The IVU shall have an internal clock that operates independently of the supporting external power supply.

Note: See also A.27.

A.14.4 In the event the external power supply fails or shuts down, the IVU internal clock shall operate for a period of at least 28 days.

A.14.5 The accuracy of the IVU internal clock shall be such that it does not deviate by more than 1 second from the UTC date and time over any 28 day period when using GPS signals.

A.14.6 The accuracy of the IVU internal clock shall be such that it does not deviate by more than 10 seconds per day from the UTC date and time over any 28 day period when not using GPS signals.

A.14.7 The accuracy of the IVU internal clock shall be such that it does not deviate by more than 20 seconds per day from the UTC date and time over any 28 day period when not using GPS signals and the IVU has no connection to the external power supply.

A.15 Vehicle position data

A.15.1 The IVU GPS receiver shall determine latitude/longitude position of the vehicle in WGS84 or GDA94.

Note: See also B.16.2.

A.15.2 The latitude/longitude position calculated by the IVU GPS receiver shall not deviate by more than 13 metres from the absolute horizontal position Australia-wide average for 95% of the observations when using at least four satellites and a HDOP of < 4.

A.15.3 The resolution of the stored latitude/longitude position calculated by the IVU GPS receiver shall be to 0.00001 degrees or better.

A.15.4 In the event of interruption to and subsequent reacquisition of GPS satellite signals, the IVU GPS receiver shall on the reacquisition of GPS satellite signals, commence to collect and store vehicle position:

a) if the interruption is for a period of less than seven days, within 60 seconds of reacquisition of GPS satellite signals; and

b) if the interruption is for a period of seven days or more, within five minutes of reacquisition of GPS satellite signals.

A.16 Vehicle direction of travel data

A.16.1 The IVU GPS receiver shall determine direction of travel of the vehicle in WGS84 or GDA94.

Note: See also B.16.2.

A.16.2 The direction of travel determined by the IVU GPS receiver shall not deviate from the actual direction of travel by more than 4 degrees for at least 95% of the observations when using at least four satellites and a HDOP of < 4.

A.16.3 The resolution of direction of travel determined by the IVU GPS receiver and recorded by the IVU shall be to 0.1 degrees or better.

Note: The assessment of direction of travel of the IVU GPS receiver will only be made when travelling between the speeds of 30km/h and 150km/h.

A.17 Vehicle speed data

A.17.1 Vehicle speed shall be measured by a GPS Doppler derived method.

A.17.2 The GPS reported vehicle speed shall be accurate to within 3.0 km/h for at least 99.9% of observations when using at least four satellites and a HDOP of < 4.

Note: The vehicle speed testing location and duration will be determined by TCA. The assessment of speed of the IVU GPS receiver will only be made when travelling at speeds in excess of 40km/h.

A.17.3 The resolution of the vehicle speed data recorded by the IVU shall be to 0.1 km/h or better.

A.18 Trailer identification data

A.18.1 For Level 1 Type-approved IVUs there is no requirement to record trailer identification data.

A.18.2 For Level 2 Type-approved IVUs, the IVU shall automatically identify and record all trailers in the overall vehicle combination for a maximum of up to ten trailers.

Note: See also A.5.

The automatic detection of trailers in a vehicle combination by a Level 2 Type- approved IVU is separate to, and independent of, the self declaration of Vehicle Type where required in a SD Condition (refer A.20.1).

A.19 Alarm status data

A.19.1 The connection of the IVU to the external power supply shall be monitored and reported upon in accordance with A.23.1a and A.23.1b.

A.19.2 Movement of the vehicle shall be detected and reported upon in accordance with A.23.1c and A.23.1d, using two different features independent from the GPS signal.

Note: See also A.27.1.

The purpose of the independent movement features is to be able to facilitate the detection of movement of the vehicle independently of the GPS satellite signal.

A.19.3 One independent feature to facilitate the indication of vehicle movement shall be the ignition status.

A.19.4 The other independent movement feature to facilitate the detection of vehicle movement shall, subject to the approval of TCA, be one of the following sensors:

a) the Engine Control Module (ECM);

b) an odometer;

c) a tachograph; or

d) some other such independent movement sensor.

A.19.5 The IAP-SP shall document its chosen method of independent movement detection and connection.

A.19.6 The connection of the independent movement features to the IVU shall be monitored and reported upon in accordance with A.23.1e through A.23.1h.

Note: The connection of the independent movement features to the IVU is monitored so as to detect any attempts to tamper which may include any attempts to disconnect and/or remove the IVU.

A.19.7 The connection of the GPS antenna shall be monitored and reported upon in accordance with A.23.1k and A.23.1l.

A.19.8 Access to the data in the IVU shall be monitored and reported upon in accordance with A.23.1i.

A.19.9 Access to IVU software shall be monitored and reported upon in accordance with A.23.1j.

A.20 Self Declaration (SD) data

A.20.1 The IVU shall have the capability of receiving, confirming receipt of and storing SD data only from a Self Declaration Input Device (SDID) connected to it.

Note: See also C.1.5.

A.21 Position Records

A.21.1 The IVU shall generate Position Records from the data collected by the IVU, and store Position Records that detail the position data for the vehicle being monitored.

A.21.2 Position Records shall be continuously generated and stored at time intervals of 30 ± 0.2 seconds when the vehicle is in operation.

A.21.3 A vehicle shall be considered to be in operation when the IVU's supporting external power supply is connected to the IVU and the ignition status is ON.

A.21.4 A Position Record shall consist of at least the following data:

a) record number;

b) date / time of generation (UTC format);

c) vehicle position (latitude/longitude);

d) direction of travel;

e) GPS quality, comprising:

i) number of GPS satellites; and

ii) HDOP;

f) status of ignition (on / off / disconnected);

g) status of other independent movement sensor (movement / no movement / disconnected); and

h) Trailer ID(s) for currently connected trailers (for Level 2 type-approved IVUs), to the maximum of ten trailers.

A.21.5 Vehicle position (latitude/longitude) shall be blank/void if the IVU used zero satellites, or was unable to determine vehicle position.

A.22 Speed Records

A.22.1 The IVU shall be capable of determining a measurement of the speed of the vehicle.

A.22.2 The IVU shall, while the vehicle is in operation, generate a Speed Record every 3.0 ± 0.1 seconds.

Note: The decision about which records are to be stored and transferred will be according to the IAP-SP's chosen method of processing and storing of Speed Records (refer A.26.2).

A.22.3 A Speed Record shall consist of at least the following data:

a) record number;

b) date / time of generation (UTC format);

c) vehicle position (latitude/longitude);

d) vehicle speed;

e) GPS quality, comprising:

i) number of GPS satellites; and

ii) HDOP; and

f) Trailer ID(s) for currently connected trailers (for Level 2 type-approved IVUs), to the maximum of ten trailers.

A.22.4 Vehicle position (latitude/longitude) shall be blank/void if the IVU used zero satellites, or was unable to determine vehicle position.

A.22.5 The IAP-SP shall process Speed Records either in the IVU, the IAP-SP System or a combination of both, according to Appendix F.

A.23 Alarm Records

A.23.1 The IVU shall generate and store Alarm Records for each of the following events:

a) the external power supply is disconnected from the IVU;

b) the external power supply is reconnected to the IVU;

c) movement is indicated by the ignition while the external power supply is disconnected from the IVU;

d) movement is detected by the other independent movement sensor while the external power supply is disconnected from the IVU;

e) the ignition is disconnected from the IVU (with and without external power being connected);

f) the ignition is reconnected to the IVU (with and without external power being connected);

g) the other independent movement sensor is disconnected from the IVU (with and without external power being connected);

h) the other independent movement sensor is reconnected to the IVU (with and without external power being connected);

i) unauthorised access to data in the IVU is detected;

j) unauthorised access to IVU software is detected;

k) the GPS antenna is disconnected from the IVU; and

l) the GPS antenna is reconnected to the IVU.

A.23.2 An Alarm Record shall consist of at least the following data:

a) record number;

b) date / time of generation (UTC format);

c) the event that triggered the generation of the Alarm Record as per A.23.1.

Note: It will be on the basis of the information in (c) that the IAP-SP maps to the Alarm Codes for subsequent reporting (in accordance with Table 1 within B.38.2).

A.24 Self Declaration (SD) Records

A.24.1 The IVU shall generate SD Records from the SD data entered.

A.24.2 An SD (Vehicle Type/TCM) Record shall consist of at least the following data:

a) record number;

b) date / time of generation (UTC format);

c) IAP Functional & Technical Specification Version Number;

d) Vehicle Category;

e) Number of Axles; and

f) Total Combination Mass.

Note: It will be on the basis of the information in (d) that the IAP-SP maps to the Vehicle Category Codes for subsequent reporting (in accordance with B.39.10).

A.24.3 An SD (Comments) Record shall consist of at least the following data:

a) record number;

b) date / time of generation (UTC format);

c) IAP Functional & Technical Specification Version Number;

d) Comment Name; and

e) Comment Text.

Note: It will be on the basis of the information in (d) that the IAP-SP maps to the Comment Codes for subsequent reporting (in accordance with B.39.13).

A.25 Record numbering

A.25.1 Position, Alarm and SD Records shall be assigned record numbers from the one record numbering sequence, with consecutive and increasing record numbers assigned to successive IVU Data Records in order of generation.

A.25.2 Speed Records shall be assigned record numbers from a separate numbering sequence, with consecutive and increasing record numbers assigned to successive Speed Records in order of generation.

A.25.3 The separate numbering sequences used for:

a) Position Records, Alarm Records and SD Records; and

b) Speed Records;

shall:

c) be different, such that record numbers never clash; and

d) each rotate through a large enough cycle to ensure that the same Record Number shall not be issued more than once every twelve months.

DATA STORAGE AND TRANSFER

A.26 IVU Data Record storage capability

A.26.1 The IVU shall be capable of storing at least 20,000 Position Records, Alarm Records and SD Records (combined) and at least:

a) 6,000 Speed Records (if all Speed Record processing is performed in the IVU); or

b) 200,000 Speed Records (if all the Speed Records are transferred to the IAP- SP System for Speed Record processing).

Note: For Position Records, Alarm Records and SD Records these record storage requirements are based on approximately 14 days of 12 hour operation.

For Speed Records the record storage requirements are based on:

- *approximately five hours of Speed Record data for (a); and*
- *14 days of 12 hour operation for (b).*

A.26.2 The IAP-SP may, subject to the approval of TCA, undertake Speed Record processing which utilises a combination of IVU and IAP-SP System processing (*refer A.22.5*) in which case the IAP-SP shall document, to the satisfaction of TCA, its chosen method of processing and storing Speed Records.

A.26.3 If the volume of data collected and generated prior to transfer to the IAP-SP System exceeds the data storage capacity of the IVU, new data shall not overwrite stored data.

Note: This approach is for evidentiary reasons. It prohibits the overwriting of data already collected, albeit at the expense of collecting new data.

A.27 IVU external power supply failure/shut down

A.27.1 In the event that the external power supply supporting the IVU fails or shuts down, the IVU shall be capable of:

a) retaining stored data for at least 28 days; and

b) monitoring the status of the ignition and other independent movement sensor (*refer A.19.2)* for at least seven days.

Note: For (a), see also A.14.3.

For (b), the primary purpose of continuing to monitor after the external power supply fails or shuts down is to facilitate the detection of any disconnection of the IVU and/or movement of the prime mover/rigid truck independently of the GPS signal.

A.28 Data security and confidentiality measures

A.28.1 It shall not be possible for collected or stored data or software memory within the IVU to be accessible or capable of being manipulated by any person, device or system (including the SDID), other than that authorised by the IAP-SP. Security and confidentiality of data stored in the IVU shall be maintained at all times.

A.29 IVU communications capability

A.29.1 The IVU shall be capable of communicating with the IAP-SP from at least the areas nominated by the IAP-SP in its application for certification as an IAP-SP.

A.29.2 The IAP-SP shall document, to the satisfaction of TCA, the selected communication networks and their coverage.

Note: For instance, selected communications networks and coverage could be:

a. some form of commercial mobile phone service area; or

b. Australia-wide service area by alternative means.

A.29.3 The channel for the transmission of IVU Data Records to the IAP-SP shall be secure and guarantee standards for privacy and data integrity and minimise the risk of interception by third parties, at a level consistent with services provided by Australian licensed telecommunications carriers.

A.30 Transfer of data from IVU to IAP-SP

A.30.1 The transfer of stored data from the IVU to the IAP-SP shall be performed at least once every 24 hours provided that the IVU is in the communication coverage area offered by the IAP-SP (*refer A.29*) and the vehicle is in operation.

Note: See also B.15.1.

A.30.2 If the vehicle is out of communication coverage or not in operation at the time of the scheduled data transfer, then data transfer shall commence within 5 minutes of when the communication network becomes available and the vehicle is in operation.

Note: See also B.15.2

A.30.3 IVU Data Records stored in the IVU shall only be deleted after such data is transferred from the IVU and successful receipt is confirmed by the IAP-SP.

Note: Communication protocols and associated handshaking for data transfers are defined by the IAP-SP (refer B.3.3).

A.31 IVU Data Records and Data Blocks

A.31.1 IVU Data Records shall be transferred from the IVU to the IAP-SP in Data Blocks.

A.31.2 Each transmission shall contain one or more complete Data Block(s).

A.31.3 If the transmitted Data Block(s) are compressed for transmission this shall be lossless compression – it shall be possible for the IAP-SP to decompress the Data Block(s) without loss of any data, with all records remaining complete.

A.31.4 Every Data Block shall include the following framing data:

a) Data Block number;

b) IVU ID;

c) IVU hardware and software version(s) including version(s) of all relevant components as type-approved;

d) the IAP Speed Threshold(s) stored in the IVU, if applicable; and

e) any values or data necessary to decode or decompress data within the Data Block.

Note: The details associated with item (c) are required to support complete traceability of IVU details from the perspective of certification status. In meeting the requirement to deliver this data, an approach using appropriately documented, abbreviated or encoded details would suffice.

A.32 Integrity and origin of Data Blocks and IVU Data Records

A.32.1 The Data Block numbering shall be sequential.

A.32.2 Data Block numbers shall cycle through a large enough number range such that Data Block number clashes associated with the particular IVU could not occur within a twelve-month timeframe.

A.32.3 Each Data Block shall contain error detection and error correction coding.

A.32.4 The IAP-SP shall ensure that the communication protocols, in conjunction with the Data Block error detection and correction procedure, achieve error-free transmission of IVU Data Records.

A.32.5 Each Data Block shall support a form of data authentication (i.e. some form of message authentication only known and accessible to the IAP-SP), subject to the approval of TCA, that can prove the origin and integrity of the IVU Data Records.

A.32.6 The IAP-SP shall document, to the satisfaction of TCA, the Data Block authentication mechanism.

A.32.7 The IAP-SP shall document, to the satisfaction of TCA, its data transfer arrangements from the IVU to the IAP-SP System, including:

a) error detection and error correction procedures;

b) management of the integrity of data transfer and data deletion in the IVU following transfer; and

c) authentication features that guarantee origin of data.

Note: At a minimum TCA expects that:

- a cryptographic hash algorithm will be used to check the integrity of data being transferred; and
- an authentication capability will be used to verify the origin of the data being transferred (e.g. a Message Authentication Code); or
- Some other alternative method which adequately meets these requirements, subject to the approval of TCA.

Information concerning hash algorithms may be obtained from TCA

A.32.8 The algorithms used to transform IVU Data to meet the requirements of Appendices G and H shall be documented by the IAP-SP and subject to the approval of TCA.

A.33 Integrity and origin of Trailer ID data

A.33.1 The transmission of Trailer ID data from the TID to the IVU shall support a form of Trailer ID data authentication (i.e. some form of Message Authentication Code only known and accessible to the IAP-SP), subject to the approval of TCA, that can prove the origin and integrity of the Trailer ID data.

A.33.2 The IAP-SP shall document, to the satisfaction of TCA, the Trailer ID data authentication mechanism.

A.34 Integrity and origin of SD data

A.34.1 The transmission of SD data from the SDID to the IVU shall support a form of SD data authentication (i.e. some form of Message Authentication Code only known and accessible to the IAP-SP), subject to the approval of TCA, that can prove the origin and integrity of the SD data.

A.34.2 The IAP-SP shall document, to the satisfaction of TCA, the SD data authentication mechanism.

PROVISION OF IVU AND TID FOR TYPE-APPROVAL

A.35 IVUs and TIDs for type-approval

A.35.1 To facilitate IVU Level 1 type-approval testing, two IVUs shall be provided to TCA. The Applicant shall adhere to the requirements in Appendix E detailing the supply of these IVUs.

A.35.2 To facilitate IVU and TID Level 2 type-approval testing, two IVUs and two TIDs shall be provided to TCA. The Applicant shall adhere to the requirements in Appendix E detailing the supply of these IVUs and TIDs.

Note: See also C.7.1.

5 REQUIREMENTS FOR IAP-SPS

5.1 Overview

5.1.1 This section contains the requirements for IAP Service Providers. The section is divided into the following:

- In-Vehicle Unit (IVU) and Trailer Identification Device (TID) installation, operation and maintenance;
- Self Declaration Input Device (SDID) installation, use and maintenance;
- Certification of IAP-SPs;
- IAP-SP System;
- Data handling;
- Business to Business (B2B) data interchanges;
- Intelligent Access Condition (IAC);
- Off-the-shelf IAP Conditions;
- Intelligent Access Map (IAM);
- Identification of non-compliance and issuing of NCRs;
- Participants Report (PR);
- Tier 1 and Tier 2 data interchange;
- IAP-SP Quality System;
- IAP-SP Quality Monitoring Station;
- TCA audit and review of IAP-SPs; and
- Restriction on post-certification change - IAP-SP.

5.2 Philosophy

5.2.1 Assessment of vehicle movement for compliance under the IAP will be carried out by IAP-SPs. IAP-SPs need to be certified to provide IAP Services. TCA has responsibility for the assessment of Applicants seeking certification and for granting certification where appropriate.

5.2.2 IAP Services will only be provided by entities certified by TCA as an IAP-SP.

5.3 Requirements

IN-VEHICLE UNIT (IVU) AND TRAILER IDENTIFICATION DEVICE (TID) INSTALLATION, OPERATION AND MAINTENANCE

B.1 Type-approved IVUs and TIDs

B.1.1 The IAP-SP shall only install IVUs and TIDs which have been type-approved by TCA.

B.1.2 Any proposed change to the type-approved IVU hardware or software or the type-approved TID will require the prior approval of TCA by way of re-certification.

B.1.3 To facilitate re-certification of IVUs or TIDs (as necessary), two samples of the hardware and/or software which has triggered the need for re-certification shall be provided to TCA.

B.2 Installation of IVUs and TIDs

B.2.1 The IAP-SP shall be responsible for installation of all IVU and TID hardware and software.

B.2.2 The IAP-SP shall, in installing IVUs and TIDs, use only suitably qualified and trained personnel and shall maintain a register of those personnel.

B.2.3 The IAP-SP shall have in place documented and appropriate procedures for the installation of its type-approved IVU(s) and TID(s) and shall supply the same to its installation personnel.

B.2.4 The IAP-SP shall have in place, document and implement, appropriate procedures for the training of its installation personnel.

B.2.5 The IAP-SP shall install the IVU and TID(s) such that they do not interfere with the normal, safe operation of the vehicle. To that end, the IAP-SPs shall consult with a vehicle's manufacturer before an installation seeking their advice on issues such as equipment placement, sensor wiring and power take-off points. The training of all IAP-SP installation personnel shall include manufacturer specific training on particular equipment.

B.3 Operation of IVUs and TIDs

B.3.1 The IAP-SP shall be responsible for the operation of all its type-approved and installed IVUs and TIDs.

B.3.2 The IAP-SP shall use IVU Data Records only from IVUs installed by the IAP-SP.

B.3.3 The IAP-SP shall document the communications protocols and associated handshaking for data transfers from the IVU including confirmation of successful data receipt.

B.3.4 The IAP-SP shall, in operating IVUs and TIDs, use only suitably qualified and trained personnel and shall maintain a register of those personnel.

B.3.5 The IAP-SP shall have in place documented and appropriate procedures for the operation of its type-approved IVU(s) and TID(s) and shall supply the same to its operational personnel.

B.3.6 The IAP-SP shall have in place, document and implement appropriate procedures for the training of its operational personnel.

B.4 Maintenance of IVUs and TIDs

B.4.1 The IAP-SP shall be responsible for the maintenance of all its type-approved and installed IVUs and TIDs.

B.4.2 The IAP-SP shall have in place, document and implement, appropriate procedures for the maintenance of its type-approved IVU(s) and TID(s) and shall supply the same to its maintenance personnel.

B.4.3 The IAP-SP shall have in place, document and implement, appropriate procedures for the training of its maintenance personnel.

B.4.4 The IAP-SP shall, in maintaining IVUs and TIDs, use only suitably qualified and trained personnel and shall maintain a register of those personnel.

B.4.5 The IAP-SP shall have a system in place for the programmed maintenance of its installed IVUs and TIDs to ensure that they are maintained in an operational state in accordance with this Specification at all times.

B.4.6 The programmed maintenance system (*refer B.4.5*) shall provide for the:

a) checking of the integrity of the IVU security seals and connections;

b) replacement of IVU internal batteries (where fitted) to ensure that an IVU's internal batteries are in good working condition at all times; and

c) checking of the integrity of the TID and connections.

B.4.7 In the event that an IVU or TID does not function in accordance with this Specification the IAP-SP shall:

a) immediately liaise with the TO to commence to resolve the malfunction;

b) immediately report the malfunction (including an estimated resolution period) to the IAC-issuing Jurisdiction(s) and TCA;

c) complete the resolution process within five working days of becoming aware of the malfunction subject to the reasonable cooperation of the TO;

d) ensure IVU Data Records held by the IVU are transferred to the IAP-SP System for processing; and

e) notify the IAC-issuing Jurisdiction and TCA when the malfunction has been resolved.

B.4.8 The IAP-SP shall immediately report to the IAC-issuing Jurisdiction(s):

a) evidence of any tampering or attempt at tampering with the IVU security seal(s), the TID(s) or any connection(s); and

b) any IVU or TID malfunction which appears to be the result of tampering or an attempt at tampering.

B.4.9 The IAP-SP shall not advise a TO of any detection of tampering, or suspected tampering, with their IVU and/or TID(s).

B.4.10 In the event that any type-approved IVU or TID is subject to more than one instance of malfunction of a particular type (not being of a programmed maintenance type) the IAP-SP shall notify TCA of each malfunction, the apparent cause and the remedy.

Note: See also B.1.2: Any remedy involving any change to the Type-approved IVU or TID hardware or software will require re-certification.

B.5 Documentation

B.5.1 For each IVU and TID, the IAP-SP shall document all installation, operation, programmed maintenance and remediation-of-malfunction activity.

B.5.2 The documentation referred to in B.5.1 shall be compiled by the IAP-SP's installation, operation and maintenance personnel and shall:

a) contain:

i) IVU ID or, if applicable, TID ID;

ii) version numbers of the hardware and software;

iii) date and time of activity;

iv) identification of personnel responsible;

v) details of the activity including cause of malfunction and the remediation;

vi) personnel signatures; and

b) be available for auditing by TCA.

B.5.3 The IAP-SP shall maintain archives of the documentation described within B.5.1 and B.5.2 for a period of not less than four years.

SELF DECLARATION INPUT DEVICE (SDID) INSTALLATION, USE AND MAINTENANCE

B.6 Installation of SDIDs

B.6.1 The IAP-SP shall be responsible for installation of all SDID hardware and software.

Note: Installation includes the presentation of the SDID ready for use by the TO and/or its nominated representative.

B.6.2 The IAP-SP shall ensure the installation of the SDID is consistent with the Australian Design Rule 42/04, Section 18.

B.6.3 The IAP-SP shall, in installing SDIDs, use only suitably qualified and trained personnel and shall maintain a register of those personnel.

B.6.4 The IAP-SP shall have in place documented and appropriate procedures for the installation of SDIDs and shall supply the same to its installation personnel.

B.6.5 The IAP-SP shall have in place, document and implement, appropriate procedures for the training of its installation personnel.

B.7 Use of SDIDs

B.7.1 The IAP-SP shall document the communication protocols and associated handshaking for data transfers from the SDID including confirmation of successful data receipt.

B.7.2 The IAP-SP shall have in place documented and appropriate procedures for the use of its SDIDs and shall supply the same to the TO.

Note: The 'use' of the SDID in this section is limited to the use of the SDID by the TO and/or its nominated representative in entering SD data.

B.7.3 The IAP-SP shall have in place, document and implement, appropriate procedures for the training of the TO, and/or its nominated representatives who will use the SDIDs, to ensure they can use them effectively.

B.8 Maintenance and replacement of SDIDs

B.8.1 The IAP-SP shall be responsible for the maintenance and replacement of installed SDIDs.

B.8.2 The IAP-SP shall, in maintaining and replacing SDIDs, use only suitably qualified and trained personnel and shall maintain a register of those personnel.

B.8.3 The IAP-SP shall have in place, document and implement, appropriate procedures for the maintenance and replacement of its SDIDs and shall supply the same to its maintenance personnel.

B.8.4 The IAP-SP shall have in place, document and implement, appropriate procedures for the training of its maintenance personnel.

B.8.5 In the event that the IAP-SP becomes aware that the SDID does not function in accordance with this Specification the IAP-SP shall:

a) immediately liaise with the TO to commence to resolve the malfunction;

b) immediately report the malfunction (including an estimated resolution period) to the IAC-issuing Jurisdiction(s) and TCA;

c) complete the resolution process within five working days of becoming aware of the malfunction subject to the reasonable cooperation of the TO; and

d) notify the IAC-issuing Jurisdiction and TCA when the malfunction has been resolved.

Note: The commercial arrangements pertaining to the maintenance and/or replacement of installed SDIDs is outside the scope of this Specification and should be specified in the commercial agreement between the IAP-SP and the TO.

B.8.6 The IAP-SP shall immediately report to the IAC-issuing Jurisdiction(s) any SDID malfunction which appears to be the result of tampering or an attempt at tampering with the SDID.

B.8.7 The IAP-SP shall not advise the TO of the detection or reporting of tampering, or suspected tampering, with their SDID.

B.8.8 In the event that any SDID is subject to more than one instance of malfunction of a particular type the IAP-SP shall notify TCA of each malfunction, the apparent cause and the remedy.

B.9 Documentation

B.9.1 For each SDID, the IAP-SP shall document all installation, maintenance, and remediation-of-malfunction activity.

B.9.2 The documentation referred to in B.9.1 shall be compiled by the IAP-SP's installation and maintenance personnel and shall:

a) contain:

i) identification of the SDID;

ii) version numbers of the hardware and software;

iii) date and time of activity;

iv) identification of personnel responsible;

v) details of the activity including cause of malfunction and the remediation;

vi) personnel signatures; and

b) be available for auditing by TCA.

B.9.3 The IAP-SP shall maintain archives of the documentation described within B.9.1 and B.9.2 for a period of not less than four years.

CERTIFICATION OF IAP-SPs

B.10 Certification of IAP-SPs

B.10.1 Additionally to the type-approval of IVUs and TIDs, certification as an IAP-SP is granted on the basis of TCA being satisfied as to the conformance with this Specification of the IAP-SP's:

a) IAP-SP System, being the IAP-SP's hardware and software (excluding IVUs, TIDs and SDIDs) used in the collection, processing, testing, storage and reporting of IAP data;

b) Quality Monitoring Station; and

c) IAP-SP Quality System, being the IAP-SP's systems and processes as detailed in this Specification.

IAP-SP SYSTEM

B.11 IAP-SP System

B.11.1 The IAP-SP System shall have sufficient transfer capability in its specified communication coverage area, and sufficient storage and processing capacity to support the number of IVUs for which it has been certified.

B.11.2 The IAP-SP shall immediately notify TCA when it has in service 80% of the number of IVUs for which it has been certified.

B.12 Maintenance and continuity of the IAP-SP System

B.12.1 In the event that the IAP-SP System does not function in accordance with this Specification the IAP-SP shall:

a) immediately commence to resolve the malfunction;

b) immediately report the malfunction (including an estimated resolution period) to TCA; and

c) complete the resolution process to the reasonable satisfaction of TCA.

Note: The resolution of the malfunction may reasonably require the reprocessing of data.

B.12.2 The IAP-SP shall have sufficient equipment and resources available such that, in the event of a component becoming inoperable, the IAP-SP System can be returned to an operational state within three working days.

B.12.3 The IAP-SP shall document, to TCA's satisfaction, their plan for duplicating IAP- SP System operations in the event of a catastrophic event, including procedures for activating critical information systems in a new location and recovering critical information systems within a maximum period of 20 working days.

B.12.4 The IAP-SP shall immediately report to TCA:

a) evidence of any tampering or attempt at tampering with the IAP-SP System; and

b) any IAP-SP System malfunction which appears to be the result of tampering or an attempt at tampering.

B.12.5 In the event that the IAP-SP System is subject to more than one malfunction of a particular type, the IAP-SP shall notify TCA of each malfunction, the apparent cause and the remedy.

Note: See also B.54: Any remedy involving any change to the IAP-SP System will require re-certification.

B.12.6 The IAP-SP shall test its procedures for recovering its IAP-SP System from failures partially or fully no less than once every calendar year.

Note: See also B.18.2.

B.12.7 The IAP-SP shall notify TCA of any planned IAP-SP System outage at least three working days prior to the scheduled event.

Note: A planned outage is the advanced scheduling of an IAP-SP System maintenance activity.

B.13 Documentation

B.13.1 The IAP-SP shall document all installation, programmed maintenance and remediation-of-malfunction activity for the IAP-SP System, and shall maintain archives of the documentation for a period of not less than four years.

DATA HANDLING

B.14 SD data

B.14.1 The IAP-SP may facilitate, as an alternative to SDID use, the entry of SD data directly to the IAP-SP System by the TO, subject to the approval of TCA. Where this facility is applied, the IAP-SP shall:

a) only accept SD data entered into the IAP-SP System up to 72 hours after the data entry time if such data entry has taken place by use of a SDID; and

b) ensure that a full audit trail is maintained to facilitate verification of all SD data so entered by the TO.

Note: An IAP-SP may offer a TO access to both facilities.

B.14.2 In the event that the IAP-SP elects to provide the alternative facility outlined in B.14.1, as a minimum they shall provide:

a) the data outlined in A.24.2 and A.24.3, with the exception of record number; and

b) a value for the date/time of generation (UTC format) which is representative of a data entry time if such data entry had taken place by use of a SDID.

B.15 Data collection

B.15.1 The IAP-SP shall ensure that all data stored within the IVU is transferred to the IAP-SP System at least once every 24 hours, provided that the IVU is in the communication coverage area and the vehicle is in operation.

Note: See also A.30.1.

B.15.2 If at the time of scheduled data transfer, the IVU is out of communication coverage or the vehicle is not in operation, the IAP-SP shall ensure that data transfer will commence within 5 minutes of when the communication network becomes available and the vehicle is in operation.

Note: See also A.30.2.

B.15.3 Noting the provisions of B.15.1, the IAP-SP shall have procedures in place to ensure that transfer of IVU Data Records from the IVU to the IAP-SP System occurs not more than 72 hours after data collection.

B.15.4 The IAP-SP shall retain all Data Blocks transferred from the IVU in unaltered format, including all framing information.

Note: See also B.18 for archival requirements.

B.16 Data processing

B.16.1 Unless otherwise specified, the requirements within Section 5 (Requirements for IAP-SPs) of this Specification shall be interpreted as considering IVU Data Records in the order of the UTC date and time of generation within each record.

Note: As an example, terms such as 'adjacent' and 'most recent' are evaluated as if the records are in the order of the UTC date and time of generation.

B.16.2 If IVU Data Records are in WGS84, the IAP-SP shall convert them to GDA94 for storage and any further processing for consistency with the IAM (*refer B.32.4*) and the IAP in general.

B.16.3 A 'period of continuous operation' shall be defined by a sequence of one or more Position Records, where each adjacent pair of Position Records is separated by 30 ± 1 second. The period of continuous operation is the difference in time between the first and last Position Record in the sequence.

B.16.4 'The last known position' shall be defined as the latitude and longitude within the most recent Position Record or Speed Record (including the IVU Data Record currently being considered) where the vehicle position is not blank/void.

B.16.5 In the case where the vehicle position within a Position Record or a Speed Record is blank/void, the last known position of the vehicle shall be used as the vehicle's position.

Note: A blank/void value in a Position Record or Speed Record is not modified or overwritten. The intent of this requirement is to provide clarity to the processing of IVU Data Records.

B.16.6 The distance between two Position Records shall be determined as the shortest line connecting the two positions.

Note: Where the position within either Position Record is blank/void then the last known position is used in the calculation (see also B.16.4 and B.16.5).

B.16.7 For the purpose of testing SD (Vehicle Type/TCM) Records, a TCM declaration of 'No Load' shall be defined as a TCM greater than zero (*refer B.39.12*).

Note: This does not alter the reporting format of a 'No Load' declaration.

B.17 Data testing

B.17.1 The IAP-SP shall test all incoming IVU Data Records for completeness, consistency and freedom from error.

B.17.2 The IAP-SP shall monitor that, upon receipt of each Data Block another Data Block is received by the IAP-SP System within 72 hours and each 72 hours thereafter.

B.17.3 The IAP-SP shall test:

a) Position Records, Alarm Records and SD Records for consecutive record numbering (*refer A.25.1*); and

b) Speed Records for consecutive record numbering *(refer A.25.2).*

Note: An Alarm is generated in the event that either of the numbering sequences legitimately resets to a lower value (e.g. because all numbers within the sequence have been used (refer A.25.3d).

B.17.4 The IAP-SP shall test that within IVU Data Records, record numbers increase chronologically.

B.17.5 The IAP-SP shall test Data Blocks for integrity and authenticity.

B.17.6 The IAP-SP shall test Position Records, Alarm Records and Speed Records for plausibility.

Note: Any IVU Data Records that are considered implausible are still used in IAP-SP processing.

B.17.7 The IAP-SP shall test that the framing data is complete and consistent.

B.17.8 The IAP-SP shall test Position Records to assess whether, for any continuous period of operation of at least five minutes the following are true of all Position Records:

a) the status of the other independent movement sensor indicated MOVEMENT; and

b) no satellites were used.

B.17.9 The Alarm associated with B.17.8 is generated as soon as a minimum period of five minutes is identified, and is not generated again until the test is first reset (i.e. continuous operation ceases, movement is no longer detected or satellites used is greater than zero) and then the test criteria again met.

B.17.10 The IAP-SP shall identify whenever no satellites were used for a continuous period of operation of at least five minutes and the determined distance between the last Position Record received before the cessation of signal and the first non- blank/void Position Record received after the recommencement of signal, exceeded 500 metres.

B.17.11 The IAP-SP shall test whether the determined distance between the last Position Record prior to a period of non-operation, and the first Position Record after that period of non-operation that has a non-blank/void position, exceeds 500 metres. In the case that there is more than one period of non-operation between these two Position Records, only one Alarm shall be raised.

B.17.12 The IAP-SP shall test whether, for all Position Records in any continuous period of operation of at least 20 minutes:

a) less than four satellites were used; and

b) the other independent movement sensor indicated MOVEMENT.

B.17.13 The Alarm associated with B.17.12 is generated as soon as a minimum period of 20 minutes is identified, and is not generated again until the test is first reset (i.e. continuous operation ceases, the number of satellites used is four or greater, movement is no longer assessed) and then the test criteria again met.

B.17.14 The IAP-SP shall test Position Records to assess whether less than four satellites were used in more than 20% of the most recent 10,000 Position Records.

B.17.15 The Alarm associated with B.17.14 is generated whenever the percentage of Position Records increases from 20% or below to more than 20%.

B.17.16 The IAP-SP shall test Position Records and SD (Vehicle Type/TCM) Records to assess whether, for any continuous period of operation of at least one hour, all of the following are true:

a) all Position Records are within the same Jurisdiction and the last Position Record does not have a blank/void position;

b) the last Position Record has at least one applicable IAC which contains an SD (Vehicle Type/TCM) condition; and

c) Vehicle Type/TCM has not been self declared within the 24 hour period prior to the last Position Record (irrespective of the Jurisdiction in which that data may have been entered).

Note: See also B.38.11

B.17.17 Once the Alarm associated with B.17.16 has been detected the test shall be reset.

Note: This Alarm can be raised multiple times but not more than once every 24 hours.

B.17.18 The IAP-SP shall test whether an IVU was malfunctioning through the monitoring of IVU Data Records.

B.17.19 Alarms associated with B.17.18 are generated when:

a) in any period of 30 seconds, more than ten Type 1 Alarm Records (of the same type) have been generated; or

b) the IVU has a malfunction (of the same type) which continues for seven or more days.

B.17.20 If the alarm associated with B.17.19a has been generated, and the cause is not deemed by the IAP-SP (having regard to B.4.8) to be a potential Tamper, the IAP-SP shall stop the generation of Alarm NCRs (of the same type) until the malfunction has been resolved to the satisfaction of TCA.

Note: This Requirement serves to stop the generation of ongoing IVU Alarm NCRs.

B.17.21 In the event that an occurrence of the type detailed in B.17.1 to B.17.18 inclusive takes place, the IAP-SP shall generate the appropriate Alarm(s) (*refer B.38.2*).

B.17.22 The algorithms to test incoming IVU Data Records to identify Alarms shall be documented, to the satisfaction of TCA.

B.17.23 In the event that any of the above tests reveal any malfunction or indication of malfunction that is specific to:

a) the IVU, then B.4.7 and B.4.10 shall apply;

b) the SDID, then B.8.5 and B.8.8 shall apply; and

c) the IAP-SP System, then B.12.1 and B.12.5 shall apply.

B.18 Data backup and archiving

B.18.1 The IAP-SP shall document and have in place, appropriate procedures for daily backup of data and applications.

B.18.2 The IAP-SP shall test its procedures for data retrieval from backup storage:

a) with a partial data retrieval, no less frequently than once every three months; and

b) with a full data retrieval, no less frequently than once every 12 months.

B.18.3 Full system backups of data, applications and operating system shall be performed before and after any hardware or software changes.

B.18.4 The IAP-SP shall document and have in place, appropriate procedures for the archiving and retrieval of data.

B.18.5 The IAP-SP shall maintain weekly archives, for a period of four years from the date received, of:

a) all data relating to NCRs, including the NCR, the associated IAC and the associated Data Blocks;

b) the original and all revisions of Off-the-shelf IAP Conditions;

c) all versions of the Intelligent Access Map (IAM); and

d) all versions of the IVU software and system application software.

B.18.6 The IAP-SP shall additionally maintain weekly archives, for a period of one year from the date received, of all IAP data not referenced in B.18.5.

B.18.7 The IAP-SP shall, at the expiration of the respective periods referred to in B.18.5 and B.18.6, destroy the archived data.

B.18.8 All archived data shall be stored at two separate places:

a) one copy shall be kept at the IAP-SP's premises; and

b) one copy shall be kept at a secure off-site facility (within five working days of archiving the data).

B.18.9 The IAP-SP shall perform a data retrieval of the archived data within five working days of being requested to do so by either the Jurisdiction, IAC-issuing Jurisdiction or TCA.

B.18.10 The IAP-SP shall test its procedures for archive retrieval no less frequently than once every 3 months.

BUSINESS TO BUSINESS (B2B) DATA INTERCHANGES

B.19 Data interchange

B.19.1 The IAP-SP shall support electronic data interchange with the respective IAC-issuing Jurisdictions and TCA to facilitate the everyday operation of the IAP.

B.19.2 Data interchange shall support data types classified at two levels:

a) Tier 1 (*refer B.42*); and

b) Tier 2 (*refer B.43*).

B.19.3 The following items shall be classified as Tier 1:

a) submission of Part 3 of the IAC by an IAP-SP to an IAC-issuing Jurisdiction (*refer B.23.9*);

b) sending of an IAC by an IAC-issuing Jurisdiction to an IAP-SP (*refer B.24.1 and B.25.3*);

c) an IAP-SP requesting an IAC-issuing Jurisdiction cancel an IAC (*refer B.25.2*);

d) an IAP-SP requesting an IAC-issuing Jurisdiction replace an IAC (*refer B.25.6*);

e) delivery of an NCR by an IAP-SP to an IAC-issuing Jurisdiction (*refer B.33.13*);

f) delivery of a PR by an IAP-SP to an IAC-issuing Jurisdiction (*refer B.41.9*);

g) sending of an IAC by TCA to an IAP-SP (*refer Appendix E.1.6*);

h) delivery of an NCR by an IAP-SP to TCA (*refer Appendix E.1.6*); and

i) delivery of a PR by an IAP-SP to TCA (*refer Appendix E.1.6*).

B.19.4 All non-Tier 1 communication between the respective parties relating to the TCA/IAP-SP Certification Agreement, or this Specification, shall be classified as Tier 2.

B.19.5 All other communication between the respective parties shall be conducted according to normal business practice.

INTELLIGENT ACCESS CONDITION (IAC)

B.20 IAC

B.20.1 An IAC is issued by an IAC-issuing Jurisdiction to a TO. Jurisdictions may grant permission for network access in the form of a scheme for a specified vehicle combination to operate under a specified set of conditions. IAP Conditions, which include spatial and may also include temporal, speed and SD, may form part of those conditions.

B.20.2 When details within an IAC change, the IAC shall be cancelled and if required, a new IAC issued.

B.20.3 Only an IAC-issuing Jurisdiction may cancel an IAC.

B.21 IAC Form

B.21.1 The IAC Form reflects the process by which a TO applies to join an IAP Application.

B.21.2 The IAC Form is described in Appendices B and H and comprises:

a) IAC identifying information;

b) Part 1 – IAP Conditions;

c) Part 2 – TO details;

d) Part 3 – IAP-SP, IVU and TID installation details; and

e) Part 4 – IAC-issuing Jurisdictional assessment.

B.21.3 The data for IAC Identification, Part 1 and Part 2 is collected outside of the B2B environment and held by the IAC-issuing Jurisdiction.

B.21.4 The IAC-issuing Jurisdiction assesses the application and either issues an Interim IAC or terminates the application.

B.21.5 The data for Part 3 is submitted by the IAP-SP to the IAC-issuing Jurisdiction within the B2B environment.

B.21.6 Once the data in Part 4 is added by the IAC-issuing Jurisdiction, the IAC Identification and Parts 1 to 4 of the IAC Form are issued, as the IAC, to the IAP-SP within the B2B environment.

B.22 IAP Conditions – Off-the-shelf and Unique

B.22.1 IAP Conditions as specified in Part 1 are either:

a) Off-the-shelf; or

b) Unique.

B.22.2 Off-the-shelf IAP Conditions will be published as a self-contained document by an IAC-issuing Jurisdiction, and shall be assigned a unique Off-the-shelf IAP Conditions Identifier.

B.22.3 IACs using Off-the-shelf IAP Conditions will do so by reference to the Off-the- shelf IAP Conditions Identifier. This reference shall implicitly be to the most current revision of those Off-the-shelf IAP Conditions for the entire period of the IAC.

Note: If an IAC-issuing Jurisdiction changes any details within a set of Off-the-shelf IAP Conditions the IACs which reference these do not themselves change and there is therefore no requirement to cancel and replace them.

B.22.4 Unique IAP Conditions are embedded within a particular IAC having been negotiated between the TO and the IAC-issuing Jurisdiction.

B.22.5 Unique IAP Conditions cannot be changed. If a change is required, the TO will need to apply to the IAC-issuing Jurisdiction for a new IAC and for the IAC-issuing Jurisdiction to cancel the original.

B.23 Interim IAC

B.23.1 At commencement of the application process, an Interim IAC will be issued by a IAC-issuing Jurisdiction to a TO containing:

a) IAC identifying information and period of applicability;

b) Interim IAC Lapse date;

c) IAP Conditions (Part 1 of the IAC Form);

d) details of the TO (Part 2 of the IAC Form); and

e) details of the vehicle combination (Part 2 of the IAC Form).

B.23.2 The issuing of an Interim IAC indicates the intention of the IAC-issuing Jurisdiction to grant the IAC contingent on the TO engaging an IAP-SP and successful completion of Part 3 of the IAC Form.

B.23.3 The IAP-SP shall enter into a IAP-SP/TO Agreement with the TO detailed in Part 2 of the IAC Form ensuring that the TO details in Part 2 of the IAC Form are identical with the details for the TO in the executed IAP-SP/TO Agreement, if it has not already done so and shall retain for a period of seven years a true copy of the IAP-SP/TO Agreement.

Note: If the IAP-SP has already entered in to an IAP-SP/TO Agreement with the TO, then there is no need for a subsequent IAP-SP/TO Agreement.

B.23.4 If the IAP-SP has at least one active IAC for the vehicle combination detailed in Part 2 of the IAC Form, the IAP-SP shall ensure that:

a) the Registration No., State and Vehicle Identification Number (VIN) or Non-VIN Identifier (if no VIN is available) details for the vehicle combination are the same as those previously provided; and

b) all required information in the IAC Form is provided.

Note: The vehicle combination may be associated with one or more TOs from the same or other IAC-issuing Jurisdiction.

B.23.5 Noting B.23.4, if any such incompleteness or inconsistency, or implausibility of information is detected, the IAP-SP shall return the Interim IAC to the TO with a notation identifying the conflict, to enable the TO to resolve any anomalies with the IAC-issuing Jurisdiction.

B.23.6 If the Interim IAC is complete and consistent, the IAP-SP shall:

a) If IVU, TID and SDID (as necessary) are not already fitted, then the IAP-SP shall check that the vehicle as physically presented by the TO is one and the same with the vehicle as identified in Part 2 of the Interim IAC. If, and only if that vehicle identity is verified then, where IVU, TIDs and SDIDs (as necessary) are not already fitted, the IAP-SP shall install them.

b) If the IVU, TID and SDID (as necessary) are already fitted, then the IAP-SP shall confirm its function in accordance with the Specification.

Note: See also B.3.2.

B.23.7 The IAP-SP shall verify the correct working order of the installed IVU, TIDs and SDIDs (as necessary).

B.23.8 The IAP-SP shall then complete Part 3 of the IAC Form, including (after physical / visual identification of the Vehicle Identification Number (VIN)) the insertion of the VIN of the prime mover/rigid truck and trailer(s) (as necessary) into Part 3 of the IAC Form. If a VIN is unavailable the IAP-SP shall provide a Non-VIN identifier which is the chassis number, or if that is also unavailable, the engine number.

B.23.9 The IAP-SP shall submit the completed Part 3 of the Interim IAC to the IAC-issuing Jurisdiction via Tier 1 data interchange by the Interim IAC Lapse date.

B.23.10 An Interim IAC may be cancelled by the IAC-issuing Jurisdiction at any time after it is issued but prior to it either lapsing or the application being Approved or Denied (*refer B.24.1*).

B.24 IAC Approval

B.24.1 The IAC-issuing Jurisdiction will then approve or deny the IAC (via Part 4 of the IAC Form) and send the complete IAC (including the IAC status i.e. whether Approved or Denied) to the IAP-SP via a Tier 1 data interchange.

Note: Figure 3 shows the data flows involved in acquiring an IAC (numbering within the diagram represents event sequence).

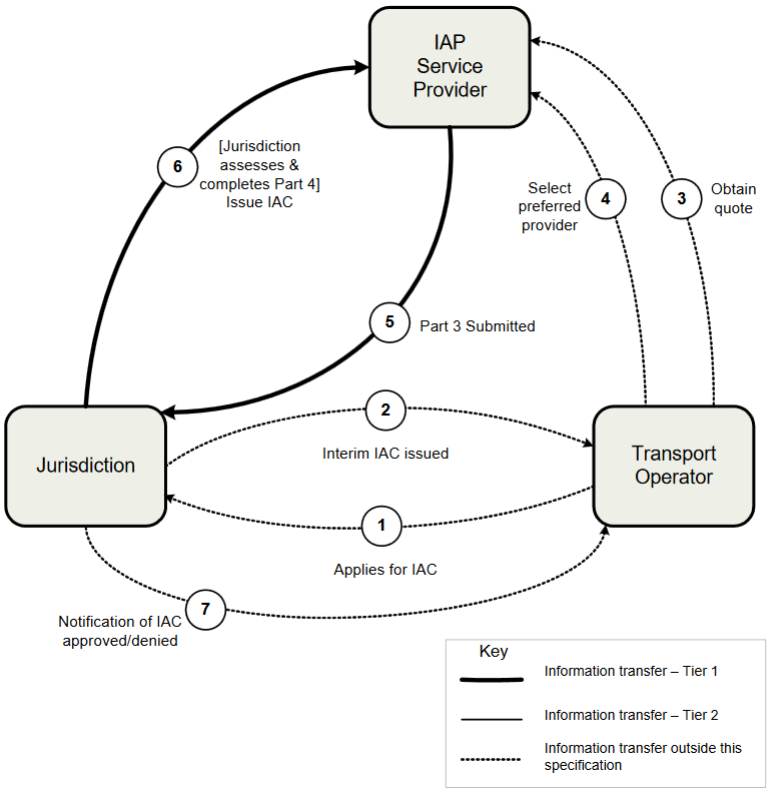


Figure 3: Acquiring an IAC

B.24.2 The IAP-SP System shall be capable of receiving, implementing, and assessing compliance with, the IAP Conditions as defined in the approved IAC.

B.24.3 Where a vehicle is operating under multiple IACs, the IAP-SP shall be capable of assessing compliance against those IACs in accordance with the requirements of this Specification.

B.24.4 The IAP-SP shall be able to commence monitoring the vehicle for compliance with the IAC no later than one working day after electronically receiving the approved IAC from the IAC-issuing Jurisdiction.

B.24.5 The IAP-SP shall activate the IAC on its stated commencement date in accordance with the approved IAC or within one working day after electronically receiving the IAC, whichever is the later.

B.24.6 The IAP-SP shall deactivate the IAC:

a) on the stated cessation date in accordance with the approved IAC;

b) on the 'Valid to' date (refer B.31.2) of a referenced Off-the-shelf Condition, if applicable; or

c) upon receiving a Cancelled IAC (refer B.25.4).

B.25 Cancellation of an IAC

B.25.1 An IAP-SP or a TO may request that an IAC-issuing Jurisdiction cancel an approved IAC. The IAP-SP must state the reasons for the request for cancellation in the comments field.

Note: Refer B.20.3.

B.25.2 An IAP-SP may apply to an IAC-issuing Jurisdiction for a cancellation of an IAC via a Tier 1 data interchange.

B.25.3 In the event that an IAC-issuing Jurisdiction cancels an IAC, the IAC-issuing Jurisdiction will electronically retransmit the complete IAC (which will include the IAC status i.e. Cancelled) to the IAP-SP via Tier 1 data interchange.

B.25.4 The IAP-SP shall deactivate the IAC within one working day after electronically receiving the retransmitted IAC.

B.25.5 If the details contained in either Parts 1 or 2 of an IAC change, the TO will request cancellation of that IAC and then proceed through the normal application process for the issuing of a new IAC.

Note: Figure 4 shows the data flows involved when an IAC-issuing Jurisdiction cancels an IAC either at their own discretion, or at the request of a TO or an IAP-SP (numbering within the diagram represents event sequence).

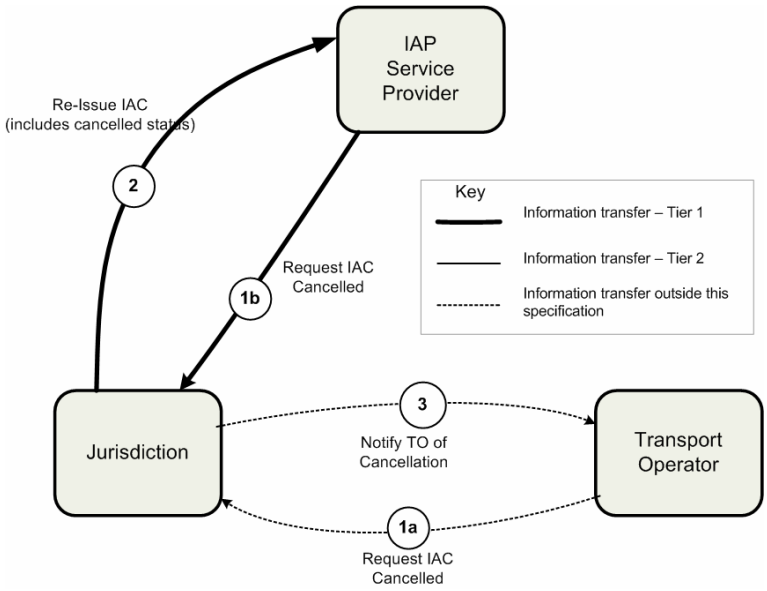


Figure 4: Cancelling an IAC

B.25.6 If the IAP-SP changes any installed device details as documented in Part 3 of the IAC then it shall submit an updated Part 3 to the IAC-issuing Jurisdiction via a Tier 1 data interchange, requesting that the existing IAC be cancelled and that a new IAC be issued.

Note: Any proposed change to the IAP-SP's business details (refer B.54) require prior approval from TCA and re-certification.

B.25.7 The IAC-issuing Jurisdiction will cancel the original IAC and constitute a new IAC, appending the new Part 3 to the original Parts 1 and 2 and transmit it to the IAP-SP via a Tier 1 data interchange.

Note: Figure 5 shows the data flows involved when an IAP-SP requests a replacement IAC (numbering within the diagram represents event sequence).

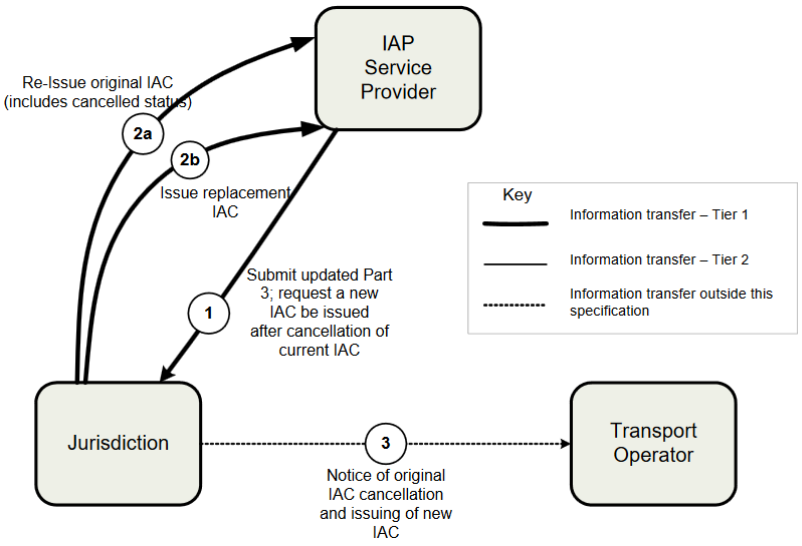


Figure 5: Replacing an IAC

B.26 Spatial Conditions

B.26.1 The IAP-SP shall provide the capability for assessing vehicle spatial compliance with the route and zone conditions, as specified in each IAC issued to that vehicle.

B.26.2 The route and zone Spatial Conditions specified by the IAC shall be confined to the territory of the Jurisdiction and shall be either:

a) where access is allowed (inclusion or absolute-inclusion); or

b) where access is not allowed (exclusion).

Note: See also B.26.13 for the rules concerning assessment against multiple Spatial Conditions within an IAC.

B.26.3 Route and zone conditions will be specified by the IAC-issuing Jurisdiction on the basis of a contiguous set of Links using the Intelligent Access Map (IAM) *(refer B.32*).

B.26.4 Links will be identified via their Persistent IDs using the IAM.

B.26.5 Route conditions will describe a route where access is allowed or not allowed, through a set of contiguous Persistent IDs that define the route from end to end.

B.26.6 The first and/or last Link in a route may be specified as partial Link(s) (rather than as complete Links), where:

a) the start route position is specified by its latitude and longitude, limiting the route definition to that position onwards, and this position must be located along the first Link of the route; and

b) optional end route position is specified by its latitude and longitude, limiting the route definition up to that position, and this position must be located along the last Link of the route.

B.26.7 Where partial Links are specified, and if the route only pertains to a single Link, then both a start route position and an end route position will be provided by the IAC-issuing Jurisdiction (even if that means that a start or end position must align with the actual start or end of the Link).

B.26.8 Where the IAC-issuing Jurisdiction specifies only one latitude/longitude for a partial single Link, the IAP-SP shall interpret the partial Link as extending from the specified position to the northernmost end of the Link. If these are precisely the same value, then the partial Link shall be interpreted as extending from the specified position to the westernmost end of the Link.

B.26.9 Zone conditions will describe an area where access is allowed or not allowed, through a closed polygon of contiguous Persistent IDs that define the boundary of the zone.

B.26.10 A specified route or zone condition will apply 24 hours a day, 7 days a week, while the IAC is active, unless further qualified by a temporal access condition (*refer B.27*).

B.26.11 One or many route and zone conditions may be collated within each IAC to define the cumulative access granted to the vehicle under that IAC (*refer Figure 6).*

Note: While a vehicle may be issued with more than one IAC by an IAC-issuing Jurisdiction, spatial non-compliance is assessed independently against each individual IAC. See also B.34.

B.26.12 Within an IAC, that area of the Jurisdiction which is not covered specifically by Spatial Condition(s) will be denoted as either Inclusion or Exclusion by the IAC-issuing Jurisdiction for that IAC. This area is known as the IAC Background.

B.26.13 Where multiple Spatial Conditions are specified within an IAC, precedence shall be assigned to the Spatial Conditions in the following order:

a) absolute-inclusion (takes precedence over all other);

b) exclusion (takes precedence over inclusion);

c) inclusion; and

d) Background.

B.27 Temporal Conditions

B.27.1 The IAP-SP shall provide the capability for assessing vehicle temporal compliance against Temporal Conditions, as specified in each IAC issued to that vehicle.

B.27.2 Any temporal access conditions specified by an IAC will qualify a corresponding Spatial Condition (*refer B.26*).

Note: Figure 6 is a schematic of a cumulative set of Spatial and Temporal IAP Conditions specified within a single IAC.

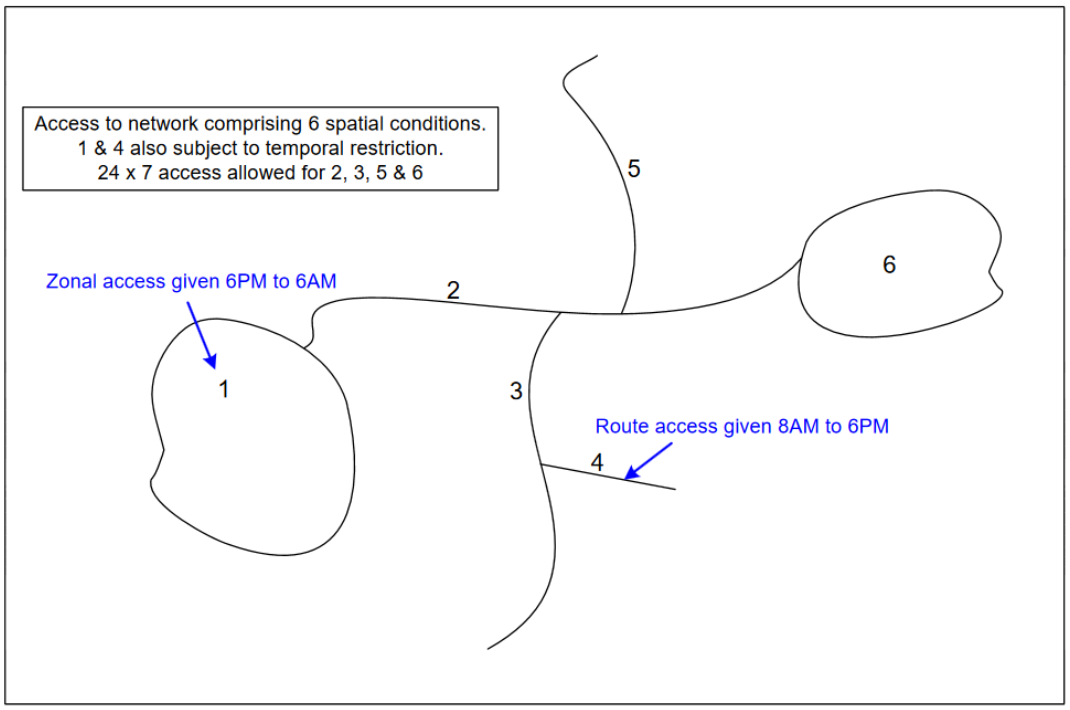


Figure 6: Spatial and Temporal IAP Conditions

B.27.3 Temporal Conditions will be specified on the basis of the local time of the capital city within the Jurisdiction.

B.27.4 Where a Spatial Condition specifies where access is allowed, access will only be permitted for those days/dates and/or times specified through the Temporal Condition.

B.27.5 Where a Spatial Condition specifies where access is not allowed, access will only be restricted for those days/dates and/or times specified through the Temporal Condition.

B.27.6 A Spatial Condition shall be 'In Effect' at the dates and times specified in the Temporal Condition.

Note: See also B.34.8.

B.28 Speed Conditions

B.28.1 The IAP-SP shall provide the capability for assessing the vehicle for compliance with Speed Conditions, as specified in one or multiple IACs issued to that vehicle (*refer Appendix F*).

Note. An IAC cannot comprise a Speed Condition alone. There must also be a Spatial Condition that describes the access granted to the vehicle.

B.28.2 A Speed Condition specified in an IAC shall apply to all usage of the vehicle in the Jurisdiction.

B.29 SD Conditions

B.29.1 The IAP-SP shall provide the capability for assessing SD compliance against the SD Conditions, as specified in one or multiple IACs issued to that vehicle.

Note: An IAC cannot comprise a SD Condition alone. There must also be a Spatial Condition that describes the access granted to the vehicle.

B.30 IAP Conditions Irregularities

B.30.1 The IAP-SP shall report to the IAC-issuing Jurisdiction any instances of apparent irregularity within an IAC, or between multiple IACs (Unique or Off-the-shelf).

Note: Instances of irregularity would include, but not be limited to, the following:

- *if any of the Persistent IDs used to specify a spatial IAP Condition do not exist within the IAM;*
- *if a spatial IAP Condition is to specify a zone and yet the set of supplied Persistent IDs do not form a closed polygon (as is required to specify a zone); and*
- *if an IAC Cessation date is after the referenced IAP Off-the-shelf Conditions 'Valid to' date.*

OFF-THE-SHELF IAP CONDITIONS

B.31 Off-the-shelf IAP Conditions

B.31.1 The IAC-issuing Jurisdiction will be responsible for the supply of Off-the-shelf IAP Conditions to the IAP-SP, including the supply of revisions as may occur from time to time.

Note: Revisions of Off-the-shelf IAP Conditions are assigned a revision number by the IAC-issuing Jurisdiction.

B.31.2 The condition details for Off-the-shelf IAP Conditions will be encoded in accordance with the Conditions schema defined within Appendix H, Annex B.

Note: Off-the-shelf IAP Conditions:

- *specify a required 'Valid from' date and an optional 'Valid to' date; and*
- *will be issued to the IAP-SPs by the IAC-issuing Jurisdictions using a Tier 2 data interchange.*

B.31.3 The IAC-issuing Jurisdiction will provide revisions of Off-the-shelf IAP Conditions at least four weeks prior to the date when the particular Off-the-shelf IAP Conditions revision is required to be adopted by the IAP-SP.

B.31.4 The IAP-SP shall have procedures in place to receive revisions of Off-the-shelf IAP Conditions.

B.31.5 The IAP-SP shall implement testing of revisions of Off-the-shelf IAP Conditions within its IAP-SP System.

B.31.6 The IAP-SP shall advise the relevant IAC-issuing Jurisdiction two weeks prior to the date when the Off-the-shelf IAP Conditions is required to be adopted whether or not it can be loaded and used reliably.

Note: Any irregularities in Off-the-shelf IAP Conditions need to be reported in accordance with B.30.

B.31.7 Noting B.31.6, the IAP-SP shall formally adopt the revised Off-the-shelf IAP Conditions at the time and date specified by the IAC-issuing Jurisdiction. Adoption of the revised conditions shall be in accordance with the 'Valid from' and 'Valid to' dates for the Conditions.

Note: Subject to the agreement of the IAP-SP and the IAC-issuing Jurisdiction, the period for the implementation of the Off-the-shelf IAP Conditions may be reduced.

B.31.8 The adoption of an Off-the-shelf IAP Conditions revision shall be implemented such that all IVU data collected:

a) before the date and time of that adoption, is processed under the old Off-the- shelf IAP Conditions; and

b) on or after that date and time, is processed under the revised Off-the-shelf IAP Conditions.

INTELLIGENT ACCESS MAP (IAM)

B.32 Intelligent Access Map

B.32.1 The IAM will use the Roads Layer of the National Transport Dataset as released and updated periodically by PSMA Australia Ltd (PSMA).

B.32.2 TCA will be responsible for the supply of the IAM to the IAP-SP, including the supply of updated versions.

Note: PSMA aims to release updates for the National Transport Dataset on a quarterly basis. TCA will consider each update and, if appropriate, supply the same to the IAP-SP.

B.32.3 TCA will supply the updated version of the IAM in two forms:

a) a copy of the full new release; and

b) a copy of the incremental change to the previous IAM, when available.

Note: TCA will supply IAP-SPs with IAM updates on DVD.

B.32.4 The IAM will be provided to the IAP-SP in MapInfo vector (.TAB) format.

Note: The IAM uses GDA94.

B.32.5 TCA will provide the updated version of the IAM at least four weeks prior to the date when the update is required to be adopted by the IAP-SPs.

B.32.6 The IAP-SP shall have procedures in place to receive the IAM and receive and implement any updated versions of the IAM.

B.32.7 The IAP-SP shall implement testing of the IAM within its IAP-SP System.

B.32.8 The IAP-SP shall confirm to TCA two weeks prior to the date when the update is required to be adopted that the IAM can be loaded and used reliably.

B.32.9 As a part of the IAM testing, the IAP-SP shall report to the relevant IAC-issuing Jurisdiction any instances where an IAC references any Persistent IDs that are rendered non-existent as a result of the intended IAM update.

B.32.10 The IAP-SP shall formally adopt updated versions of the IAM at the time and date specified by TCA.

B.32.11 The adoption of the updated version of the IAM shall be implemented such that all IVU data collected:

a) before the date and time of that adoption, is processed under the old IAM; and

b) on or after that date and time, is processed under the updated version of the IAM.

IDENTIFICATION OF NON-COMPLIANCE AND ISSUING OF NCRs

B.33 Non-Compliance Reports

B.33.1 The IAP-SP shall assess the IVU Data Records against all applicable IACs to determine whether any non-compliant activity has occurred.

B.33.2 When assessing the applicability of an IAC issued by an IAC-issuing Jurisdiction for the purposes of identifying spatial, temporal, speed and SD non-compliance for a Jurisdiction:

a) if the IAC has only a prime mover/rigid truck identified in Part 2 (no trailers specified) then the IAC applies to that prime mover/rigid truck regardless of any trailers being attached; and

b) if the IAC has trailers identified in Part 2 then the IAC applies only when the vehicle is in the nominated vehicle combination.

B.33.3 For each such identified non-compliant activity, the IAP-SP shall generate and issue a Non-Compliance Report (NCR) as specified in Appendices C and H.

B.33.4 An NCR shall list all the applicable IACs against which the non-compliant activity was assessed:

a) a Spatial/Temporal NCR lists only the individual IAC against which the non-compliant activity was assessed;

b) a Speed NCR lists all applicable IACs which include a Speed Condition; and

c) a SD (Vehicle Type/TCM) NCR lists all applicable IACs which include a SD (Vehicle Type/TCM) Condition.

B.33.5 Each NCR shall be issued to the IAC-issuing Jurisdiction, reporting only non-compliant activity occurring within that Jurisdiction, with the exception of Alarm NCRs (see B.38).

B.33.6 Each NCR shall be assigned a unique identifier.

Note: TCA will provide each IAP-SP with a unique, three character identifier which the IAP-SP shall use as a prefix in the NCR identifier.

B.33.7 An NCR shall contain the time and date upon which it was generated, which shall be based upon the IAP-SP's local time.

B.33.8 An NCR shall identify the Version Numbers, as implemented in the IAP-SP System at the time of the NCR's audit reference date/time stamp (*refer B.40.1*), for the following:

a) IAP Functional & Technical Specification; and

b) IAM.

B.33.9 Each NCR shall identify the nature of the non-compliant activity for that particular NCR (spatial, temporal, speed, alarm or SD).

B.33.10 The NCR shall summarise the period of spatial, temporal or SD (Vehicle Type/TCM) non-compliant activity by providing beginning date/time and position, ending date/time and position, and total duration (*refer Appendices C and H*).

Note: The beginning date/time is the date/time of the first Position Record which triggers the NCR, except for a Continuation NCR (refer B.34.17 and B.39.9), in which case it is 72 hours after the beginning time of the previous NCR.

The ending date/time is the date/time of the last Position Record in the non- compliant period, except for a Continued NCR (refer B.34.17 and B.39.9), in which case it is 72 hours after its beginning time.

Position as recorded in the summary is the last known position of the vehicle.

B.33.11 Where the IACs listed in the NCR include trailer details, the NCR shall detail only those trailers which are identified in the associated NCR Data Records.

B.33.12 The NCR data shall, as applicable, include the following records:

a) NCR Position Records (*refer B.36.1*);

b) NCR Speed Records (*refer B.36.1*);

c) NCR Alarm Records Type 1 (*refer B.38.3*);

d) NCR Alarm Records Type 2A (*refer B.38.7*);

e) NCR Alarm Records Type 2B (*refer B.38.8*); and

f) NCR SD Records (*refer B.39.14*).

B.33.13 The NCRs shall be delivered to the IAC-issuing Jurisdiction via Tier 1 data interchange.

Note: Figure 7 shows the data flows involved in issuing an NCR (numbering within the diagram represents event sequence).

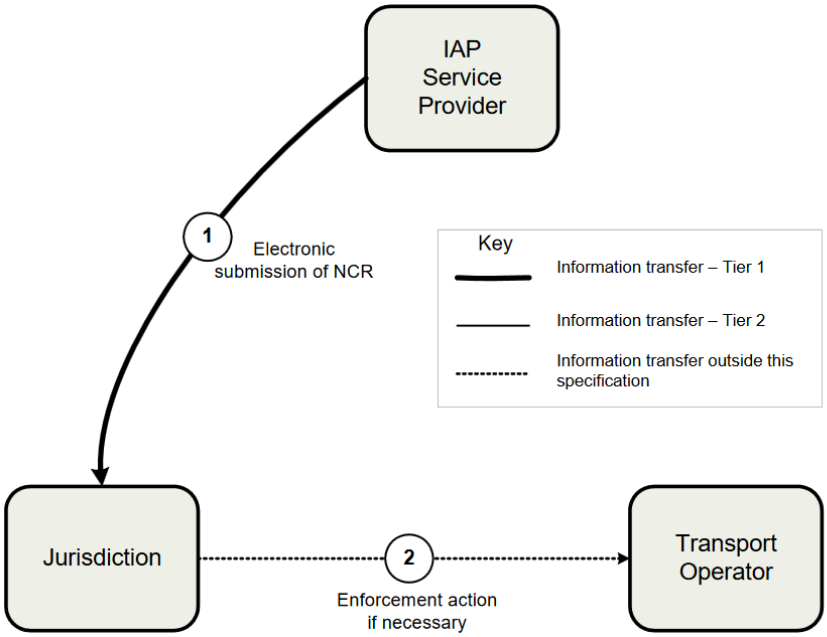


Figure 7: Issuing an NCR

B.33.14 The IAP-SP shall issue an NCR no later than one working day after transfer of the relevant IVU Data Records from the IVU and SD Records entered through an alternative to SDID use facility.

Note: SD Records shall not be considered relevant where applicable IACs do not include SD Conditions.

B.33.15 The IAP-SP shall consolidate all data applicable to the NCR and shall:

a) store it in accordance with B.18.5, for potential use by the IAC-issuing Jurisdiction(s); and

b) promptly provide all necessary assistance to those IAC-issuing Jurisdiction(s) in such action as they may wish to take with respect to the NCR.

B.34 Spatial and Temporal compliance

B.34.1 A vehicle shall be independently assessed for spatial and temporal compliance against each applicable IAC issued to it.

B.34.2 Using the IAM, the IAP-SP shall assess each Position Record against the set of spatial and temporal IAP Conditions within each IAC. Non-compliance shall be described as either spatial or temporal non-compliance.

B.34.3 When assessing spatial non-compliance, the applicable IACs shall be those pertaining to the vehicle combination, date/time and vehicle position as specified within the Position Record.

B.34.4 An IAC inclusion route (a route that is allowed) shall be defined as within 100 metres of the road centreline from the IAM.

B.34.5 An IAC exclusion route (a route that is not allowed) shall be defined as within 100 metres of the road centreline from the IAM.

B.34.6 An IAC inclusion zone (a zone that is allowed) is the zone defined by the road centreline from the IAM defining the inclusion zone boundary, extended outwards from the road centreline by 100 metres.

B.34.7 An IAC exclusion zone (a zone that is not allowed) is the zone defined by the road centreline from the IAM defining the exclusion zone boundary, extended inwards from the road centreline by 100 metres.

B.34.8 An inclusion or exclusion route or zone may be further qualified by Temporal Conditions which limit when the Spatial Conditions are In Effect (*refer B.27.6 and B.34.11*).

B.34.9 When assessing spatial non-compliance of a Position Record against the set of Spatial Conditions within an applicable IAC, assessment shall be according to the following:

a) identify the set of Spatial Conditions which are relevant to the vehicle's position;

b) select those conditions which are 'In Effect' at the time of data collection; and

c) separate these 'In Effect' conditions into the hierarchy (absolute-inclusion, exclusion, inclusion).

B.34.10 To determine precedence of conditions within an IAC, the IAP-SP shall assess each Position Record against the 'In Effect' conditions according to the following precedence rules:

a) if an absolute-inclusion condition is present, the vehicle is compliant – otherwise;

b) if an exclusion condition is present, the vehicle is non-compliant – otherwise;

c) if an inclusion condition is present, the vehicle is compliant – otherwise;

d) if Background is inclusive, the vehicle is compliant – otherwise;

e) if Background is exclusive, the vehicle is non-compliant.

B.34.11 Where spatial non-compliance of a Position Record has been identified in accordance with B.34.9 and B.34.10 the IAP-SP shall subsequently assess if the vehicle is additionally temporally non-compliant.

B.34.12 Temporal non-compliance of a Position Record shall be deemed to have occurred when:

a) the vehicle is spatially non-compliant at that position; and

b) there is at least one Temporal Condition which applies to that position.

B.34.13 An IAP-SP shall trigger an NCR when two or more consecutive Position Records are found to be spatially non-compliant and the first two triggering Position Records are generated within 72 hours of each other.

Note: Such a Spatial NCR may be subsequently assessed as Temporal (refer B.34.18).

B.34.14 The NCR shall include all NCR Position Records for the full period of non- compliance, this being the set of NCR Position Records commencing with the first non-compliant Position Record and ending with the first collected of either:

a) the last non-compliant Position Record preceding the first subsequent compliant Position Record;

b) the last non-compliant Position Record collected within 72 hours of the first non-compliant Position Record; or

c) the last Position Record collected prior to some event occurring which renders the IAP-SP unable to continue assessing the non-compliant activity.

Note: (c) includes events such as a spatially non-compliant vehicle exiting across the Jurisdiction's border.

B.34.15 Where the Position Record immediately preceding the first non-compliant Position Record in an NCR is compliant, the NCR shall also include that record and all other preceding NCR Position Records for a period of five minutes, but excluding any Position Records in which the vehicle was not in the Jurisdiction.

B.34.16 Where the Position Record immediately following the last non-compliant Position Record in an NCR is compliant, the NCR shall also include that record and all other subsequent NCR Position Records for a period of five minutes, but excluding any Position Records in which the vehicle was not in the Jurisdiction.

B.34.17 In the event that the period of non-compliant activity continues for more than 72 hours (*refer B.34.14b*), the IAP-SP shall generate NCRs after each 72 hour period of non-compliant activity. NCRs which record such continuous non-compliant activity shall identify the NCR covering the prior 72 hour period by its NCR identifier.

Note: An NCR which runs the full 72 hours is known as a Continued NCR; it is followed by a Continuation NCR. Such a Continuation NCR may itself become a Continued NCR if the reported period of non-compliant activity reaches 72 hours.

B.34.18 A period of non-compliant activity ends if the 72 hour period following receipt of the last non-compliant Position Record contains no additional received IVU Data Records.

Note: In this case, the NCR is not a Continued NCR, even if Position Records are received after the 72 hour period indicating ongoing non-compliant activity; such Position Records represent a new period of non-compliant activity and do not form a Continuation NCR.

This addresses the scenario where a Continuation NCR is normally expected but the vehicle ceases operation for an extended period of time.

B.34.19 If a vehicle remains temporally non-compliant for every NCR Position Record throughout the period of non-compliance covered in the NCR then the non- compliant activity shall be identified as 'Temporal' in the NCR (*refer B.33.9*).

B.34.20 The algorithms to compare Position Records to IAC routes and zones and to check for spatial and temporal compliance shall be documented, to the satisfaction of TCA.

B.35 Speed compliance

B.35.1 When the applicable IACs over the period of a Speed Event include at least one Speed Condition, the IAP-SP shall assess and report the Speed Event, in an NCR denoted as 'Speed', to each IAC-issuing Jurisdiction which issued an applicable IAC which specified a Speed Condition.

Note: In the case where a Speed Event crosses a Jurisdiction's border, a Speed NCR may be issued to each of the IAC-issuing Jurisdictions, subject to a Speed Condition being applicable to that Jurisdiction.

A Speed NCR will be issued regardless of whether the vehicle is spatially or temporally compliant or non-compliant over the period of the Speed Event.

B.35.2 When assessing speed non-compliance the applicable IACs shall be those pertaining to the vehicle combination, date / time and vehicle position as specified within the Speed Record.

B.35.3 All Speed Records for the Speed Event shall be included in the NCR in the form of NCR Speed Records.

B.36 NCR Position Records and NCR Speed Records

B.36.1 The IAP-SP shall process Position Records and Speed Records to form NCR Position Records and NCR Speed Records respectively for inclusion in an NCR, by:

a) including Jurisdiction local date and time (derived from UTC date and time of generation); and

b) assessing vehicle position (latitude and longitude) against the IAM to identify the location (i.e. relevant Persistent ID, road name, locality, State) as follows:

i) if the vehicle position is within 13 metres of a road centreline, then all location details shall be assigned to the NCR record; but

ii) if the vehicle position is not within 13 metres of a road centreline or there are two or more possible roads, then all location details shall be left blank.

B.36.2 The IAP-SP shall additionally for each Position Record, when forming NCR Position Records, indicate whether it represents 'compliant' or 'non-compliant' activity.

Note: Within Spatial, Temporal and SD (Vehicle Type/TCM) NCRs, those NCR Position Records that fall within the NCR summary period as defined in B.33.10 are considered non-compliant, and the other NCR Position Records (i.e. those within the lead-in or lead-out period) are considered compliant. Within an Alarm NCR all NCR Position Records are considered compliant. This convention is adopted for ease of use.

B.36.3 The IAP-SP shall additionally for Speed Records, when forming NCR Speed Records, include the IAP Speed Threshold.

B.37 SD Data in Spatial, Temporal and Speed NCRs

B.37.1 For Spatial, Temporal and Speed NCRs, if at least one of the IACs listed in the NCR includes at least one SD Condition, the NCR shall include:

a) for each included SD Condition type, all NCR SD Records (relevant to that SD Condition type) from the 24 hour period prior to the NCR Summary beginning date/time for Spatial and Temporal NCRs and the first included Speed Record for a Speed NCR; and

b) for each included SD Condition type, all NCR SD Records (relevant to that SD Condition type) for:

i) the period of 12 hours after the start of the non-compliance; and

ii) the entire non-compliant period if non-compliant for more than 12 hours.

Note: All SD data collected within the specified time periods is included, irrespective of the Jurisdiction.

B.38 Alarm NCRs

B.38.1 The IAP-SP shall check for the presence of:

a) Alarm Records transferred from the IVU in accordance with A.23; and

b) IAP-SP System generated Alarms in accordance with B.17.19.

B.38.2 The IAP-SP shall use the Alarm Codes shown in Table 1, when reporting Alarm Records and Alarms, categorised as follows:

a) Alarm Codes 1 to 12 relate to Alarm Records; and

b) Alarm Codes 51 to 59 and 80 to 86 relate to Alarms.

Table 1: Summary of Alarm Codes

Alarm Code	Alarm Description (to assist interpretation only; requirement details are found at the appropriate Reference)	Reference	Alarm Record Type
1	External power supply disconnected from IVU	A.23.1a	
2	External power supply reconnected to IVU	A.23.1b	
3	External power supply disconnected from IVU - Vehicle movement indicated by ignition	A.23.1c	1
4	External power supply disconnected from IVU - Vehicle movement detected by other independent movement sensor	A.23.1d	1
5	Ignition disconnected	A.23.1e	1
6	Ignition reconnected	A.23.1f	1
7	Other independent movement sensor disconnected	A.23.1g	1
8	Other independent movement sensor reconnected	A.23.1h	1
9	Unauthorised access to data in IVU detected	A.23.1i	1
10	Unauthorised access to IVU software detected	A.23.1j	1
11	GPS antenna disconnected from IVU	A.23.1k	1
12	GPS antenna reconnected to IVU	A.23.1l	1
51	No Vehicle Type and TCM data self declared, when required, where at least one SD (Vehicle Type/TCM) Condition is applicable	B.17.16	2A
52	Position Records, Alarm Records and SD Records are not numbered consecutively	B.17.3a	2A
53	Speed Records are not numbered consecutively	B.17.3b	2A
54	IVU Data Record numbering does not increase chronologically	B.17.4	2A
55	After a period of non-operation, the distance between the Position Record before and the Position Record after that period exceeds 500 metres	B.17.11	2A
56	Zero satellites used for a continuous period of operation of at least five minutes while the vehicle was moving	B.17.8	2A
57	After a period where zero satellites were used for a continuous period of operation of at least five minutes, the distance between the Position Record before and the Position Record after the cessation of signal, exceeds 500 metres	B.17.10	2A
58	Less than four satellites used for a continuous period of operation of at least 20 minutes, while the vehicle was moving	B.17.12	2A
59	Less than four satellites used in more than 20% of a sequence of 10,000 Position Records	B.17.14	2A
80	No Data Blocks have been received within a 72 hour period	B.17.2	2B
81	Loss of integrity and/or authenticity of Data Blocks	B.17.5	2B
82	Incomplete or inconsistent framing data	B.17.7	2B
83	IVU Data Records incomplete, inconsistent or containing errors	B.17.1	2B
84	Implausibility of incoming Position, Alarm and Speed Records	B.17.6	2B
85	IVU defective for more than seven days	B.17.19	2B
86	Type 1 Alarm Malfunction – Threshold reached	B.17.19	2B

B.38.3 The IAP-SP shall process Alarm Records from the IVU with Alarm Codes 3 to 12 to form NCR Alarm Records Type 1, by including Jurisdiction local date and time (derived from UTC date and time of generation).

B.38.4 Alarm Records with Alarm Codes 3 to 12 shall be reported by the generation of an NCR containing:

a) the NCR Alarm Record Type 1;

b) NCR Position Records for the vehicle generated for a period of one hour prior to the UTC date and time in the triggering Alarm Record; and

c) Alarm Records with Alarm Codes 1 and 2 for a period of one hour prior to the UTC date and time in the triggering Alarm Record.

B.38.5 *Note: This requirement has been removed.*

B.38.6 The algorithm to identify the Alarm Codes for Alarm Records shall be documented, to the satisfaction of TCA.

B.38.7 When an Alarm is detected whose associated Alarm Code is 51 to 59, an NCR shall be generated, supported by the following:

a) NCR Alarm Record Type 2A consisting of:

(i) Alarm Code;

(ii) UTC date and time of the last generated IVU Data Record that contributed to the Alarm being identified; and

(iii) the associated Jurisdiction local date and time (derived from UTC date and time).

b) NCR Position Records for the vehicle generated over a period of one hour prior to the UTC date and time in the triggering NCR Alarm Record.

B.38.8 When an Alarm is detected whose associated Alarm Code is 80 to 86, an NCR shall be generated. Any such Alarm NCR contains the triggering NCR Alarm Record Type 2B consisting of:

a) Alarm Code;

b) UTC date and time of the last generated IVU Data Record that contributed to the Alarm being identified; and

c) the associated Jurisdiction local date and time (derived from UTC date and time).

B.38.9 For Type 1 or Type 2A Alarm NCRs, if at least one of the IAC-issuing Jurisdiction's applicable IACs includes at least one SD Condition, the NCR shall include:

a) for each included SD Condition type, all NCR SD Records (relevant to that SD Condition type) from the 24 hour period prior to the UTC date and time in the triggering NCR Alarm Record; and

b) for each included SD Condition type, all NCR SD Records (relevant to that SD Condition type) for the 12 hour period after that date/time.

Note: All SD data collected within the specified time periods is included, irrespective of the Jurisdiction.

B.38.10 For Alarm NCRs the applicable IACs shall be those which are active at the UTC date and time within the triggering NCR Alarm Record irrespective of any consideration of vehicle combination.

B.38.11 An Alarm NCR shall be generated and issued to each IAC-issuing Jurisdiction, excluding Alarm NCR (Alarm Code 51), which shall be generated and issued only to the IAC-issuing Jurisdiction associated with the Jurisdiction in which the vehicle was in operation when the Alarm was triggered.

B.38.12 The IAP-SP shall:

a) continuously monitor for evidence of tampering, or attempted tampering, with the IVU and its data, assessing the nature and types of Alarm Records and Alarms, together with all other information and evidence available from the vehicle and from inspection and investigation; and

b) immediately report to the IAC-issuing Jurisdiction(s) in accordance with B.4.8 and B.4.9.

B.39 Assessment of SD data against SD Conditions

B.39.1 When assessing SD non-compliance the applicable IACs shall be those pertaining to the vehicle combination, date/time and vehicle position as specified within the Position Record.

B.39.2 For each Position Record the IAP-SP shall assess SD (Vehicle Type/TCM) non-compliance using:

a) the most recent SD (Vehicle Type/TCM) Record, irrespective of the Jurisdiction in which it was generated; and

b) the SD (Vehicle Type/TCM) Conditions identified in the applicable IACs for that Position Record.

Note: The only IAP SD Condition assessed for compliance is the SD (Vehicle Type/TCM) Condition.

B.39.3 Noting B.39.2, an IAP-SP shall trigger an NCR, denoted as ‘SD (Vehicle Type/TCM)’, when a self declared TCM value exceeds the TCM Threshold for the Vehicle Type.

Note: Each vehicle will have no more than one set of SD (Vehicle Type/TCM) Conditions per Jurisdiction.

An SD (Vehicle Type/TCM) NCR will be issued regardless of whether the vehicle is spatially or temporally compliant or non-compliant over the period of non- compliance.

A TCM Threshold of zero indicates that the Vehicle Type is not permitted, even if ‘no load’ is declared.

A Vehicle Type not listed in the SD Conditions is considered to have a TCM Threshold of zero.

B.39.4 The period of SD (Vehicle Type/TCM) non-compliance shall start at the time of the first Position Record in the Jurisdiction where SD (Vehicle Type/TCM) non-compliance was identified.

B.39.5 The period of non-compliance shall end with the last Position Record prior to the first identified of either:

a) the next compliant SD (Vehicle Type/TCM) Record;

b) 72 hours from the commencement of non-compliance; or

c) some event occurring which renders the IAP-SP unable to continue assessing the non-compliant activity.

Note: (c) includes events such as a SD (Vehicle Type/TCM) vehicle exiting across the Jurisdiction's border.

B.39.6 The SD (Vehicle Type/TCM) NCR shall include the following NCR SD (Vehicle Type/TCM) Records (*refer B.39.14*):

a) all those within the 24 hour period prior to the start of the non-compliant activity;

b) the most recent prior to the start of the non-compliant period (if not already provided);

c) all those from the start of the non-compliant period to either the end of that period or 12 hours after the start of that period, whichever is later; and

d) the next compliant SD (Vehicle Type/TCM) Record in the case that the non-compliant period ended according to B.39.5a. (if not already provided).

Note: All SD data collected within the specified time periods is included, irrespective of the Jurisdiction.

B.39.7 The SD (Vehicle Type/TCM) NCR shall include all NCR SD (Comments) Records (*refer B.39.14)*:

a) within the 24 hour period prior to the start of the non-compliant activity; and

b) from the start of the non-compliant period to either the end of that period or 12 hours after the start of that period, whichever is later.

Note: All SD data collected within the specified time periods is included, irrespective of the Jurisdiction.

B.39.8 The SD (Vehicle Type/TCM) NCR shall additionally include the Position Records for the period of SD (Vehicle Type/TCM) non-compliance, and (where available) the five minutes before and the five minutes after the period of non-compliance, but excluding any Position Records in which the vehicle was not in the Jurisdiction.

B.39.9 In the event that the period of non-compliant activity continues for more than 72 hours (*refer B.39.5b*), the IAP-SP shall generate NCRs after each 72 hour period of non-compliant activity. NCRs which record such continuous non-compliant activity shall identify the NCR covering the prior 72 hour period by its NCR identifier.

Note: An NCR which runs the full 72 hours is a Continued NCR; it is followed by a Continuation NCR. Such a Continuation NCR may itself become a Continued NCR if the reported period of non-compliant activity reaches 72 hours.

B.39.10 The IAP-SP shall allocate a Vehicle Category Code to a self declared Vehicle Category as issued by TCA.

Note: See also C.5.1.

B.39.11 The IAP-SP shall allocate zero to the Number of Axles in the case that 'N/A' was self declared (*refer C.5.1*).

B.39.12 The IAP-SP shall allocate a Vehicle Load Status (*refer Appendix C*) of 'No Load' to a self declared TCM of 'No Load' (*refer C.5.3*).

B.39.13 The IAP-SP shall allocate a Comment Code to a self declared Comment Name as issued by TCA.

Note: See also C.6.1.

B.39.14 The IAP-SP shall process SD Records to form NCR SD Records by including:

a) Jurisdiction local date and time (derived from UTC date and time of generation);

b) for the vehicle, its last known position in latitude and longitude and the UTC date and time of that position (*refer B.16.4*);

c) GPS quality of the last known position reading, comprising:

i) number of GPS satellites; and

ii) HDOP;

d) vehicle location (i.e. relevant Persistent ID, road name, locality, State) at last known position of the vehicle as follows:

i) if the vehicle position is within 13 metres of a road centreline, then all location details shall be assigned to the NCR record; but

ii) if the vehicle position is not within 13 metres of a road centreline or there are two or more possible roads, then all location details shall be left blank.

B.39.15 The algorithm to compare SD (Vehicle Type/TCM) Records with SD Conditions shall be documented, to the satisfaction of TCA.

B.40 Audit reference date/time stamp

B.40.1 An NCR shall contain an audit reference date/time stamp, in Jurisdiction local date and time, which shall be based upon the following deterministic algorithm:

a) for a Spatial, Temporal or SD NCR, the NCR Summary ending date and time;

b) for a Speed NCR, the IVU date and time of the last Speed Record of the Speed Event;

c) for an Alarm NCR Type 1, the IVU date and time of the last NCR Alarm Record (i.e. the Alarm Record that triggered the Alarm NCR being generated); and

d) for an Alarm NCR Type 2A and Type 2B, the IVU date and time of the triggering NCR Alarm Record.

Note: In the TCA Audit System (TAS) (refer Appendix G), it is important to be able to:

- *reliably match TAS generated NCRs against IAP-SP generated NCRs. The deterministic audit reference date/time stamp facilitates this process; and*
- *reliably replicate PRs generated by the IAP-SP. The deterministic audit reference date/time stamp facilitates this by providing a means of allocating an NCR to a PR reporting period. See also B.41.5.*

PARTICIPANTS REPORT (PR)

B.41 Participants Report

B.41.1 The IAP-SP shall issue Jurisdiction specific Participants Reports (PRs) monthly as specified in Appendices D and H.

B.41.2 The IAP-SP shall generate a PR for every Jurisdiction for which an IAC-issuing Jurisdiction issued IAC(s) that were applicable to any of the vehicles being monitored by the IAP-SP during the reporting period.

B.41.3 The PR shall report upon all vehicles which were monitored for a Jurisdiction at some time during the reporting period, which shall start and end based upon the Jurisdiction's local date and time (which may differ from that of the IAP-SP).

B.41.4 Each PR shall be assigned a unique identifier.

Note: TCA will provide each IAP-SP with a unique, three character identifier which the IAP-SP shall use as a prefix in the PR identifier.

B.41.5 The IAP-SP shall use the audit reference date/time stamp for an NCR (*refer B.40*) in assigning it to a particular PR reporting period, for the purposes of establishing the NCR tallies for the respective vehicles for the period.

B.41.6 The PR shall contain the time and date of generation of the report, which shall be based upon the IAP-SP's local time.

B.41.7 The IAP-SP shall, if later requested by TCA, revise the standard period against which the PR is reported for Jurisdictions to a shorter (e.g. daily, weekly) or longer timeframe (e.g. quarterly).

B.41.8 The IAP-SP shall issue each PR by the 7th day of the following month, or the next working day if the 7th day of the month is a non-working day.

B.41.9 The PR shall be delivered to the IAC-issuing Jurisdiction via Tier 1 data interchange.

B.41.10 Noting B.41.9, the PR shall also be delivered to TCA via Tier 1 data interchange.

Note: Figure 8 shows the data flows involved in issuing a PR (numbering within the diagram represents event sequence).

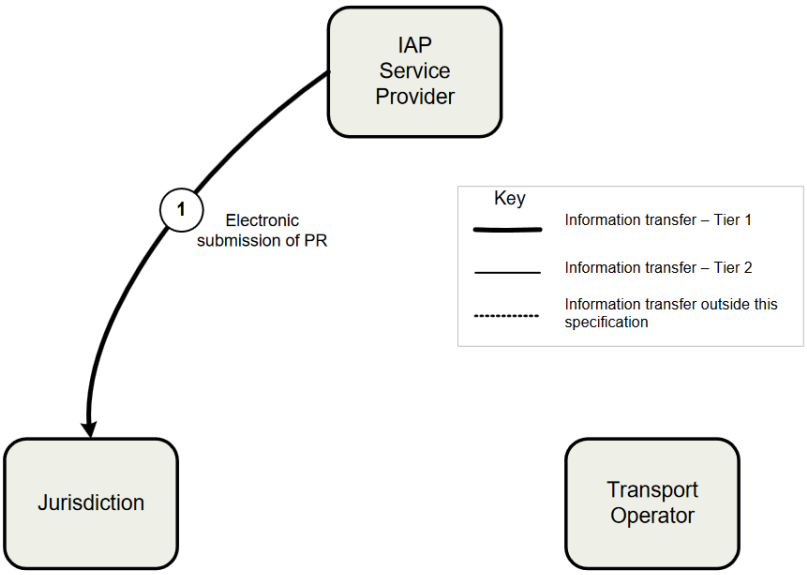


Figure 8: PR Data Flow

TIER 1 AND TIER 2 DATA INTERCHANGE

B.42 Tier 1 data interchange – B2B

B.42.1 Tier 1 data interchange shall be supported using an automated B2B interface, employing web services, as specified in Appendix H.

Note: See also B.19.3.

B.42.2 The IAP-SP shall be responsible for the implementation of the IAP-SP elements of the B2B interface being as follows:

a) the provision of IAP-SP client-side elements invoking IAC-issuing Jurisdiction services;

b) the provision of IAP-SP server-side elements to support IAC-issuing Jurisdiction client activity;

c) logging of transactions requested, and of actions performed;

d) error checking and error response actions;

e) the provision of suitably dimensioned hardware; and

f) sufficient Internet bandwidth to meet transmission requirements.

B.42.3 The IAC-issuing Jurisdictions will be responsible for the implementation of their corresponding IAC-issuing Jurisdiction elements of the B2B interface.

B.42.4 The B2B interface shall use the Internet as the transmission network for transactions.

B.42.5 Confidentiality of B2B transactions shall be provided via an SSL connection between the client and server, using server-side authentication.

B.42.6 The PKI infrastructure associated with the issue and management of the SSL certificates used by the IAP-SP to meet B2B interface requirements shall be subject to approval by TCA.

Note: The operation of the IAP, including its data security, must be beyond reproach. Hence SSL certificates must be issued through a well-credentialed certification authority and registration authority. PKI infrastructure must provide all relevant certificate management services (e.g. 100 point ID checks by registration authority, support for certificate revocation, etc).

B.42.7 Integrity of B2B transactions shall be provided by transaction signing using an Australian Business Number Digital Signature Certificate (ABN-DSC) Device (Type 3) X.509 digital certificate.

Note: Further information concerning ABN-DSC may be obtained from TCA.

B.42.8 Tier 1 data interchange shall support the IPv4 protocol.

B.43 Tier 2 data interchange

B.43.1 Tier 2 data interchange shall be supported using secure email, ftps, registered mail and/or secure web portal.

Note: See also B.19.4.

B.43.2 For the purposes of Tier 2 data interchange via secure email, the IAP-SP shall:

a) utilise an IAP specific email address within its organisation (e.g. iap@serviceprovidername.com.au);

b) sign transmitted emails (*refer B.43.3*);

c) maintain electronic registers of transmissions to and from other parties for the purposes of checking the integrity and completeness of email transmissions; and

d) acknowledge receipt of email.

B.43.3 Secure email shall be digitally signed using the S/MIME secure email format.

B.43.4 Secure email shall not be encrypted.

B.43.5 Secure email shall be signed by a digital certificate that has a 1024 bit RSA key pair, encodes the email address of the sender, and is issued by a Certification Authority (CA) for which the IAP-SP has sought and gained approval from TCA.

B.43.6 For the purposes of Tier 2 data interchange via ftps, the IAP-SP shall:

a) implement ftps using SSL and associated security infrastructure;

b) use ftps for communication with TCA for data interchanges as outlined in Appendix E; and

c) provide details of its implementation for the approval of TCA.

B.43.7 For the purposes of Tier 2 data interchange via registered mail, the IAP-SP shall appropriately register and file copies of such communications.

B.43.8 For the purposes of Tier 2 data interchange via a secure web portal, the IAP-SP shall:

a) access the secure web portal via an up-to-date web browser or via the IAP-SP System;

b) use the secure web portal for reporting to IAC-issuing Jurisdictions and TCA (as applicable) malfunctions and possible tampering in relation to the IVU, TID, SDID, IAP-SP System and Quality System; and

c) document, to the satisfaction of TCA, details of its implementation.

B.43.9 The IAC-issuing Jurisdictions and TCA will be responsible for the implementation of their Tier 2 data interchange requirements.

B.43.10 IAP-SP requests for approval by TCA shall be submitted as a Tier 2 data interchange, with supporting information appropriate for the approval request.

B.43.11 Any TCA response approving or rejecting a request for approval will be provided as a Tier 2 data interchange. No verbal communication or representations will be binding.

B.43.12 Table 2 provides a non-exhaustive list of Tier 2 data interchanges.

Note: It is anticipated that some NCRs (e.g. Alarm NCRs) will require Tier 2 reports that will provide additional detail to the IAC-issuing Jurisdiction.

Table 2: Non-Exhaustive List of Tier 2 Data Interchanges

Item of Information	From	To
Request re-certification by TCA for Type-approved IVU hardware or software	IAP-SP	TCA
Report IVU, TID or SDID malfunction	IAP-SP	IAC-issuing Jurisdiction and TCA
Report rectification of IVU, TID or SDID malfunction	IAP-SP	IAC-issuing Jurisdiction and TCA
Report IVU, TID or SDID tampering	IAP-SP	IAC-issuing Jurisdiction
Report IVU, TID or SDID repeated malfunctions	IAP-SP	TCA
Request re-certification by TCA for Type-approved TID hardware or software	IAP-SP	TCA
Advise when 80% of IVUs are in service	IAP-SP	TCA
Supply Off-the-Shelf IAP Conditions (and revisions)	IAC-issuing Jurisdiction	IAP-SP
Advise concerning adoption of revision of Off-the-Shelf IAP Conditions	IAP-SP	IAC-issuing Jurisdiction
Report IAP Conditions' Irregularities	IAP-SP	IAC-issuing Jurisdiction
Notify dispatch of IAM updates	TCA	IAP-SP
Confirm that newly received IAM is functional	IAP-SP	TCA
Report of non-existent Persistent IDs resulting from IAM update	IAP-SP	IAC-issuing Jurisdiction
Advise adoption date for updated IAM version	TCA	IAP-SP
Request for approval by TCA for IAP-SP PKI Infrastructure arrangements	IAP-SP	TCA
Report IAP-SP System malfunction	IAP-SP	TCA
Report IAP-SP System tampering	IAP-SP	TCA
Report IAP-SP System repeated malfunctions	IAP-SP	TCA
Report IAP-SP Quality System malfunction	IAP-SP	TCA
Report IAP-SP Quality System tampering	IAP-SP	TCA
Report quality of performance of algorithms	IAP-SP	TCA
Provide Annual Report concerning IAP-SP Quality System	IAP-SP	TCA
Provide internal and external Audit Reports	IAP-SP	TCA
Report failure of Quality Monitoring Station	IAP-SP	TCA
Report breach of data access restrictions	IAP-SP	TCA
Advise concerning Approval/Rejection by TCA to IAP-SP request	TCA	IAP-SP
Provide SD Vehicle Type options and SD Comments options, including updates and adoption dates	TCA	IAP-SP
Advise concerning adoption of SD Vehicle Type options and SD Comments options	IAP-SP	TCA

IAP-SP QUALITY SYSTEM

B.44 General

B.44.1 The IAP-SP shall have in place a documented Quality System to meet the requirements of this Specification and in alignment with AS/NZ ISO 9001:2000, or equivalent as approved by TCA.

B.44.2 The IAP-SP Quality System shall include appropriate configuration management procedures for the accurate control and monitoring of any changes to:

a) IAP-SP's type-approved IVU(s);

b) IAP-SP's type-approved TID(s);

c) SDID(s);

d) the IAP-SP System;

e) the IAP-SP's Quality Monitoring Station; and

f) the IAP-SP's Quality System.

B.44.3 The IAP-SP shall keep records of all changes to its staff, and make the records available to TCA.

B.44.4 The IAP-SP shall maintain all documentation originating from B.44 to B.48 for a period of not less than four years.

B.45 Internal and external audits

B.45.1 The IAP-SP Quality System shall include both internal audits and formal external audits by a qualified independent party.

B.45.2 The IAP-SP shall document all internal and formal external audits, including feedback received and corrective actions taken.

B.45.3 Internal and external audit reports shall be supplied to TCA upon request.

B.45.4 The IAP-SP Quality System shall establish full audit trails for:

a) receiving IACs;

b) receiving other TCA and IAC-issuing Jurisdictional instructions;

c) receiving and storing Data Blocks from IVUs; and

d) issuing NCRs and PRs.

B.45.5 The IAP-SP Quality System shall include an event-reporting mechanism whereby any relevant exceptional event such as computer system failure, hardware failure or manual intervention, is recorded and the records subjected to internal and external auditing.

B.45.6 The IAP-SP shall monitor and report to TCA monthly, through test procedures, test results and operational results, the quality of the performance of the algorithms that:

a) compare Position Records against the Spatial Conditions within an IAC (*refer B.34.19*);

b) apply the Temporal Conditions of those IACs (*refer B.34.19*);

c) produce Speed Events from Speed Records (*refer Appendix F, F.3*);

d) produce Alarms (*refer B.17.20*); and

e) compare SD data against the SD Conditions of the IAC, or set of applicable IACs for a vehicle (*refer B.39.15*).

B.46 Information security

B.46.1 The IAP-SP shall adopt information security management practices complying with ISO IEC 27001-2006 and 27002-2005 including as a minimum, the management of:

a) the development and endorsement of an Information Security Policy;

b) security for internal and external access to information;

c) organisational assets;

d) human resource security;

e) physical and environmental security;

f) communications and operations;

g) access control;

h) information systems acquisition, development and maintenance;

i) information security incident processes;

j) business continuity; and

k) compliance.

B.46.2 The IAP-SP shall ensure that data storage and processing facilities are physically secure and that access is restricted to the IAP-SP's personnel as approved by the IAP-SP and appropriately controlled.

B.46.3 All IAP-SP System external interfaces shall be protected against intrusion and attack, including, without limitation, the use of effective and up-to-date firewall, anti- virus and intrusion detection software.

B.46.4 The IAP-SP shall ensure that its information security arrangements meet the confidentiality requirements of the TCA/IAP-SP Certification Agreement.

B.46.5 The IAP-SP shall monitor and review the information security practices in general, against documented objectives and targets.

B.47 Data access controls

B.47.1 The IAP-SP shall adopt a risk-based data access control policy, and monitor for compliance with the policy.

B.47.2 Access rights to data shall be granted in a layered manner, whereby users will be given access only to data and program functions that are required by him/her to execute his/her legitimate tasks on a need to know basis.

B.47.3 The IAP-SP shall periodically review the access rights of users against their job roles to ensure that access does not continue after it becomes inappropriate.

B.47.4 Details of accessed data shall be recorded, including the user involved and the data accessed.

B.47.5 The IAP-SP shall report to TCA any breach of access restrictions within one working day of such breach becoming apparent.

B.48 Reporting to TCA

B.48.1 The IAP-SP shall prepare, and deliver annually to TCA, a report concerning the IAP-SP Quality System with respect to:

a) its effectiveness;

b) any proposed future developments; and

c) any proposed modifications.

B.48.2 The IAP-SP shall immediately report to TCA:

a) evidence of any tampering or attempt at tampering with the IAP-SP Quality System; and

b) any IAP-SP Quality System malfunction which appears to be the result of tampering or an attempt at tampering.

IAP-SP QUALITY MONITORING STATION

B.49 IAP-SP Quality Monitoring Station

B.49.1 The IAP-SP shall operate a Quality Monitoring Station (QMS) which includes one of each type-approved IVU and, if applicable, one of each type-approved TID.

Note: The purpose of the QMS is to facilitate the monitoring of the performance of the Type-approved IVU and Type-approved TID, if applicable, to ensure their continued compliance with this Specification. Setup should be as representative of a normal installation as possible.

B.49.2 The QMS shall be static, mobile or a combination of both.

B.49.3 The QMS shall report its quality-monitoring data to the IAP-SP in such a manner as the IAP-SP, with the approval of TCA, deems appropriate.

B.49.4 The QMS shall produce a log of performance for the Type-approved IVU and the Type-approved TID, if applicable, to demonstrate their compliance.

B.49.5 The QMS log of characteristic performance for the Type-approved IVU and the Type-approved TID, if applicable, shall be analysed by the IAP-SP to determine whether the IVU and TID continue to meet this Specification.

B.49.6 Any failure of the QMS to meet this Specification shall be immediately reported to TCA.

B.49.7 The IAP-SP shall maintain all QMS documentation referred to in B.49.3, B.49.4 and B.49.6 for a period of not less than four years.

TCA AUDIT AND REVIEW OF IAP-SPs

B.50 General

B.50.1 In addition to fulfilling any TCA audit obligations required under the TCA/IAP- SP Certification Agreement, the IAP-SP shall meet all inspection and audit related requirements detailed within this Specification.

B.50.2 The IAP-SP shall ensure that, in fulfilling its audit and review obligations required under the TCA/IAP-SP Certification Agreement and this Specification, its provision of IAP Services is not adversely impacted.

B.50.3 The IAP-SP shall provide TCA with access to the following:

a) all IAP data (IACs, NCRs, PRs, IAMs, Off-the-shelf Conditions and all data transmitted from IVUs); and

b) all IAP documentation (related to IVUs, TIDs and SDIDs, and the IAP-SP System, IAP-SP Quality System and the QMS).

B.50.4 Such data access shall include support, procedural guidance, user login account(s) and access to appropriate software tools or utilities to allow the decoding, decryption, decompression, extraction, etc. of data held in any proprietary or custom format, to permit further viewing or analysis of data by TCA.

B.51 IVU and TID audit

B.51.1 Upon entering into the TCA/IAP-SP Certification Agreement, the IAP-SP shall leave with TCA the two IVUs and, if applicable, two TIDs that were type- approved. It shall also leave with TCA one SDID. These devices shall remain with TCA for the duration of the TCA/IAP-SP Certification Agreement.

B.51.2 As and when applicable, upon re-certification by TCA, the IAP-SP shall leave with TCA the two samples of any changed hardware and/or software for the duration of the TCA/IAP-SP Certification Agreement.

B.51.3 For B.51.1 and B.51.2 the IAP-SP shall adhere to the requirements in Appendix E detailing the supply of IVUs, TIDs and SDID to TCA.

Note: TCA will operate a mobile testing system that will have installed one of each of the IAP-SP's type-approved IVU(s) and TID(s), if applicable, and SDID.

TCA will operate a Quality Monitoring Station (separate from the IAP-SP Quality Monitoring Station specified in B.49) that will have installed one of each of the IAP-SP's type-approved IVU(s) and TID(s), if applicable.

B.52 IAP-SP data audit

B.52.1 The IAP-SP shall support data transmission to the TCA Audit System (TAS) to facilitate the auditing of IAP-SP System data handling, processing and reporting.

B.52.2 The IAP-SP shall meet the relevant service provider requirements of the Data Requirements Specification for TAS, as specified within Appendix G.

Note: See also A.32.8.

B.53 Position audit

B.53.1 For auditing purposes only, the IAP-SP shall upon request from TCA provide from the IAP-SP's premises:

a) where the IVU is in the communication coverage area offered by the IAP-SP, the current position (being not more than five minutes beforehand) of an IVU (direct polling); or

b) where the IVU is not in operation or not in the communication coverage area offered by the IAP-SP:

i) the most current Position Record available to the IAP-SP; or

ii) notification of the position of the IVU at a date and time as requested by TCA which shall be made available immediately upon communications being re-established with the IVU and in compliance with the IVU Data Record transfer requirements in A.30.

RESTRICTION ON POST-CERTIFICATION CHANGE – IAP-SP

B.54 IAP-SP restriction on post-certification change

B.54.1 Subsequent to certification as an IAP-SP, the IAP-SP shall not, without prior written approval of TCA by way of re-certification:

a) make any change to its IAP-SP System or QMS; and

b) make any material change to its Quality Systems, being systems and processes as detailed in this Specification.

B.54.2 The IAP-SP shall use only the IAP-SP System, Quality Monitoring Station and IAP-SP Quality System as certified, and no others.

6 REQUIREMENTS FOR SELF DECLARATION INPUT DEVICES

6.1 Overview

6.1.1 This section contains the requirements for the Self Declaration Input Device (SDID) which is used by the TO and/or its nominated representative to self declare data into the IVU. The section is divided into the following:

a) Physical and environmental characteristics;

b) SDID Self Declared data; and

c) Provision of SDID to support IVU type-approval.

6.2 Requirements

PHYSICAL AND ENVIRONMENTAL CHARACTERISTICS

C.1 Self Declaration Input Device (SDID)

C.1.1 The SDID is used by the TO and/or its nominated representative to self declare data into the IVU. The SDID is inclusive of the hardware, software and cabling and connection leading up to, but not including, the IVU.

Note: The SDID can include greater functionality than the requirements specified in this Specification. The choice of SDID is a matter for commercial agreement between the IAP-SP and the TO.

C.1.2 The data entered into the SDID shall be transferred to the IVU within 30 seconds of being collected.

C.1.3 Where the IAP-SP elects to provide an alternative facility for the entry of SD data which involves a direct link between a SDID and the IAP-SP System, the data shall be time-stamped by the SDID immediately upon entry.

C.1.4 It shall not be possible for the SDID to access or modify the data in the IVU or the IVU software.

C.1.5 After the entry of SD data, the SDID shall provide the TO and/or its nominated representative with confirmation of the IVU's successful receipt of that data.

Note: See also A.20.1.

C.2 SDID SD data entry prompt

C.2.1 The SDID shall prompt for entry of SD data. An initial prompt shall appear immediately after the SDID and/or ignition is turned on and shall be repeated as a minimum once every 24 hours. The prompt shall read 'Please confirm relevant IAP data'.

Note: The intention of the prompt is to assist the TO and/or its nominated representative to meet any obligation they may have under the IAP to self declare data.

C.3 Non-IAP applications in SDID

C.3.1 It shall be permissible, subject to the approval of TCA from the perspective of the integrity of the IAP, for non-IAP functionality to be accommodated within the SDID.

C.3.2 The IAP-SP shall document, to the satisfaction of TCA, any non-IAP functionality to be provided by the SDID.

C.3.3 The IAP functionality shall be isolated from any non-IAP functionality that may be provided by the SDID such that the performance of the SDID for IAP purposes is not hindered or degraded, and such that the IAP is not compromised.

C.3.4 The IAP-SP shall document, to the satisfaction of TCA, the design features of the SDID which isolate and protect IAP functionality from any non-IAP functionality.

SDID SELF DECLARED DATA

C.4 SD data

C.4.1 The SD data supported is:

a) Vehicle Type and TCM; and

b) Comments.

C.4.2 The SDID shall have the capability to include additional SD data types as required by TCA from time to time.

C.4.3 The SDID shall have the capability of expanding the existing SD Vehicle Type options (*refer C.5.1*) and SD Comments options (*refer C.6.1*).

C.4.4 TCA will be responsible for the supply of SD Vehicle Type options and SD Comments options to the IAP-SP, including the supply of updated versions.

C.4.5 The adoption of new versions of SD Vehicle Type options and SD Comments options shall be aligned with the IAM version number and IAM adoption dates.

Note: Not all IAM versions will require an update to SD Vehicle Type options and/or SD Comments options.

C.4.6 SD Vehicle Type options shall include:

a) Vehicle Category Code; and

b) Vehicle Type, comprising:

i) Vehicle Category; and

ii) Number of Axles.

C.4.7 SD Comments options shall include:

a) Comment Code; and

b) Comment name.

C.4.8 TCA will provide the updated version of SD Vehicle Type options and SD Comments options at least four weeks prior to the date when the update is required to be adopted by the IAP-SPs.

C.4.9 The IAP-SP shall have procedures in place to receive and implement any updated versions of SD Vehicle Type options and SD Comments options.

C.4.10 The IAP-SP shall confirm to TCA two weeks prior to the date when the update is required to be adopted that the SD Vehicle Type options and SD Comments options can be loaded and used reliably.

C.4.11 The adoption of an SD Vehicle Type options and SD Comments options revision shall be implemented such that after the date and time of that adoption:

a) IACs and/or Off-the-shelf IAP Conditions created after the adoption date and time support the revised SD Vehicle Type options; and

b) the Vehicle Type options and SD Comments options available for self declaration match the adoption.

Note: This requirement allows a reasonable timeframe for update of SDIDs to occur taking communications coverage into consideration.

C.5 SD Vehicle Type

C.5.1 The SDID shall provide for the SD Vehicle Type (Vehicle Category/Number of Axles) options as issued by TCA.

Note: See also B.39.10.

The Vehicle Category of Prime Mover with 'N/A' Number of Axles refers to a Prime Mover with no trailer(s) connected.

C.5.2 The SDID shall provide for the selection, by the TO and/or its nominated representative, of a Vehicle Type from the predefined list of Vehicle Categories and Number of Axles (*refer C.5.1).*

C.5.3 The SDID shall provide for the TO and/or its nominated representative to enter a TCM value or select 'No Load'.

Note: See also B.39.12.

The IAP-SP has discretion in the design of the user interface and may offer such features as:

- *the ability to confirm the previously entered Vehicle Type and/or TCM, rather than specifically entering the data each time;*
- *a graphical interface; and*
- *a set of Vehicle Category/Number of Axles customised to the needs of the TO.*

C.6 SD Comments

C.6.1 The SDID shall provide for the SD Comments options as issued by TCA.

C.6.2 The SDID shall provide for the selection, by the TO and/or its nominated representative, of a Comment Name from the predefined list of Comment Names (*refer C.6.1)* followed by the optional entry of a free form comment text.

PROVISION OF SDID TO SUPPORT IVU TYPE-APPROVAL

C.7 SDID provision in support of IVU type-approval

C.7.1 To facilitate IVU type-approval testing, one SDID shall be provided to TCA. The Applicant shall adhere to the requirements in Appendix E detailing the supply of the SDID.

Note: See also A.35.

Appendix A Acronyms and Definitions

Acronym	Meaning
B2B	Business to Business
ECM	Engine Control Module
FTPS	File Transfer Protocol using SSL
GDA94	Geocentric Datum of Australia 1994
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HDOP	Horizontal Dilution of Precision
IAC	Intelligent Access Condition
IAM	Intelligent Access Map
IAP	Intelligent Access Program
IAP-SP	Intelligent Access Program Service Provider
ID	Identifier
IT	Information Technology
IVU	In-Vehicle Unit
NCR	Non-Compliance Report
PKI	Public Key Infrastructure
PR	Participants Report
PSMA	PSMA Australia Ltd
QMS	Quality Monitoring Station
SD	Self Declaration
SDID	Self Declaration Input Device
SSL	Secure Sockets Layer
TAS	TCA Audit System
TCA	Transport Certification Australia Limited
TCM	Total Combination Mass
TID	Trailer Identification Device
TO	Transport Operator
UTC	Coordinated Universal Time
VIN	Vehicle Identification Number
WAN	Wide Area Network
WGS84	World Geodetic System 1984
XML	Extensible Markup Language

Term	Definition
Alarm	An IAP-SP System response resulting from testing data transmitted from the IVU against pre-defined criteria.
Alarm Code	A code categorising an Alarm or an Alarm Record.
Alarm Record	A record generated and stored in the IVU as a result of testing IVU data against pre-defined criteria.
Applicant	A party which has applied for certification as an IAP-SP.
Business to Business (B2B)	Business to Business electronic data interchange.
Certification	The formal confirmation that an Applicant has satisfied all the requirements for appointment as an IAP-SP.
Framing data	Identifying data attached to each Data Block transmitted from the IVU to the IAP-SP.
GDA94	The Geocentric Datum of Australia 1994 is part of a global coordinate reference frame and is directly compatible with the Global Positioning System (GPS).
GNSS	The Global Navigation Satellite System comprises several networks of satellites that transmit high-frequency radio signals containing time and distance data that can be picked up by a receiver, allowing the user to identify the location of the receiver anywhere around the globe.
Global Positioning System (GPS)	A form of GNSS controlled by the US Department of Defense.
GPS Antenna	The antenna used to receive GPS signal within the IVU.
GPS Doppler derived method	A method to calculate vehicle speed based on the change in the frequency or timing of signals caused by movement of the different GPS satellites relative to the GPS receiver.
GPS receiver	A GPS unit functioning within the IVU.
GPS Satellite Signal or GPS Signal	GPS satellites transmit two low power radio signals, designated L1 and L2. IAP utilises civilian GPS which usually uses the L1 frequency.
HDOP	Horizontal Dilution of Precision is a measure quantifying the quality of the determination of horizontal position (latitude and longitude) based on the number and geometric distribution of the satellites used in the determination.
IAC Background	The area within a Jurisdiction which is not specifically identified in the Spatial Conditions of the IAC.
IAC Form	The document (paper or electronic) which details the contents of an IAC.
IAC-issuing Jurisdiction	An entity with the authority to issue IACs on behalf of one or more Jurisdictions.
IAP	The IAP is a voluntary program which provides to the operators of heavy vehicles, access, or improved access, to the Australian road network in return for the monitoring of their compliance with specific access conditions by vehicle telematics solutions.

Term	Definition
IAP Application	The generic term for road access schemes, permits, concessions, exemptions, gazettals or notices which include an IAP compliance solution.
IAP Audit	Review of a party's capacity to meet, or continue to meet, the initial and ongoing certification requirements set by TCA for IAP-SPs.
IAP Auditor	A party appointed by TCA to conduct reviews of applications for certification as an IAP-SP and ongoing post-certification reviews.
IAP Conditions	The conditions determined by the IAC-issuing Jurisdiction which must be complied with, by the vehicle, in return for the access granted by the IAP Application.
IAP Data	The electronic data collected by the IAP-SP within the IAP.
IAP Functional & Technical Specification	The specification defining the functional and technical requirements which a party applying for certification as an IAP-SP must satisfy with respect to its hardware, software and systems.
IAP Service Provider (IAP-SP)	A party which is certified by TCA as suitable to provide IAP Services.
IAP Services	The IAP vehicle-monitoring and reporting services which are provided by an IAP-SP.
IAP Speed Threshold	The maximum speed, specified in the Speed Condition of an IAC, beyond which a Speed Event is triggered.
IAP Vehicle	A vehicle operating under an IAC.
IAP-SP System	The IAP-SP's hardware and software, excluding the IVU, TID and SDID, used in the collection, processing, testing, storage and reporting of IAP Data.
IAP-SP/TO Agreement	A written agreement between an IAP-SP, a TO and TCA which sets out the terms on which the IAP-SP will provide IAP Services to the TO.
Independent Movement Sensor	A sensor which detects movement of a vehicle independent of GPS signal.
Intelligent Access Condition (IAC)	The document (paper or electronic) by which a specified TO, and its vehicle combination, are granted access to road networks by an IAC-issuing Jurisdiction under a particular IAP Application, on condition that its vehicle complies with certain conditions (IAP Conditions) which are referenced in the IAC.
Intelligent Access Map (IAM)	A map, in electronic form, issued, by TCA as the reference against which compliance with the Spatial Conditions of an IAC is assessed.
Interim IAC	The document issued by the IAC-issuing Jurisdiction which indicates its intention to grant the IAC contingent on the TO engaging an IAP-SP to provide IAP Services.
In-Vehicle Unit (IVU)	The telematics unit installed, operated and maintained by the IAP-SP which monitors parameters.
IVU Data	The raw data collected by the IVU.
IVU Data Records	Position, Speed, Alarm and SD Records generated by the IVU.

Term	Definition
IVU Identifier (IVU ID)	A unique identifier assigned to an IVU which identifies the IVU and the data from that IVU.
Jurisdiction	As the context may apply, either: a) A geographical area containing a road network (i.e. typically an Australian State or Territory), or b) An entity which has authority to make available IAP Applications pertaining to a Jurisdiction.
Level 1 Type-approved IVU	A type-approved IVU with no automatic trailer identification capability.
Level 2 Type-approved IVU	A type-approved IVU with automatic trailer identification capability.
Link	A section of road that is identified within the IAM by reference to its Persistent ID.
Local date and time	Date and time at a particular locale. A Jurisdiction's local date and time is according to the time zone of the capital city within the Jurisdiction.
Local time	Equivalent to local date and time.
Message Authentication Code	A code known only to the IAP-SP to ensure the authenticity of the IVU, Trailer ID and SDID communication origin.
Non-Compliant activity	An activity of an IAP vehicle which does not comply with the conditions of applicable IAC(s).
Non-Compliance Report (NCR)	A report forwarded to an IAC-issuing Jurisdiction by an IAP-SP in respect to a non- compliance with applicable IAC(s), or suspected tampering with the system.
Off-the-shelf IAP Application	A standard IAP Application developed for widespread use.
Parameter	A feature of vehicular movement being monitored as part of an IAC. There are three parameters which are currently monitored: position, time and speed.
Participants Report (PR)	A report forwarded to an IAC-issuing Jurisdiction by an IAP-SP in respect of a specified period, aggregating the number of NCRs for each individual participating vehicle.
Persistent ID	A Persistent ID identifies a particular Link within the network in the IAM.
PKI	Public Key Infrastructure is the IT infrastructure associated with the use and management of digital keys and certificates to support information security.
Position Record	A record generated and stored in the IVU every 30 ± 0.2 seconds when the vehicle is in operation, containing positional and other data for the vehicle being monitored.
Prime mover/rigid truck	That part of a vehicle which contains the power unit and, in the context of IAP, to which the IVU is affixed.

Term	Definition
Quality Monitoring Station (QMS)	Equipment used by the IAP-SP and TCA to provide a log of the output of a Type-approved IVU or TID with respect to its accuracy and integrity.
Route	The roads or set of roads defined by a set of contiguous Persistent IDs.
Route Condition	A condition specified in the IAP Conditions within an IAC which describes a continuous road or set of roads to which access is allowed, or not allowed, by specifying a contiguous set of Persistent IDs that identify the route.
Scheme	The generic term used to define the approval arrangement and documentation utilised by Jurisdictions for granting vehicles access to particular roads or types of roads subject to certain conditions. Each Jurisdiction uses their own terminology including, but not limited to, permit, application, scheme, concession, exemption, gazettal and notice.
SD Comments	Comments self declared by the TO and/or its nominated representative.
SD Condition	A condition specified in the IAP Conditions within an IAC which requires that data be self declared by the TO and/or its nominated representative.
SD Data	Data which is self declared by the TO and/or its nominated representative.
SD Record	A record generated and stored in the IVU and/or an alternative to SDID use facility whenever a TO and/or its nominated representative self declares SD data.
SD (Vehicle Type/TCM)	The Vehicle Type and TCM self declared by the TO and/or its nominated representative to the IAP-SP.
Self Declaration (SD)	The self declaration of data by a TO and/or its nominated representative.
Self Declaration Input Device (SDID)	A device used by the TO and/or its nominated representative to enter SD data into the IVU.
Spatial Condition	A condition specified in the IAP Conditions within an IAC which describes a vehicle's route or zone access.
Speed Condition	A condition specified in the IAP Conditions within an IAC which prescribes the IAP Speed Threshold.
Speed Event	The set of Speed Records which covers the period during which the vehicle exceeded the IAP Speed Threshold including 60 seconds before and 60 seconds after that period.
Speed Record	A record generated in the IVU every 3.0 ± 0.1 seconds containing vehicle speed and other data for the vehicle being monitored.
SSL	Secure Sockets Layer is an IT cryptographic communications protocol, predominantly used to provide secure communications on the Internet.
Tamper	Conduct towards any Intelligent Access System (including without limitation, the IVU) which is intended to prevent the system from functioning correctly.

Term	Definition
TCA/IAP-SP Certification Agreement	The written agreement made between TCA and an IAP-SP which recognises the fact that the IAP-SP, having satisfied TCA's requirements for appointment as an IAP-SP, is appointed in that capacity, and sets out the legal obligations of each of the IAP-SP and TCA with respect to the ongoing role of the IAP-SP as an IAP Service Provider.
TCA Reference System	The reference system used by TCA for GPS quality testing of IVUs
TCM Threshold	The maximum TCM value specified against a particular Vehicle Type in a SD Condition.
Temporal Condition	A condition specified in the IAP Conditions within an IAC that describes the permitted date and time for accessing, or not accessing, particular routes and zones.
Total Combination Mass (TCM)	The combined mass of the laden or unladen trailer(s) and the prime mover/rigid truck.
Trailer ID	A unique identifier assigned to a Trailer Identification Device which identifies the trailer.
Trailer Identification Device (TID)	A passive device that uniquely identifies a trailer when detected by a Level 2 IVU.
Transform	The process by which an IAP-SP reformats, converts and rounds its IVU Data to meet the requirements of Appendicies G and H.
Transport Operator (TO)	An operator of one or more vehicles eligible to enter an IAP Application.
Type-approved IVU	An IVU which is of a type which has been approved by TCA for use within the IAP.

Appendix B Intelligent Access Condition Form

The Intelligent Access Condition Form (IAC Form) sets out the data that is collected by the IAC-issuing Jurisdiction and contained within the IAC.

An IAC-issuing Jurisdiction may use a pro forma document to collect IAC data from a TO, but all IAC data is transmitted between the IAC-issuing Jurisdiction and the IAP-SP via an automated web service environment when:

- *Part 3 is submitted to the IAC-issuing Jurisdiction by the IAP-SP; and*
- *Parts 1 to 4 (the IAC) are issued to the IAP-SP.*

The detail in this IAC Form also provides a sample report layout for an Interim IAC or an IAC. Delivery of the Interim IAC to the IAP-SP can be in a paper based or XML form.

INTELLIGENT ACCESS PROGRAM (IAP)
IAC Form

*** An asterisk indicates required information**

Identification details provided by the IAC-issuing Jurisdiction

IAC identifier:*
If this IAC replaces a cancelled IAC, provide details of the previous IAC in the box below.
Previous IAC identifier:

Details of the Jurisdiction for which this IAC is being issued	
Name of Jurisdiction:*	
Postal address	Enquiries
Address 1:*	Phone:* ( )
Address 2:	
City/Suburb:*	Fax:* ( )
State:*	
Postcode:*	Email:*

IAC Commencement date:*	hrs / /	(hrs dd/mm/yyyy)
IAC Cessation date:	hrs / /	(hrs dd/mm/yyyy)

N O T E	*Operation under this IAC cannot occur until the IAP Service Provider (IAP-SP) has received notification of final approval of this IAC from the IAC-issuing Jurisdiction.*

PART 1 – details provided by the IAC-issuing Jurisdiction

IAP Application

Name of IAP Application:*	

IAP Application is (select **ONE only**):*	☐ Off-the-shelf	☐ Unique

NOTE	*Off-the-shelf IAP Conditions are **referenced** .....*	*Off-the-shelf IAP Conditions ID:*	
	*Unique IAP Conditions are **specified below.***		

Unique IAP Conditions – Self Declaration (SD) Conditions

This IAC requires the self declaration of Vehicle Type and Total Combination Mass (TCM)*: (this question is part of the IAC Form but is not part of the XML schema)	☐ Yes	☐ No

Permitted Vehicle Types and TCMs when operating under this IAC are (Jurisdiction nominates):

Vehicle Category:	Rigid Truck	No. of axles:	3	TCM Threshold:	
Vehicle Category:	Rigid Truck	No. of axles:	4	TCM Threshold:	
Vehicle Category	Rigid Truck	No. of axles:	5	TCM Threshold:	
Vehicle Category	Rigid Truck	No. of axles:	6	TCM Threshold:	
Vehicle Category:	Prime Mover	No. of axles:	0	TCM Threshold:	
Vehicle Category:	Semi Trailer	No. of axles:	4	TCM Threshold:	
Vehicle Category:	Semi Trailer	No. of axles:	5	TCM Threshold:	
Vehicle Category:	Semi Trailer	No. of axles:	6	TCM Threshold:	
Vehicle Category	Etc.	No. of axles:		TCM Threshold:	

Notes:
1. A Total Combination Mass (TCM) Threshold must be entered for every listed Vehicle Type. A TCM Threshold of zero (0) indicates that that vehicle is not permitted.
2. This form serves only as a template. The most up to date Vehicle Types must be obtained from TCA. Only Vehicle Types issued by TCA are allowed to be included in an SD Condition. An IAC with Vehicle Types not issued by TCA must be rejected.
3. It is acceptable to exclude a Vehicle Type from the IAC by not listing it. In this case, the Vehicle Type is treated as not permitted.

This IAC requires the reporting of Self Declared (SD) Comments:*	☐ Yes	☐ No

Unique IAP Conditions – IAP Speed Threshold

IAP Speed Threshold:	……..km/h (this IAP Speed Threshold must not vary between IACs issued for a Jurisdiction for this prime mover/rigid truck)

Unique IAP Conditions – IAC Background

Background to be set at (select **ONE only**):*	☐ Inclusion	☐ Exclusion	

Unique IAP Conditions – Route or Zone Condition with associated Temporal Conditions

Spatial Condition 1 with associated Temporal Condition:

Access applies to (select **ONE only**):*	☐ Route	☐ Zone

Type of condition (select **ONE only**):*	☐ Absolute-inclusion	☐ Exclusion	☐ Inclusion

Route/Zone access description:*	Identifying Persistent IDs:*

First Link - Start lat/long (optional):	Last Link - End lat/long (optional):

If there is a time limitation associated with this route or zone condition provide details below:

Every day	Weekday	Weekend	Mon	Tue	Wed	Thu	Fri	Sat	Sun
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Start Time and Date	End Time and Date	and/or	Start Time 1	End Time 1	Start Time 2	End Time 2	Start Time 3	End Time 3	etc…

Spatial Condition 2 with associated Temporal Condition:									
Access applies to (select **ONE only**):* ☐ Route ☐ Zone									
Type of condition (select **ONE only**):* ☐ Absolute-inclusion ☐ Exclusion ☐ Inclusion									
Route/Zone access description:*						Identifying Persistent IDs:*			
First Link - Start lat/long (optional):		Last Link - End lat/long (optional):							
If there is a time limitation associated with this route or zone condition provide details below:									
Every day	Weekday	Weekend	Mon	Tue	Wed	Thu	Fri	Sat	Sun
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Start Time and Date	End Time and Date	and/or	Start Time 1	End Time 1	Start Time 2	End Time 2	Start Time 3	End Time 3	etc…

Spatial Conditions with associated Temporal Conditions are defined as required. There is no limit to the number of Spatial/Temporal Conditions that can be defined.

Unique IAP Conditions – Comments / further information

PART 2 – details provided by the Transport Operator

Details of the Transport Operator applying for this IAC

Transport Operator:*	Company name:*	ABN:*	ACN:

Postal address	Enquiries
Address 1:*	Phone (Bus hours):* ( )
Address 2:	Phone (After hours): ( )
City/Suburb:*	Fax: ( )
State:*	Email:
Postcode:*	
Nominated officer for TO	Name: Title/Position: Contact phone:
Comments / further information:	

Prime mover/rigid truck details

Make:	Model:	Body type:	Registration No:*	State:*

Vehicle Identification Number (VIN):	OR	Non-VIN Identifier (if no VIN available):*
VIN:		**Non-VIN:**

Garaging address	Street address:	City/Suburb:	State:	Post code:

Note: If using Non-VIN identifier use Chassis Number, and if this is unavailable, use Engine Number. When issued to the TO, the Interim IAC does not include the Vehicle VIN or Vehicle Non-VIN Identifier.

Trailer details

NOTE	
	1. *This IAC can be issued for the use of a single prime mover or rigid truck and may also be issued for a vehicle combination involving one or more trailers.*
	2. *The Jurisdiction must specify whether a Level 1 (no automatic trailer identification capability) or Level 2 (automatic trailer identification capability) Type-approved IVU is required for a particular IAP Application.*
	3. *The various combinations (if any) as stated by the TO are subject to the approval of the Jurisdiction.*
	4. *If this IAC supports the self declaration of Vehicle Type and TCM then when listing the potential trailers, ensure they are consistent with the permitted Vehicle Types specified in Part 1.*

What level of Type-approved IVU is required for this IAP Application?*	☐ Level 1 Type-approved IVU ☐ Level 2 Type-approved IVU
If a Level 1 Type-approved IVU is required for this IAC then the TO need **proceed no further, in this Part 2 of the Form**. If a Level 2 Type-approved IVU is required for this IAC then continue completing Part 2:	
How many trailers may operate in conjunction with the prime mover/rigid truck?*	☐
Using the trailer numbers specified below, list the allowable combinations.* List the allowable combinations only once – trailer order is not significant. Separate unique combinations with a comma; use a '+' to separate individual trailers in a combination.	

Trailer No. 1				
Trailer make:*	Trailer model:*	Trailer type:*	Registration No:*	State:*
Vehicle Identification Number (VIN)		**OR**	**Non-VIN identifier (if no VIN):***	
VIN			**Non-VIN**	
Garaging address	Street address:	City/Suburb:	State:	Post code:

Trailer No. 2				
Trailer make:*	Trailer model:*	Trailer type:*	Registration No:*	State:*
Vehicle Identification Number (VIN)		**OR**	**Non-VIN identifier (if no VIN):***	
VIN			**Non-VIN**	
Garaging address	Street address:	City/Suburb:	State:	Post code:

Note: When issued to the TO, the Interim IAC does not include The Trailer VIN or Trailer Non-VIN Identifier.

Trailer identification continues for all trailers which operate under this IAC.

IAC-issuing Jurisdictional authorisation (Interim Approval)

Comments / further information:	
Interim IAC Approval date:*	hrs / / (hrs dd/mm/yyyy)
Interim IAC Lapse date:* *[This Interim IAC will lapse if Part 3 is not received from the IAP-SP by this date*]	hrs / / (hrs dd/mm/yyyy)

Authorised by:* Title/position:*
Phone:*

For IAC-issuing Jurisdictional use only –
If the IAC-issuing Jurisdiction cancels this Interim IAC after the date of Interim IAC Approval but before either the Interim IAC has Lapsed or the IAC been Approved/Denied, then the following information must be supplied:

Comments / further information:	
Interim IAC Cancelled date:	hrs / / (hrs dd/mm/yyyy)

Authorised by: Title/position:
Phone:

PART 3 – details provided by the IAP-SP and submitted in the B2B environment to the IAC-issuing Jurisdiction

IAC identifier:*

Note: The IAC identifier is supplied so that the IAC-issuing Jurisdiction can link the submitted Part 3 to the appropriate Interim IAC.

IAP Service Provider details

Company name:*	ABN:*	ACN:

Postal address:	Enquiries:
Address 1:*	
Address 2:	Phone:* ( )
City/Suburb:*	Fax:* ( )
State:*	Email:*
Postcode:*	
Comments / further information:	

Dated:* hrs / / (hrs dd/mm/yyyy)

Details of prime mover/rigid truck in which the IVU is installed

Vehicle Identification Number (VIN)	**OR**	Non-VIN Identifier (if no VIN)*
VIN:		**Non-VIN:**

Note: Either the VIN or Non-VIN Identifier must be supplied so that the IAC-issuing Jurisdiction can verify that the equipment has been installed in the prime mover/rigid truck as listed in Part 2 of the IAC Form. If using Non-VIN Identifier use firstly Chassis Number, and if this is unavailable, use Engine Number.

Details of the installed IVU

In-Vehicle Unit (IVU) identifier:*	Time and date IVU installed:*
	Hours / / (details in 24hr dd/mm/yyyy)
IVU location:*	
GPS antenna location:*	

Details of installed Trailer Identification Device (if any)

Trailer No 1: Vehicle Identification Number (VIN)		**OR** Non-VIN identifier (if no VIN)*	
VIN:		**Non-VIN:**	
Note: Either the VIN or Non-VIN Identifier is required so that the IAC-issuing Jurisdiction can verify that the equipment has been installed on the correct trailer as listed in Part 2 of the IAC Form.			
Details of the Trailer Identification Device (TID) mounted in **Trailer No 1** are:			
Trailer ID:*		Time and date TID installed (details in 24hr dd/mm/yyyy):*	
		Hours / /	
TID location:*			

Trailer No 2: Vehicle Identification Number (VIN)		**OR** Non-VIN identifier (if no VIN)*	
VIN:		**Non-VIN:**	
Note: Either the VIN or Non-VIN Identifier is required so that the IAC-issuing Jurisdiction can verify that the equipment has been installed on the correct trailer as listed in Part 2 of the IAC Form.			
Details of the Trailer Identification Device (TID) mounted in **Trailer No 2** are:			
Trailer ID:*		Time and date TID installed (details in 24hr dd/mm/yyyy):*	
		Hours / /	
TID location:*			

TID installation details continue for all trailers which operate under this IAC.

PART 4 – completed by IAC-issuing Jurisdiction

IAC-issuing Jurisdictional Approval of IAC

This application to enter the IAP Application is:*	☐ APPROVED	☐ DENIED
Comments / further information:		
IAC Approved/Denied date:*	hrs / /	(hrs dd/mm/yyyy)
Authorised by:*	Title/position:* Phone:*	

For IAC-issuing Jurisdictional use only – If the IAC-issuing Jurisdiction cancels this IAC then the following information must be supplied		
Comments / further information:		
IAC Cancelled date:*	hrs / /	(hrs dd/mm/yyyy)
Authorised by:*	Title/position:* Phone:*	

Note: Once the IAC-issuing Jurisdiction has considered all submitted details and Approved or Denied the IAC application:

- *The IAC-issuing Jurisdiction issues the entire IAC (Parts 1 to 4) to the IAP-SP within the B2B environment; and*
- *Communication between the IAC-issuing Jurisdiction and the TO proceeds outside of the B2B environment as specified in the IAC-issuing Jurisdiction's guidelines.*

Appendix C Non-Compliance Report Form

The Non-Compliance Report Form (NCR Form) sets out the supporting data that is provided by the IAP-SP to an IAC-issuing Jurisdiction when reporting a non-compliant activity.

Within the IAP this data is actually exchanged between the IAP-SP and the IAC-issuing Jurisdiction via an automated web service environment.

The detail in the NCR Form also provides a sample report layout for an NCR.

INTELLIGENT ACCESS PROGRAM (IAP)
NCR

Details of the NCR

NCR identifier:	
If this NCR is a continuation NCR, supply the identifier for the previous NCR:	
This NCR was generated by the IAP-SP on (IAP-SP local time):	hrs / / (hrs dd/mm/yyyy)
Audit reference date/time stamp (Jurisdiction local time):	
At the time of the audit reference date/time stamp the following versions were implemented in the IAP-SP System	
IAP Functional & Technical Specification Version:	
IAM Version:	
Comments / further information:	

Details of applicable IAC(s)

Name of Jurisdiction for which this IAC was issued:	

IAC identifier:	
Name of IAP Application:	
Off-the-shelf IAP Conditions ID (if applicable):	
Off-the-shelf IAP Conditions Revision # (if applicable):	

IAC identifier:	
Name of IAP Application:	
Off-the-shelf IAP Conditions ID (if applicable):	
Off-the-shelf IAP Conditions Revision # (if applicable):	

All applicable IACs over the period of this NCR are listed.

Details (current) of the IAP Service Provider (IAP-SP) forwarding this NCR

Company name:	ABN:	ACN:

Postal address:	Enquiries:
Address 1:	Phone (Bus hours): ( )
Address 2:	Fax: ( )
City/Suburb:	Email:
State:	
Postcode:	

This NCR has been generated regarding the following Transport Operator

NOTE ***The 'Transport Operator' 'Company name' 'ABN' and 'ACN' fields are pre-populated (as depicted) by the IAP-SP.***

Transport Operator:	Company name:	ABN:	ACN:
XXXXXXXX	**XXXXXXXX**	**00000000000**	**000000000**

Nature of the non-compliant activity

Non-compliant activity *(select **ONE only**):*

- ☐ Spatial
- ☐ Temporal
- ☐ Speed
- ☐ Alarm
- ☐ SD (Vehicle Type/TCM)

Summary of the Spatial, Temporal or SD (Vehicle Type/TCM) non-compliant activity
(left blank for Speed and Alarm NCRs)

Non-compliant activity began: (Jurisdiction local time)	hh:mm:ss dd/mm/yyyy		
(UTC time)	hh:mm:ss dd/mm/yyyy UTC		
Initial Position:	Latitude	and Longitude	(decimal degrees)
Non-compliant activity ended: (Jurisdiction local time)	hh:mm:ss dd/mm/yyyy		
(UTC time)	hh:mm:ss dd/mm/yyyy UTC		
Final Position:	Latitude	and Longitude	(decimal degrees)
Total duration of the non-compliant activity was:	hours	minutes	seconds

Prime mover/rigid truck details

NOTE	*The 'Make' and 'Model' fields are pre-populated (as depicted) by the IAP-SP.*

Details of the prime mover/rigid truck being operated by the TO during the non-compliant activity			
Make:	Model:	Registration No:	State:
XXXXXXX	**XXXXXXX**		
Vehicle Identification Number (VIN) **OR** Non-VIN identifier (if no VIN)*		IVU Identifier:	
VIN:	**Non-VIN:**		

Trailer details

NOTE	
	1 *The 'Trailer make' and 'Trailer model' fields (if required in the IAC) are pre-populated (as depicted) by the IAP-SP.*
	2 *The IAP-SP completes this section only if the applicable IACs specify the use of a Level 2 Type-approved IVU.*
	3 *Whilst the applicable IAC(s) may be issued for the use of a prime mover/rigid truck with a number of different trailer combinations, the IAP-SP only supplies details of the trailer(s) attached during the non-compliant activity.*

Details of the trailer being operated by the TO during the non-compliant activity			
Trailer make:	*Trailer model:*	*Registration No:*	State:
XXXXXXXX	**XXXXXXXX**		
Vehicle Identification Number (VIN) OR Non-VIN identifier (if no VIN#)		Trailer ID:	
VIN:	**Non-VIN:**		

Details of the trailer being operated by the TO during the non-compliant activity			
Trailer make:	Trailer model:	Registration No:	State:
XXXXXXXX	**XXXXXXXX**		
Vehicle Identification Number (VIN) OR Non-VIN identifier (if no VIN#)		Trailer ID:	
VIN:	**Non-VIN:**		

Trailer details continue for all trailers which were connected to the prime mover/rigid truck.

Details of the Non-Compliant Activity

NCR Position, Speed, Alarm and SD Records will be output (as defined in this Specification) in substantiation of non-compliant activity. The format of the respective records is guided by the XML schema within Appendix H. The records are briefly described below.

NCR Position Record

NCR Position Record									
Record No.	UTC date/time generated	Vehicle Position latitude	Vehicle Position longitude	Direction of travel	No. of Satellites	HDOP	Ignition status	Other independent movement sensor status	Trailer ID (up to a maximum of 10)

NCR Position Record (continued)					
Jurisdiction Local Date & Time	Persistent ID	Road name	Locality	State	Compliant/ non-compliant

NCR Speed Record

NCR Speed Record							
Record No.	UTC date/time generated	Vehicle Position latitude	Vehicle Position longitude	Vehicle speed	No. of Satellites	HDOP	Trailer ID (up to a maximum of 10)

NCR Speed Record (continued)					
IAP Speed Threshold	Jurisdiction Local Date & Time	Persistent ID	Road name	Locality	State

NCR Alarm Record Type 1

NCR Alarm Record Type 1			
Record No.	UTC date/time generated	Alarm Code	Jurisdiction Local Date & Time

NCR Alarm Record Type 2A

NCR Alarm Record Type 2A		
Alarm Code	UTC date/time of last generated IVU Data Record that contributed to the Alarm being identified	Jurisdiction Local Date & Time

NCR Alarm Record Type 2B

NCR Alarm Record Type 2B		
Alarm Code	UTC date/time of last generated IVU Data Record that resulted in the Alarm being generated	Jurisdiction Local Date & Time

NCR SD Records

NCR SD (Vehicle Type/TCM) Record							
Record No.	UTC date/time generated	Specification Version No	Vehicle Category Code	Vehicle Category	No of Axles	Vehicle Load Status	Total Combination Mass (TCM)

NCR SD (Vehicle Type/TCM) Record (continued)									
Jurisdiction Local Date & Time	Last known position UTC date/time	Last known position latitude	Last known position longitude	No. of Satellites	HDOP	Persistent ID	Road name	Locality	State

In an NCR SD (Vehicle Type/TCM) Record a Vehicle Load Status of 'No Load' is associated with a self declaration of 'No Load'.
In all other cases the Vehicle Load Status is set to 'Load'.

NCR SD Comments Record					
Record No.	UTC date/time generated	Specification Version No	Comment Code	Comment Name	Comment Text

NCR SD Comments Record (continued)									
Jurisdiction Local Date & Time	Last known position UTC date/time	Last known position latitude	Last known position longitude	No. of Satellites	HDOP	Persistent ID	Road name	Locality	State

Appendix D Participants Report Form

The Participants Report Form (PR Form) sets out the aggregated data that is provided by the IAP-SP to an IAC-issuing Jurisdiction in a Participants Report.

Within IAP this data is actually exchanged between the IAP-SP and the IAC-issuing Jurisdiction via an automated web service environment.

The detail in the PR Form also provides a sample report layout for a PR.

INTELLIGENT ACCESS PROGRAM (IAP)
PR

Details of the PR

Report for period Starting (Jurisdiction local time):	
Ending:	
PR identifier:	
This PR was generated by the IAP-SP on (IAP-SP local time):	Hrs / / (hrs dd/mm/yyyy)
Comments / further information:	

Details of the Jurisdiction

Name of Jurisdiction:

Details of the IAP Service Provider (IAP-SP) forwarding this PR

Company name:	ABN:	ACN:

Postal address:	Enquiries:
Address 1:	Phone (Bus hours): ( )
Address 2:	Fax: ( )
City/Suburb:	Email:
State:	
Postcode:	

Vehicle Details				Transport Operator		IACs	Number of NCRs Issued					
Vehicle VIN or Non-VIN identifier	IVU Identifier	Entered IAP during period on hh:mm dd/mm/yyyy	Exited IAP during period on hh:mm dd/mm/yyyy	Transport Operator	ABN	IACs issued against this vehicle for this Jurisdiction (one or many)	Spatial	Temporal	Speed	Alarm	SD	TOTAL
				XXXXXXXX	00000000000							
				XXXXXXXX	00000000000							
				XXXXXXXX	00000000000							
						TOTALS:						

Total number of vehicles monitored during the period: _____

Notes:

1. Details for 'Entered IAP during period' are only required if the vehicle had its first IAC issued during the period being reported upon by the PR. If the vehicle was already operating within the IAP at the commencement of the reporting period, then 'Entered IAP during period' shall be left blank.

2. Details for 'Exited IAP during period' are only required if the vehicle had its last IAC 'ceased' or 'cancelled' during the period being reported upon by the PR. If the vehicle was still operating within the IAP at the end of the reporting period, then 'Exited IAP during period' shall be left blank.

3. IVU Identifier shows the most recently installed IVU.

4. The 'Transport Operator' field is pre-populated "XXXXXXXX" and the 'ABN' field is pre-populated "00000000000" by the IAP-SP.

Appendix E Requirements for the Provision of IVUs, TIDs and SDIDs to TCA

E.1 General

E.1.1 The requirements contained in this Appendix shall apply to both Applicants and IAP-SPs unless otherwise stated.

E.1.2 The requirements contained in this Appendix shall apply to all IVUs, TIDs if applicable, and SDIDs presented to TCA for:

a) type-approval testing (as applicable);

b) ongoing audit and review; and

c) re-certification (as applicable).

E.1.3 TCA will, if requested, complete and return to the Applicant a signed confidentiality agreement in reasonable terms for the protection of the Applicant's intellectual property in the devices under test.

E.1.4 The Applicant / IAP-SP shall be responsible, at its cost, for the installation, operation and maintenance of all IVUs, TIDs if applicable, and SDIDs provided to TCA.

E.1.5 The Applicant / IAP-SP shall provide to TCA all IAP Services reasonably required to enable TCA to carry out the activities specified in E.1.2.

E.1.6 Noting the requirements of E.1.5, all IACs, NCRs and PRs shall be provided as a Tier 1 data interchange between the IAP-SP and TCA as appropriate.

E.2 TCA access to data

E.2.1 For the type-approval testing, ongoing audit and review, and re-certification activities referred to in E.1.2, the Applicant / IAP-SP shall provide to TCA via Tier 2 data interchange:

a) all IVU Data Records in audit record format, as specified in Appendix G, at daily intervals and only upon receipt of all relevant IVU Data Records for a particular UTC day;

b) all applicable Data Blocks at no greater than weekly intervals; and

c) support, procedural guidance, user login account(s) and access to appropriate software tools or utilities to allow the decoding, decryption, decompression, extraction, etc. of data held in any proprietary or custom format, to permit further viewing or analysis of the transmitted data by TCA.

Note: Where an IAP-SP provides an alternative to SDID use facility, relevant IVU Data Records shall include SD Records.

See also B.43.6b.

E.2.2 The data referred to in E.2.1a and E.2.1b shall be:

a) backed up by the Applicant for the duration of the type-approval process; and

b) backed up and archived by the IAP-SP in accordance with B.18.

Appendix F Requirements for Speed Record Processing

F.1 The IAP Speed Threshold for a vehicle, as specified in IAP Condition(s), shall be stored in:

a) the IVU, where Speed Record processing is performed in the IVU; and

b) the IAP-SP System, where Speed Record processing is performed in the IAP-SP System.

Note: It is the responsibility of the IAC-issuing Jurisdiction to ensure that any prime mover/rigid truck operating under a Speed Condition shall be limited to one IAP Speed Threshold within any one Jurisdiction.

F.2 A Speed Event occurs if:

a) the rolling average of the speed value within 10 consecutively generated Speed Records, where such Speed Records are at 3 ± 0.1 second intervals, exceeds the applicable IAP Speed Threshold; and

b) the GPS quality within each Speed Record in the 10 record period is at least four satellites with a HDOP of < 4.

F.3 A Speed Event ends:

a) when the rolling average of the speed value within 10 consecutively generated Speed Records does not exceed the applicable IAP Speed Threshold; or

b) at the last Speed Record collected prior to some event occurring which renders the IAP-SP unable to continue assessing the non-compliant activity.

Note: (b) includes events such as a non-compliant vehicle exiting across the Jurisdiction's border.

F.4 The algorithm to identify a Speed Event from Speed Records shall be documented, to the satisfaction of TCA.

F.5 A Speed Event (*refer to Figure F – 1* for a graphical representation) includes the data:

a) from the determined speeds used to calculate the rolling average which first exceeded the IAP Speed Threshold; until

b) the determined speeds used to calculate the rolling average which last exceeded the IAP Speed Threshold;

and during continuous operation

c) the 20 Speed Records that lead into F.4a; and

d) the 20 Speed Records that lead out of F.4b.

Note: A Speed Record may be part of more than one Speed Event.

The Speed Records in the lead in and lead out periods of a Speed Event are not tested for GPS quality as per F.2b.

The rolling average used to determine whether a Speed Event has occurred may include Speed Records from more than one Jurisdiction.

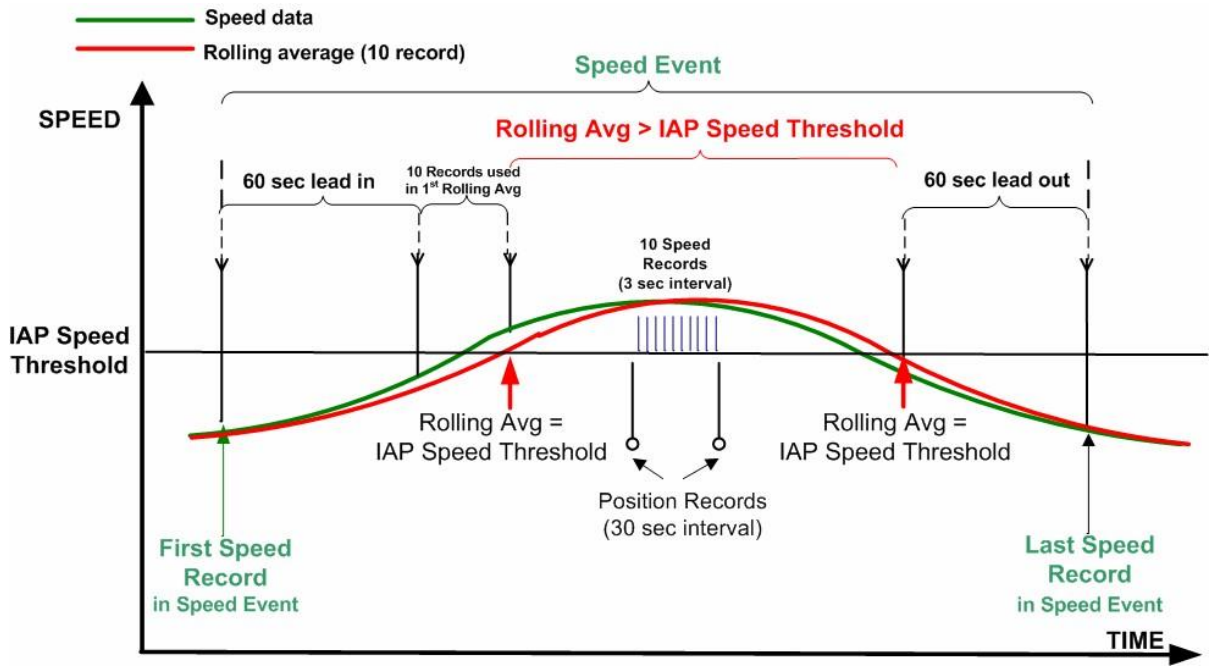


Figure F – 1. Data Required for Speed Event (not to scale)

F.6 The IAP-SP shall provide the capability of identifying a Speed Event and the included Speed Records.

F.7 Where there are less than 20 Speed Records in the lead in or lead out periods, the Speed Event shall include all available Speed Records.

Appendix G Data Requirements Specification for TCA Audit System (TAS)

Contents

Figures

Tables

G.1 Introduction

G.1.1 Overview

G.1.1.1 This Appendix specifies the data requirements and formats that shall be supported by the IAP-SP to facilitate automated auditing of IAP-SP System data handling, processing and reporting using the TCA Audit System (TAS).

G.1.2 Philosophy

G.1.2.1 The automated audit of IAP-SP data involves two discrete phases (*refer Figure G - 1*):

a) *generation* – the input data for the audit period is processed by TAS to produce a set of baseline NCRs and PRs; and

b) *comparison* – the set of baseline NCRs and PRs generated by TAS is compared with those actually generated by the IAP-SP and an audit report is generated.

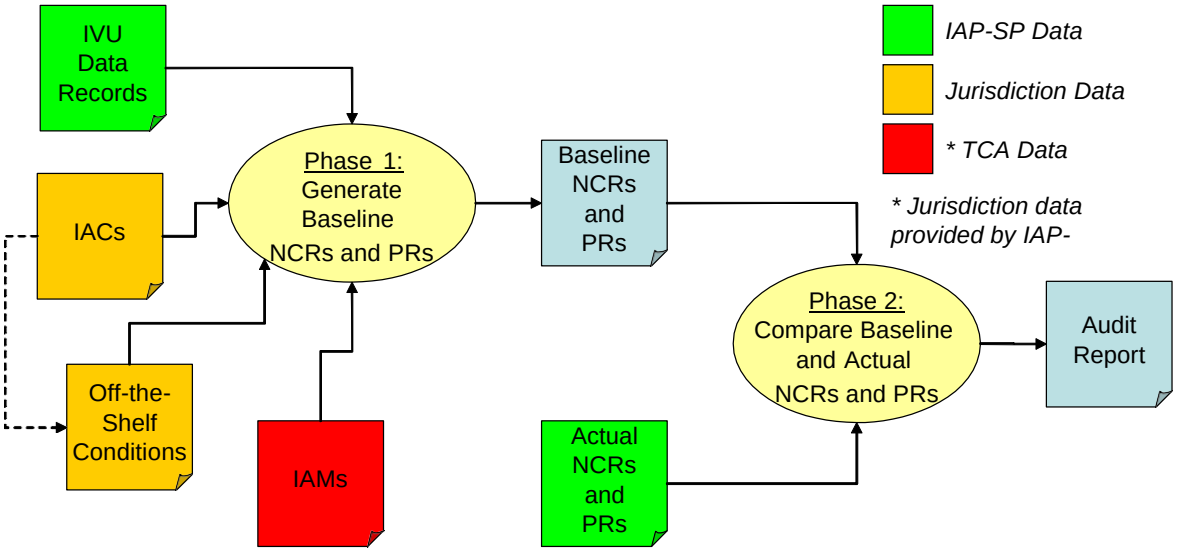


Figure G - 1. Automated Audit of IAP-SP Processing Data Flow

G.1.2.2 The input data required for the automated audit process comprises IVU Data Records, NCRs, PRs, IACs, Off-the-shelf IAP Conditions and Intelligent Access Maps (IAMs). The IAP-SP provides all input data to the audit process, with the exception of the IAM(s) (which are provided by TCA).

G.1.2.3 The NCRs, PRs, IACs and Off-the-shelf Conditions are provided in the XML Schema-based data formats as defined in Appendix H.

G.1.2.4 The IVU Data Records are provided for auditing purposes in the format described in this Appendix. This data format reflects consideration of the significant volume of IVU Data Records that may need to be provided to the automated auditing process, and the associated requirement for efficiency within the automated auditing software.

G.2 Requirement

G.2.1 Audit period

G.2.1.1 Upon request from TCA, the IAP-SP shall provide data for a nominated audit period in accordance with G.2.2.

Note: The audit period is expressed as a whole number of consecutive days and exactly matches a period covering one or more entire PR periods.

G.2.1.2 The IAP-SP shall apply the nominated audit period in the local time of each and every Jurisdiction to which it provides reports.

G.2.2 Data selection

G.2.2.1 The Audit Data Collection Period shall encompass the period covering the different Jurisdiction audit periods, in complete UTC days, the three complete UTC days preceding this period, and the single UTC day following this period (*refer Figure G - 2*).

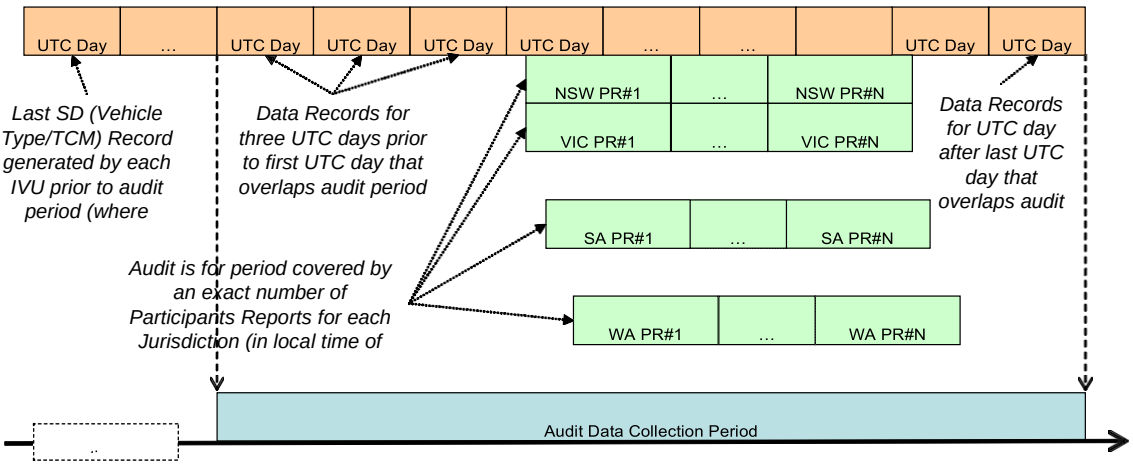


Figure G - 2. An Audit Data Collection Period

G.2.2.2 The IAP-SP shall provide:

a) all IACs that were active for any part of the Audit Data Collection Period. In the event that an IAC was cancelled during the Audit Data Collection Period, the IAC that includes the cancellation date shall be provided (i.e. not the originally approved IAC);

b) all Off-the-shelf IAP Conditions that are referenced by any IAC identified in (a), including all revisions that were active for any part of the Audit Data Collection Period;

c) all NCRs that have an audit reference date/time stamp that falls within the Audit Data Collection Period;

d) all PRs that cover the audit period; and

e) all IVU Data Records generated by the IVUs that are specified in the IACs identified in (a), over the Audit Data Collection Period.

G.2.2.3 The IAP-SP shall provide the SD (Vehicle Type/TCM) Record generated most recently prior to the start of the Audit Data Collection Period for each IVU pertaining to any IAC identified in G.2.2.2a where such a record exists.

G.2.2.4 The IAP-SP shall provide the last Position Record or Speed Record generated prior to the SD (Vehicle Type/TCM) Record specified in G.2.2.3 that contains a non-blank/void position.

G.2.2.5 In the case where the first Position Record or Speed Record within the Audit Data Collection Period contains a blank/void position, the IAP-SP shall provide the last Position Record or Speed Record generated prior to the Audit Data Collection Period that contains a non-blank/void position.

G.2.3 Audit data formats

G.2.3.1 IACs shall be provided in the form of an XML document as received by the IAP-SP from the IAC-issuing Jurisdiction. Each IAC shall be provided in a separate file.

G.2.3.2 Off-the-shelf IAP Conditions shall be provided in the form of an XML document, as received by the IAP-SP from the IAC-issuing Jurisdiction. Each revision of each Off-the-shelf IAP Conditions document shall be provided in a separate file.

G.2.3.3 NCRs shall be provided in the form of an XML document, as originally sent to the IAC-issuing Jurisdiction by the IAP-SP. Each NCR shall be provided in a separate file.

G.2.3.4 PRs shall be provided in the form of an XML document, as originally sent to the IAC-issuing Jurisdiction by the IAP-SP. Each PR shall be provided in a separate file.

G.2.3.5 IVU Data Records shall be provided in ASCII text files that meet the following requirements:

f) A separate file shall exist, even if no records exist, for each unique combination of:

i) IVU identifier;

ii) each UTC day in the Audit Data Collection Period identified in

iii) G.2.2.1 and the prior records identified in G.2.2.3;

iv) type of IVU Data Record, being one of Position Record, Speed Record, Alarm Record, SD (Comments) Record or SD (Vehicle Type/TCM) Record;

v) the IAP-SP System's associated Specification Version Number and the IVU's associated Specification Version Number;

g) the internal format of the files shall be a sequence of zero or more fixed- length records, each of which is followed by a carriage return character (ASCII 13) and a line feed character (ASCII 10); and

h) the IVU Data Records within each file shall be in ascending order of date and time of generation.

Note: Where no IVU Data Records of the relevant type were generated on the day to which the file pertains, an empty file is produced. This enables the audit system to verify that no files are missing over the audit period.

G.2.3.6 Fixed length records within IVU Audit Data Record files shall be formatted in accordance with G.2.3.8, G.2.3.9, G.2.3.10, G.2.3.11 and G.2.3.12, and subject to the following conventions:

a) fields where the value does not occupy the full length allocated shall be padded by trailing spaces (for alphanumeric data) or leading zeros (for numeric and decimal data) in order to maintain the fixed length record structure; and

b) blank/void values for optional fields shall be specified by padding the entire field with spaces.

Note: In describing the format of fixed length record structures, the format of each field is specified as "YYYYMMDD" (date), "HHMMSS" (time), "D" (fixed decimal), "AN" (alphanumeric) or "N" numeric; the latter two formats include an associated field length. The format for decimal has an associated field length and number of decimal places (e.g. 9.2 is a total field length of 9 characters with 2 decimal places).

G.2.3.7 The IAP-SP shall include with each IVU Data Record the Receipt Date and Receipt Time (this data is used to assist in reproduction of Alarm NCRs).

Note: The Receipt Date and Receipt Time are the date and time at which the IVU Data Block, in which the IVU Data Record was transmitted, was received by the IAP-SP from the IVU.

G.2.3.8 Files containing Position Records shall have the record format detailed in Table G - 1.

Number	Name	Use	Format	Notes
POS001	Date	Mandatory	YYYYMMDD	The UTC format date from the IVU
POS002	Time	Mandatory	HHMMSS	The UTC timezone time from the IVU
POS003	Record Number	Mandatory	N (10)	As recorded by the IVU
POS004	Position Latitude	Optional	D (9.5)	Signed decimal degrees (GDA94) from -90.00000 to +90.00000, for example -39.12312
POS005	Position Longitude	Optional	D (10.5)	Signed decimal degrees (GDA94) from -180.00000 to +180.00000, for example +141.12345
POS006	Direction of Travel	Mandatory	D (5.1)	Decimal degrees from 000.0 to 359.9 (always 1 decimal place)
POS007	Number of Satellites	Mandatory	N (2)	
POS008	HDOP	Mandatory	D (4.1)	Decimal value
POS009	Ignition Switch Status	Mandatory	AN (1)	0 – Disconnected 1 – Off 2 – On
POS010	Other Independent Movement Sensor Status	Mandatory	AN (1)	0 – Disconnected 1 – No Movement 2 – Movement
POS011	Trailer Identifier #1	Optional	AN (20)	Trailer ID from first connected trailer
POS012	Trailer Identifier #2	Optional	AN (20)	Trailer ID from second connected trailer
POS013	Trailer Identifier #3	Optional	AN (20)	Trailer ID from third connected trailer
POS014	Trailer Identifier #4	Optional	AN (20)	Trailer ID from fourth connected trailer
POS015	Trailer Identifier #5	Optional	AN (20)	Trailer ID from fifth connected trailer
POS016	Trailer Identifier #6	Optional	AN (20)	Trailer ID from sixth connected trailer
POS017	Trailer Identifier #7	Optional	AN (20)	Trailer ID from seventh connected trailer
POS018	Trailer Identifier #8	Optional	AN (20)	Trailer ID from eighth connected trailer
POS019	Trailer Identifier #9	Optional	AN (20)	Trailer ID from ninth connected trailer
POS020	Trailer Identifier #10	Optional	AN (20)	Trailer ID from tenth connected trailer
POS021	Receipt Date	Mandatory	YYYYMMDD	Date of receipt by Service Provider (UTC)
POS022	Receipt Time	Mandatory	HHMMSS	Time of receipt by Service Provider (UTC)

Table G - 1. Position Record Format

Note: The following is an example Position Record (spaces have been shown as '^' and artificial field separators (|) have been inserted purely for clarity in this document):

```
20050101|123456|9876543210|39.12312|+141.12345|000.1|01|03.1|1|1|
TID000000001^^^^^^^^|TID000000002^^^^^^^^|TID000000003^^^^^^^^|
TID000000004^^^^^^^^|^^^^^^^^^^^^^^^^^^^^|^^^^^^^^^^^^^^^^^^^^|^^^^
^^^^^^^^^^^^^^^^|^^^^^^^^^^^^^^^^^^^^|^^^^^^^^^^^^^^^^^^^^|^^^^^^^^
^^^^^^^^^^^^|20050102|235956<CR><LF>
```

G.2.3.9 Files containing Speed Records shall have the record format detailed in Table G - 2. The IAP Speed Threshold is extracted from the framing data and added.

Number	Name	Use	Format	Notes
SPD001	Date	Mandatory	YYYYMMDD	The UTC format date from the IVU
SPD002	Time	Mandatory	HHMMSS	The UTC timezone time from the IVU
SPD003	Record Number	Mandatory	N (10)	As recorded by the IVU
SPD004	Position Latitude	Optional	D (9.5)	Signed decimal degrees (GDA94) from -90.00000 to +90.00000, for example -39.12312
SPD005	Position Longitude	Optional	D (10.5)	Signed decimal degrees (GDA94) from -180.00000 to +180.00000, for example +141.12345
SPD006	Speed	Mandatory	D (5.1)	For example 100.1
SPD007	Number of Satellites	Mandatory	N (2)	
SPD008	HDOP	Mandatory	D (4.1)	Decimal value
SPD009	Trailer Identifier #1	Optional	AN (20)	Trailer ID from first connected trailer
SPD010	Trailer Identifier #2	Optional	AN (20)	Trailer ID from second connected trailer
SPD011	Trailer Identifier #3	Optional	AN (20)	Trailer ID from third connected trailer
SPD012	Trailer Identifier #4	Optional	AN (20)	Trailer ID from fourth connected trailer
SPD013	Trailer Identifier #5	Optional	AN (20)	Trailer ID from fifth connected trailer
SPD014	Trailer Identifier #6	Optional	AN (20)	Trailer ID from sixth connected trailer
SPD015	Trailer Identifier #7	Optional	AN (20)	Trailer ID from seventh connected trailer
SPD016	Trailer Identifier #8	Optional	AN (20)	Trailer ID from eighth connected trailer
SPD017	Trailer Identifier #9	Optional	AN (20)	Trailer ID from ninth connected trailer
SPD018	Trailer Identifier #10	Optional	AN (20)	Trailer ID from tenth connected trailer
SPD019	IAP Speed Threshold	Optional	D (5.1)	The IAP Speed Threshold setting stored in the IVU, if applicable
SPD020	Receipt Date	Mandatory	YYYYMMDD	Date of receipt by Service Provider (UTC)
SPD021	Receipt Time	Mandatory	HHMMSS	Time of receipt by Service Provider (UTC)

Table G - 2. Speed Record Format

Note: The following is an example Speed Record (spaces have been shown as '^' and artificial field separators (|) inserted purely for clarity in this document):

```
20050101|123456|9876543210|-39.12312|+141.12345|110.0|01|03.0|
TID000000001^^^^^^^^|TID000000002^^^^^^^^|TID000000003^^^^^^^^|
TID000000004^^^^^^^^|^^^^^^^^^^^^^^^^^^^^|^^^^^^^^^^^^^^^^^^^^|
^^^^^^^^^^^^^^^^^^^^|^^^^^^^^^^^^^^^^^^^^|^^^^^^^^^^^^^^^^^^^^|
^^^^^^^^^^^^^^^^^^^^|120.0|20050102|235956
<CR><LF>
```

G.2.3.10 Each Alarm Record shall have the format detailed in Table G - 3.

Number	Name	Use	Format	Notes
ALM001	Date	Mandatory	YYYYMMDD	The UTC format date from the IVU
ALM002	Time	Mandatory	HHMMSS	The UTC timezone time from the IVU
ALM003	Record Number	Mandatory	N (10)	As recorded by the IVU
ALM004	Trigger event	Mandatory	N (2)	Event that triggered the Alarm Record (mapping of value from IVU to Alarm Code of 1 to 12)
ALM005	Receipt Date	Mandatory	YYYYMMDD	Date of receipt by Service Provider (UTC)
ALM006	Receipt Time	Mandatory	HHMMSS	Time of receipt by Service Provider (UTC)

Table G - 3. Alarm Record Format

Note: The following is an example Alarm Record (spaces have been shown as '^' and artificial field separators (|) inserted purely for clarity in this document):

```
20050101|123456|9876543210|08|20050102|235959<CR><LF>
```

G.2.3.11 Each SD (Comments) Record shall have the format detailed in Table G - 4.

Number	Name	Use	Format	Notes
SDC001	Date	Mandatory	YYYYMMDD	The UTC format date from the IVU
SDC002	Time	Mandatory	HHMMSS	The UTC timezone time from the IVU
SDC003	Record Number	Mandatory	N (10)	As recorded by the IVU
SDC004	IAP Specification Version	Mandatory	AN (10)	The Specification Version Number against which the Comment Code fields were collected.
SDC005	Comment Code	Mandatory	N (4)	Predefined code to identify Comment Name
SDC006	Comment Name	Mandatory	AN (100)	Predefined comment text
SDC007	Comment Text	Mandatory	AN (256)	Manually entered free-form text
SDC008	Receipt Date	Mandatory	YYYYMMDD	Date of receipt by Service Provider (UTC)
SDC009	Receipt Time	Mandatory	HHMMSS	Time of receipt by Service Provider (UTC)

Table G - 4. SD (Comments) Record Format

Note: The following is an example SD (Comments) Record (spaces have been shown as '^' and artificial field separators (|) inserted purely for clarity in this document):

```
20050101|123456|9876543210|0000001.05|0002|Redirection by
Authorised Officer^^^^...^^^^|Advised by PC#123^^^^...^^^^
|20050102|235959<CR><LF>
```

G.2.3.12 Each SD (Vehicle Type/TCM) Record shall have the format detailed in Table G - 5.

Number	Name	Use	Format	Notes
SDM001	Date	Mandatory	YYYYMMDD	The UTC format date from the IVU
SDM002	Time	Mandatory	HHMMSS	The UTC timezone time from the IVU
SDM003	Record Number	Mandatory	N (10)	As recorded by the IVU or Blank/Void where the SD Record was generated in the IAP-SP System.
SDM004	IAP Specification Version	Mandatory	AN (10)	The Specification Version Number against which the Vehicle Type fields were collected.
SDM005	Vehicle Category Code	Mandatory	N (4)	Predefined code to identify Vehicle Category
SDM006	Vehicle Category Name	Mandatory	AN (100)	Vehicle category name/description
SDM007	Axle Count	Mandatory	N (2)	Value of 00 should be used when this field is Not Applicable (e.g vehicle configuration is prime mover only).
SDM008	Mass Status	Mandatory	AN (1)	L – Load N – No Load
SDM009	Total Combination Mass	Optional	D (5.1)	Decimal value in tonne Should be blank if Mass Status = “N” Should be populated if Mass Status = “L”
SDM010	Receipt Date	Mandatory	YYYYMMDD	Date of receipt by Service Provider (UTC)
SDM011	Receipt Time	Mandatory	HHMMSS	Time of receipt by Service Provider (UTC)

Table G - 5. SD (Vehicle Type/TCM) Record Format

Note: The following is an example SD (Vehicle Type/TCM) Record (spaces have been shown as ‘^’ and artificial field separators (|) inserted purely for clarity in this document):

```
20050101|123456|9876543210|0000001.05|0001|AAAAAAAAAAA^^^^...^^^^|12|L|
123.4|20050102|235959<CR><LF>
```

G.2.4 Packaging

G.2.4.1 The IAP-SP shall package the required audit data:

a) where possible, across one or more DVD media. Where multiple “volumes” of data are provided, Off-the-shelf IAP Conditions, and PRs shall be packaged on the first volume. The number of volumes shall not exceed four (4); or

b) on one removable, external hard disk unit with USB2 or IEEE 1394 (Firewire) interface.

G.2.4.2 The audit data media shall be formatted using a file system that is readable from Microsoft Windows and Unix operating systems, and that supports “long file names”.

G.2.4.3 Each volume of data provided by the IAP-SP shall have the directory structure shown in Figure G - 3.

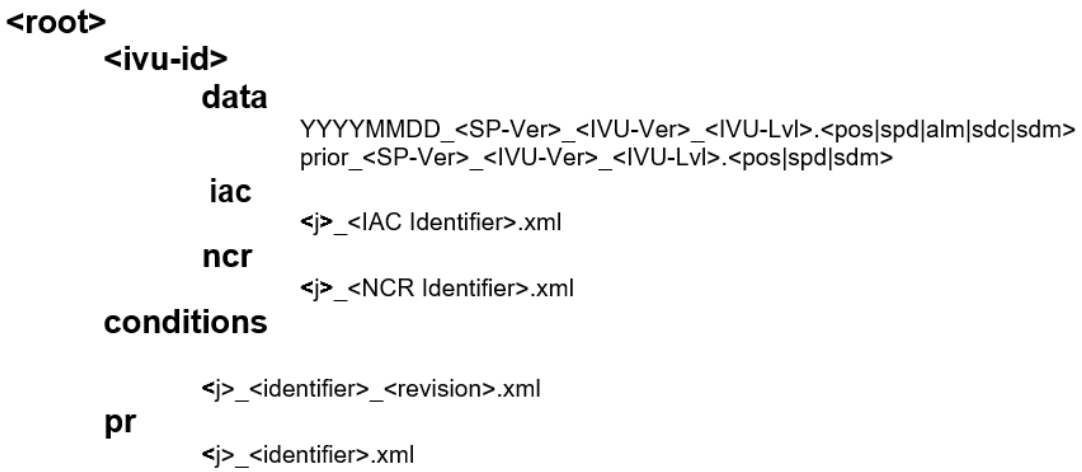


Figure G - 3. Directory Structure

G.2.4.4 Each file of audit data (located within the distribution media) shall be named in accordance with Table G - 6.

Data	Directory	Filename
General		• <ivu-id> is the unique IVU identifier • <j> is the one character TCA assigned Jurisdiction code • <SP-Ver> is the Specification Version Number which the IAP-SP System is certified against at the time of the NCR audit reference date/time stamp • <IVU-Ver> is the Specification Version Number that the IVU (including firmware and reference tables) is Type-approved against • <IVU-Lvl> is the level of type-approval of the IVU
IVU	<ivu-id>/data	<YYYYMMDD>_<SP-Ver>_<IVU-Ver>_<IVU-Lvl>.<pos|spd|alm|sdc|sdm> • YYYYMMDD is UTC day to which all data within the file pertains • pos indicates Position Record data • spd indicates Speed Record data • alm indicates Alarm Record data • sdc indicates SD (Comment) Record Data • sdm indicates SD (Vehicle Type/TCM) Record data
IVU	<ivu-id>/data	Prior_<SP-Ver>_<IVU-Ver>_<IVU-Lvl>.<sdm|pos|spd> *For last SD Record (*Vehicle Type/TCM) *received prior to audit period (refer G.2.2.3)* *For last Position/Speed Record, the record from which last known position is established for the commencement of data.*
IAC	<ivu-id>/iac	<j>_<IAC identifier>.xml • IAC identifier is Jurisdiction-assigned IAC identifier
NCR	<ivu-id>/ncr	<j>_<NCR identifier>.xml • NCR identifier is IAP-SP-assigned NCR identifier
Off-the-shelf Conditions	conditions	<j>_<identifier>_<revision>.xml • identifier is IAC-issuing Jurisdiction-assigned Off-the-shelf IAP Conditions ID • revision is IAC-issuing Jurisdiction-assigned Off-the-shelf IAP Conditions
PR	pr	<j>_<PR identifier>.xml • PR identifier is IAP-SP-assigned PR identifier

Table G - 6. Data File Naming Convention

G.2.4.5 The following file types shall be compressed when provided by the IAP-SP:

a) IVU data files (file extension “pos|spd|alm|sdc|sdm”); and

b) NCR data files (file extension “xml”).

G.2.4.6 File compression shall be implemented by using any software application that is able to be decompressed using the open source program *gunzip, Version 1.2.4*.

G.2.4.7 Compressed files shall be named identically to the original source file, but with an added extension of either “gz” or “zip”.

Appendix H Business to Business Interface Specification

Contents

H.1 Introduction

H.1.1 Purpose of Appendix

H.1.1.1 The purpose of this Appendix is to specify and explain the Business-to-Business (B2B) document formats (XML Schemas) and communication interfaces (Web Services) that have been designed to support the IAP Tier 1 data interchanges as documented in the main body of this Specification. These B2B document formats and interfaces contain components to be implemented by both IAC-issuing Jurisdictions and IAP-SPs.

H.1.1.2 The requirements as specified in this Appendix are explicit for IAP-SPs but implied for IAC-issuing Jurisdictions.

H.1.1.3 The scope of this document excludes Tier 2 data interchanges.

H.1.2 References

H.1.2.1 Documents referenced in this Appendix are listed below:

a) [SOAP] SOAP: Simple Object Access Protocol 1.1, W3C Note, 8th May 2000.

b) [WSDL] Web Services Description Language (WSDL) 1.1, W3C Note, 15th March 2001.

c) [WSS] Web Services Security: SOAP Message Security 1.0 (WS-Security 2004), OASIS Standard 200401, March 2004.

H.2 Overview

H.2.1 Architectural Context

H.2.1.1 This Appendix defines an electronic Business-to-Business (B2B) architecture to support Tier 1 data interchange within the Intelligent Access Program (IAP). This architecture has been designed to accommodate a number of specific architectural requirements as follows:

a) *formality* – the architecture must exist in the form of a specification (i.e. rather than as a software product) that is able to be implemented consistently by each of the IAP-SPs and IAC-issuing Jurisdictions, such that all IAP-SPs are rendered uniformly to all IAC-issuing Jurisdictions, and that all IAC-issuing Jurisdictions are rendered uniformly to all IAP-SPs, as illustrated in *Figure H - 1*;

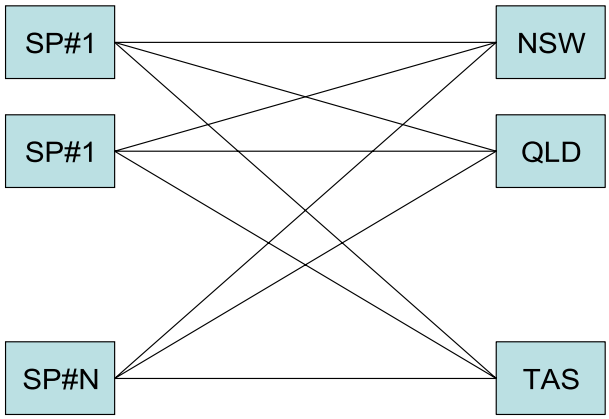


Figure H - 1. IAP B2B Connectivity Topology

b) *security* - the architecture must offer a high-degree of privacy (i.e. confidentiality of data) and non-repudiation (i.e. confidence regarding the source and integrity of transmitted data);

c) *flexibility* - the architecture must allow for evolving business practices and increases in scope over time;

d) scalability - the architecture must be applicable to both 'small' and 'large' Jurisdictions (and IAC-issuing Jurisdictions) with transaction loads ranging from tens to tens-of-thousands per day; and

e) *achievability* - the architecture must be straightforward to implement, especially for those IAC-issuing Jurisdictions and IAP-SPs for which IAP implementation and operation may be tightly constrained by budget, IT infrastructure and availability of technical expertise.

H.2.1.2 The requirements outlined above are reflected in the design detailed below.

H.2.2 Business Model

H.2.2.1 The B2B solution specified in this document has been designed to support a sub- set of the IAP business processes through the electronic exchange of data between IAP-SPs and IAC-issuing Jurisdictions; a full and formal description of the IAP business processes appears in the main document *IAP Functional & Technical Specification*.

H.2.2.2 The use case diagram in *Figure H - 2* captures the IAP business processes supported by the B2B solution.

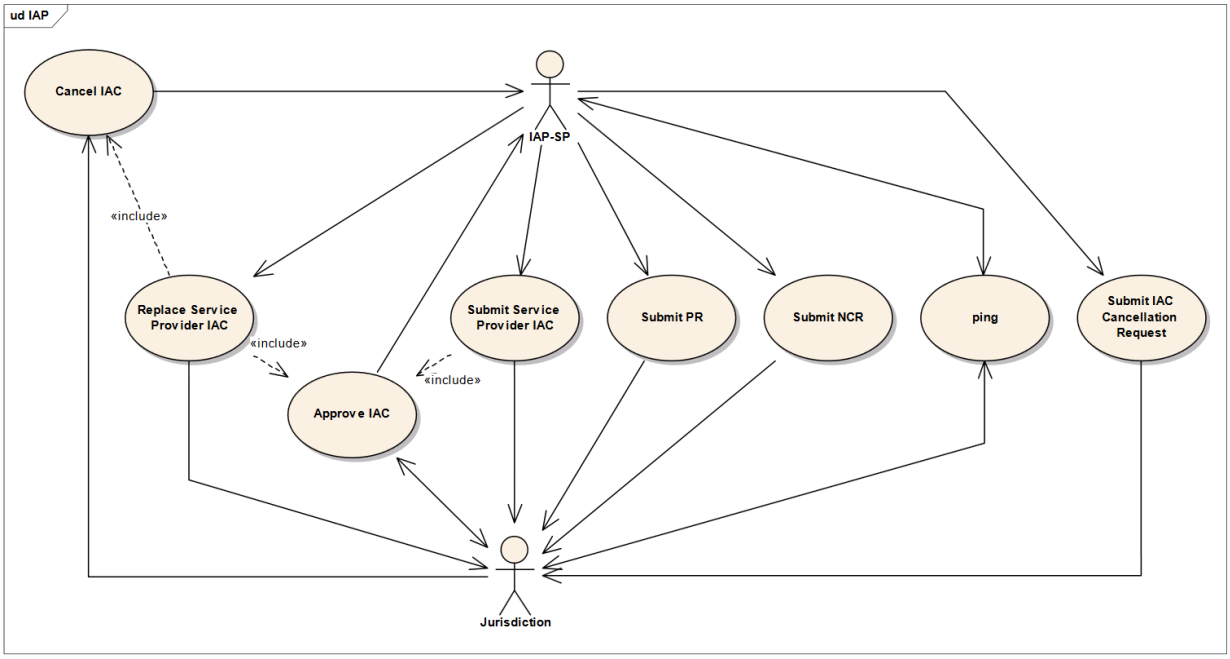


Figure H - 2. IAP B2B Use Case Model

H.2.2.3 The business processes appearing within this diagram are:

a) Submit Service Provider IAC – this process occurs when an IAP-SP has completed the *Service Provider Section* (Part 3) of an IAC, including the fitting of IVU and TID devices. In the normal case the IAP-SP submits the *Service Provider Section* (Part 3) to the IAC-issuing Jurisdiction, and the IAC-issuing Jurisdiction subsequently approves the IAC (Part 4) (*refer H.2.2.3d*);

b) Replace Service Provider IAC – this process occurs when an IAP-SP wishes to revise the *Service Provider Section* (Part 3) of an IAC, perhaps because an IVU or TID device has been replaced. In the normal case, the IAP-SP submits the revised *Service Provider Section* (Part 3) to the IAC-issuing Jurisdiction, which cancels the existing IAC (*refer H.2.2.3c*) and fast-track approves a replacement IAC (*refer H.2.2.3d*);

c) Cancel IAC – this process is initiated by the IAC-issuing Jurisdiction either independently (e.g. at the request of the Transport Operator or IAP-SP), or as a constituent activity for replacing an IAC with a new IAC (i.e. the existing IAC is cancelled). In the normal case the IAC-issuing Jurisdiction cancels the IAC and electronically notifies the IAP-SP that this has occurred by sending the IAC with the changed status;

d) Approve IAC – this process is internal to the IAC-issuing Jurisdiction and can only occur as a constituent activity of the Submit Service Provider IAC and Replace Service Provider IAC processes. In the normal case the IAC-issuing Jurisdiction approves the IAC and electronically notifies the IAP-SP that this has occurred by sending the IAC with the changed status;

e) Submit NCR – this process occurs when an IAP-SP generates a Non-Compliance Report (NCR) and electronically submits it to the IAC-issuing Jurisdiction;

f) Submit PR – this process occurs when an IAP-SP generates a Participants Report (PR) and electronically submits it to the IAC-issuing Jurisdiction;

g) Submit IAC Cancellation Request – this process occurs when an IAP-SP has a business requirement to request that the IAC-issuing Jurisdiction cancels an IAC and electronically submits this request to the IAC-issuing Jurisdiction; and

h) Ping – this is a technically-oriented business process and involves either the IAC-issuing Jurisdiction IAP software or the IAP-SP IAP software testing the connection to counterpart organisations' IAP software, either automatically (e.g. as a scheduled and periodic background task) or upon operator request.

H.2.2.4 Each of these business processes (except Ping) is discussed in further detail later in this document, with the exception of Approve IAC which only appears as a constituent activity within other business processes.

H.2.3 Technical Model

H.2.3.1 The B2B solution is predicated upon Web Services technology, whereby IAP-SPs and IAC-issuing Jurisdictions communicate over the Internet using XML messages and the HTTP protocol. The Web Services Description Language (WSDL) is used to formally specify two 'Web Services', each of which provides a discrete set of operations that may be invoked by counterpart organisations:

a) the IAC-issuing Jurisdiction Web Service provides a consistent interface to each IAC-issuing Jurisdiction's IAP software, and exposes the following operations for invocation by IAP-SP IAP software:

i) *submitServiceProviderIac* – invoked by IAP-SPs to submit the

ii) Service Provider Section (Part 3);

iii) *replaceServiceProviderIac* – invoked by IAP-SPs to replace the

iv) Service Provider Section (Part 3) of an IAC;

v) *submitNcr* – invoked by IAP-SPs to submit a Non-Compliance Report (NCR);

vi) *submitPr* – invoked by IAP-SPs to submit a Participants Report (PR);

vii) *submitIacCancellationRequest* – invoked by IAP-SPs to submit an IAC Cancellation Request; and

viii) *ping* – invoked by IAP-SPs to confirm the current availability of the IAC-issuing Jurisdiction's IAP software.

b) the IAP-SP Web Service provides a consistent interface to each IAP-SP's system software, and exposes the following operations for invocation by IAC-issuing Jurisdiction IAP software:

i) *notifyIac* – invoked by IAC-issuing Jurisdictions to advise of a change to the IAC and involves sending the revised IAC to the IAP-SP;

ii) *notifyRejection* – invoked by IAC-issuing Jurisdictions to advise that a *Service Provider Section* (Part 3) for an IAC has been rejected; and

iii) *ping* – invoked by IAC-issuing Jurisdictions to confirm the current availability of the IAP-SP's IAP software.

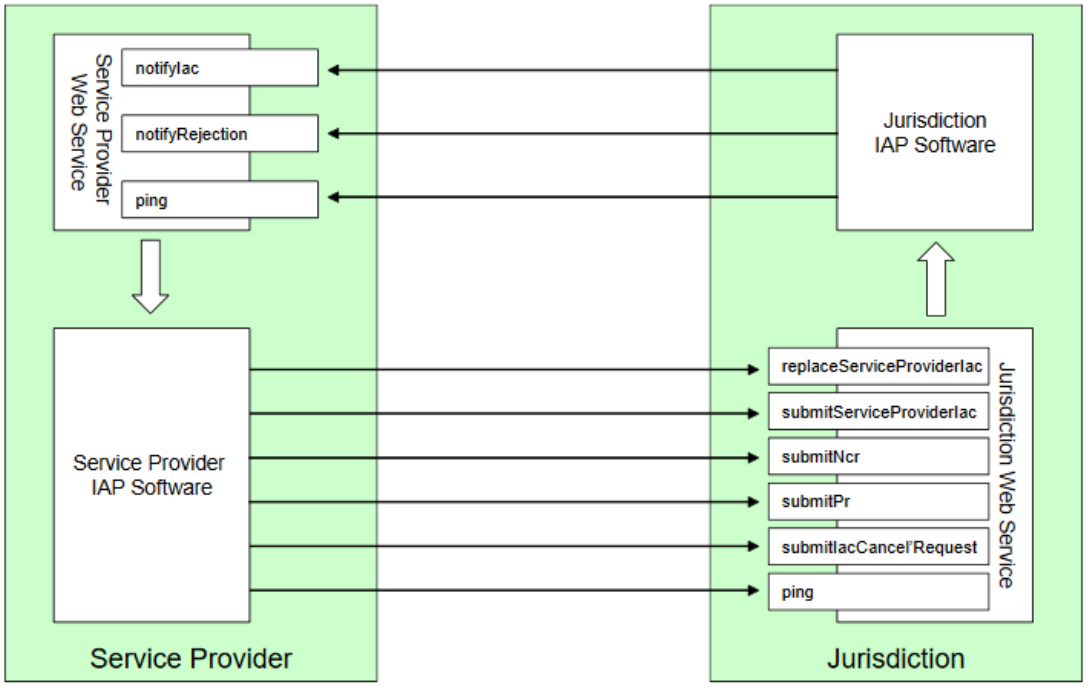


Figure H - 3. IAP B2B Component Model

H.2.3.2 As shown in *Figure H - 3*, the B2B solution is logically composed of four software components:

a) Jurisdiction IAP Software – implements IAC-issuing Jurisdictional aspects of IAP, including a Web Service client for invoking operations on the IAP-SP Web Service;

b) Jurisdiction Web Service – a wrapper around the Jurisdictional IAP Software that enables IAP-SPs to invoke Web Service operations on the IAC-issuing Jurisdiction;

c) Service Provider IAP Software – implements IAP-SP aspects of IAP, including a Web Service client for invoking operations on the Jurisdiction Web Service; and

d) Service Provider Web Service – a wrapper around the IAP-SP IAP Software that enables IAC-issuing Jurisdictions to invoke Web Service operations on the IAP-SP.

H.2.3.3 The B2B solution is underpinned by a security layer that addresses stated business requirements, and also stated architectural requirements of consistency across IAP-SPs and IAC-issuing Jurisdictions and achievability for all stakeholders. It involves:

a) use of HTTPS (i.e. HTTP over SSL) to provide confidentiality for transactions over public networks, and server authentication; and

b) use of WS-Security digital signatures using PKI X.509 digital certificates to provide data integrity and client authentication. By using ABN-DSC digital certificates the identity of the message signer is available as an ABN and so can be correlated directly to known IAP-SPs and IAC-issuing Jurisdictions without the need for additional identity management infrastructure.

H.2.3.4 Within the Web Service definitions, those operations that support electronic document exchange are underpinned by a simple document exchange model that permits and requires the sender to resend until certain of delivery, and that enables the receiver to resolve multiple receipt of the same document.

H.3 Business Flows

H.3.1 Service Provider Submits IAC Service Provider Section

H.3.1.1 This use case occurs when an IAP-SP has generated an IAC *Service Provider Section* (Part 3) for an IAC, including fitting of In-Vehicle Units (IVUs) and Trailer-Identification Devices (TIDs).

H.3.1.2 As illustrated in *Figure H - 4*, the normal flow of events within this use case is:

a) The IAP-SP delivers the IAC *Service Provider Section* (Part 3) to the IAC-issuing Jurisdiction using the Web Service operation *submitServiceProviderIac;*

b) The IAC-issuing Jurisdiction performs offline processing to validate the IAC *Service Provider Section*; and

c) The IAC-issuing Jurisdiction attaches the IAC *Service Provider Section* (Part 3) to the Interim IAC (Parts 1 and 2) and approves the IAC (Part 4); this includes notifying the IAP-SP by delivering the entire IAC to the IAP-SP using the Web Service operation *notifyIac.*

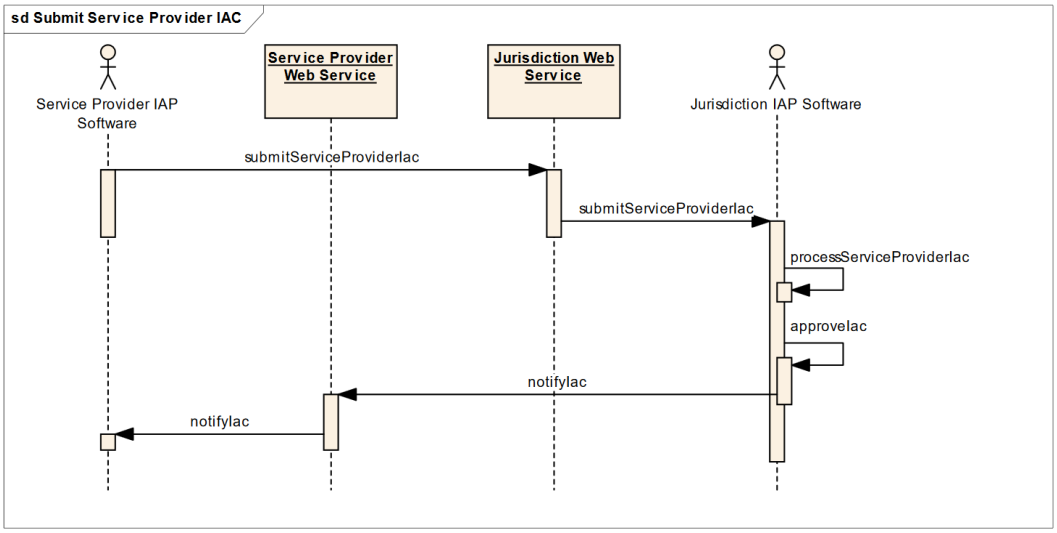


Figure H - 4. Submit Service Provider IAC (Normal Flow)

H.3.1.3 Significant alternative flows are where the IAC-issuing Jurisdiction:

a) finds the IAC *Service Provider Section* (Part 3) to be invalid. The IAP-SP is notified by the IAC-issuing Jurisdiction invoking the Web Service operation *notifyRejection* (*see Figure H - 5*). Note that rejection of an IAC *Service Provider Section* (Part 3) does not affect the referenced IAC; and

b) accepts the IAC *Service Provider Section* (Part 3), attaches it to the relevant Interim IAC (Parts 1 and 2), but then denies the IAC (Part 4); this includes notifying the IAP-SP by delivering the entire IAC to the IAP-SP using the Web Service operation *notifyIac.*

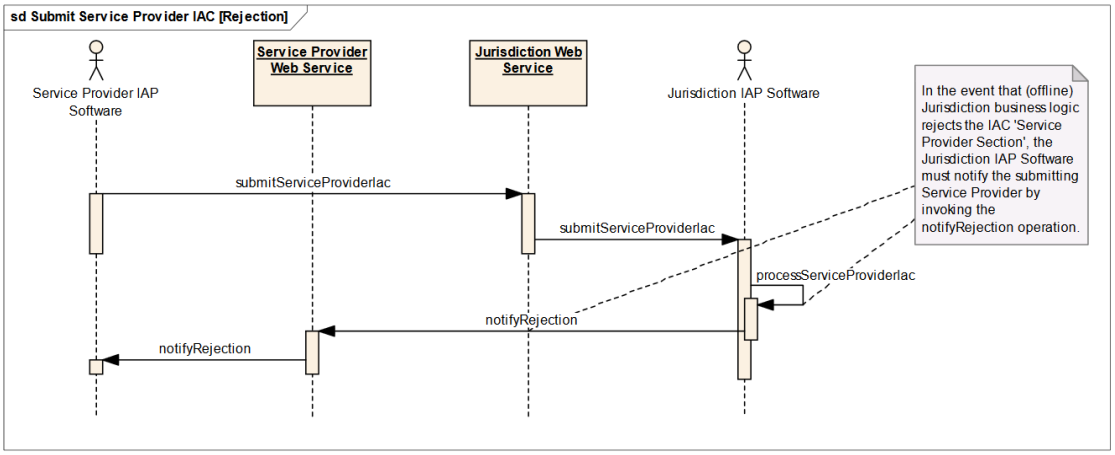


Figure H - 5. Submit Service Provider IAC (Rejection Alternate Flow)

H.3.2 Service Provider Replaces IAC Service Provider Section

H.3.2.1 This use case occurs when an IAP-SP has generated a replacement IAC *Service Provider Section* (Part 3) for an IAC, perhaps because an unserviceable IVU or TID has been replaced.

H.3.2.2 As illustrated in *Figure H - 6*, the normal flow of events within this use case is:

a) The IAP-SP delivers the replacement IAC *Service Provider Section* (Part 3) to the IAC-issuing Jurisdiction using the Web Service operation *replaceServiceProviderIac;*

b) The IAC-issuing Jurisdiction performs offline processing to validate the IAC *Service Provider Section* (Part 3);

c) The IAC-issuing Jurisdiction cancels the existing IAC, as per the use case 'Cancel IAC'; this includes notifying the IAP-SP of the cancellation of the IAC by invoking the Web Service operation *notifyIac*; and

d) The IAC-issuing Jurisdiction creates and automatically approves a replacement IAC; this includes notifying the IAP-SP by delivering the entire IAC to the IAP-SP using the Web Service operation *notifyIac.*

Note: Steps c. and d. must be atomic and no IAP-SP notifications shall occur until both steps are successfully completed within the IAC-issuing Jurisdiction.

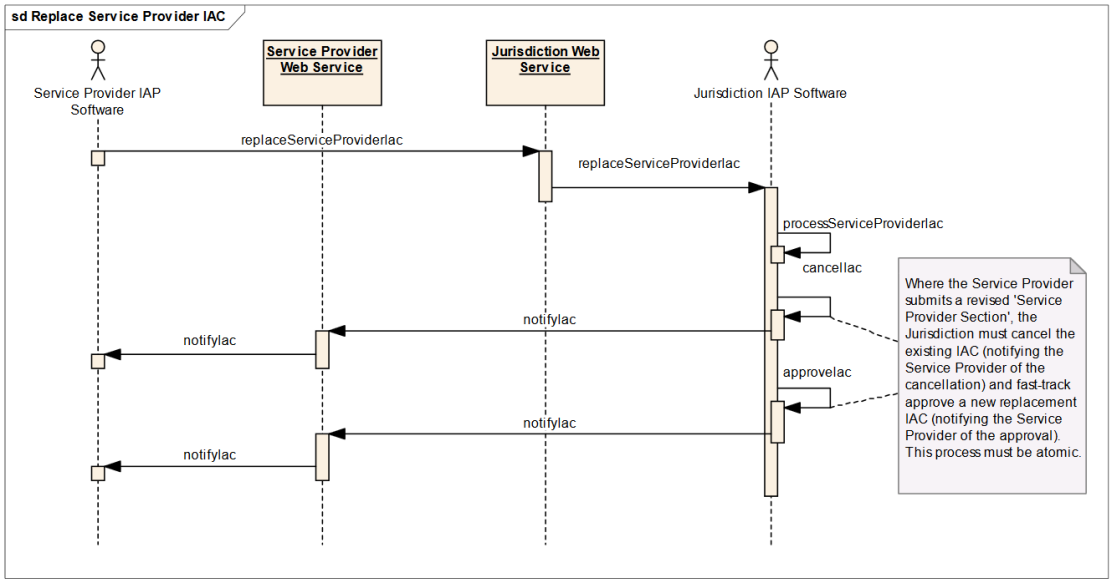


Figure H - 6. Replace Service Provider IAC (Normal Flow)

H.3.2.3 Significant alternative flows are where the IAC-issuing Jurisdiction:

a) finds the IAC *Service Provider Section* (Part 3) to be invalid, the IAP-SP is notified by the IAC-issuing Jurisdiction invoking the Web Service operation *notifyRejection* (*see Figure H - 5*). Note that rejection of an IAC *Service Provider Section* does not affect the state of the referenced IAC.

H.3.3 IAC-issuing Jurisdiction Cancels IAC

H.3.3.1 This use case occurs when an IAC-issuing Jurisdiction needs to cancel an IAC, either as an integral component of the 'Service Provider Replaces IAC Service Provider Section' use case or independently (e.g. the Transport Operator or IAP-SP has requested a cancellation; the IAC-issuing Jurisdiction initiates a cancellation).

H.3.3.2 The normal flow of events within this use case is:

a) The IAC-issuing Jurisdiction modifies the IAC by attaching a Cancellation Section and changing the status to Cancelled; and

b) Where the IAC was previously in an Approved state, the IAC-issuing Jurisdiction notifies the IAP-SP of the change-of-state by delivering the entire IAC (with cancelled state) to the IAP-SP via the Web Service operation *notifyIac.*

H.3.3.3 There are no significant alternative flows.

H.3.4 Service Provider Submits Non-Compliance Report

H.3.4.1 This use case occurs when an IAP-SP has generated a Non-Compliance Report for an IAC-issuing Jurisdiction.

H.3.4.2 As illustrated in *Figure H - 7*, the normal flow of events within this use case is:

a) The IAP-SP delivers the Non-Compliance Report to the IAC-issuing Jurisdiction using the Web Service operation *submitNcr;*

b) The IAC-issuing Jurisdiction performs offline processing to validate the Non-Compliance Report; and

c) The IAC-issuing Jurisdiction stores the Non-Compliance Report.

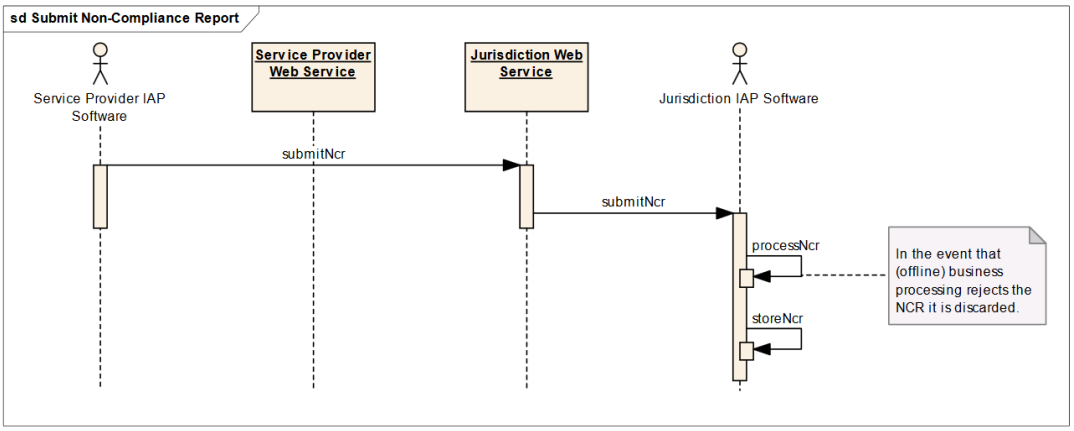


Figure H - 7. Service Provider Submits NCR (Normal Flow)

H.3.4.3 Significant alternative flows are where the IAC-issuing Jurisdiction:

a) finds the Non-Compliance Report to be invalid, this issue is resolved outside the scope of the B2B interface and the invalid Non-Compliance Report is discarded.

H.3.5 Service Provider Submits Participants Report

H.3.5.1 This use case occurs when an IAP-SP has generated a Participants Report for an IAC-issuing Jurisdiction, probably through completion of (end-of-month) reconciliation processing.

H.3.5.2 As illustrated in *Figure H - 8*, the normal flow of events within this use case is:

a) The IAP-SP delivers the Participants Report to the IAC-issuing Jurisdiction using the Web Service operation *submitPR;*

b) The IAC-issuing Jurisdiction performs offline processing to validate the Participants Report; and

c) The IAC-issuing Jurisdiction stores the Participants Report.

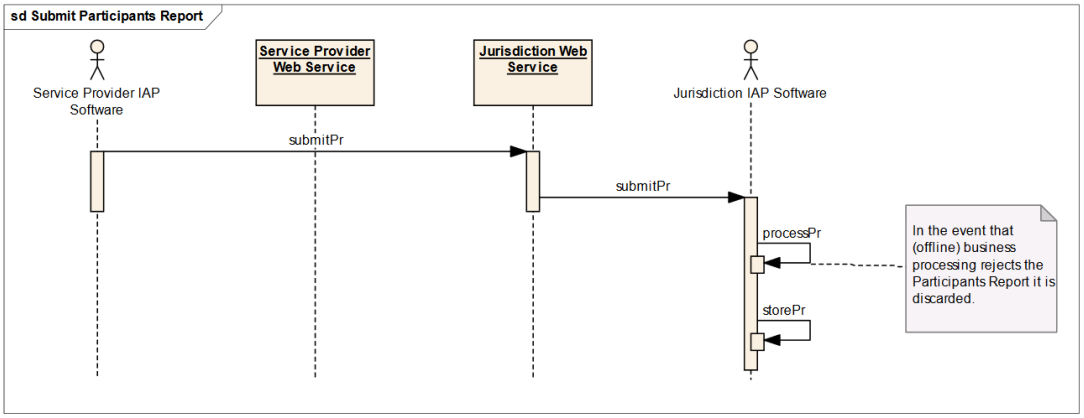


Figure H - 8. Service Provider Submits PR (Normal Flow)

H.3.5.3 Significant alternative flows are where the IAC-issuing Jurisdiction:

a) finds the Participants Report to be invalid, this issue is resolved outside the scope of the B2B interface and the invalid Participants Report is discarded.

H.3.6 Service Provider Submits IAC Cancellation Request

H.3.6.1 This use case occurs when an IAP-SP has a business requirement to request that an IAC-issuing Jurisdiction cancel a previously-issued and approved IAC. It is emphasised that the scope of this function does not include the actual cancellation of the IAC, as this is considered an issue of IAC-issuing Jurisdictional policy and responsibility.

H.3.6.2 As illustrated in *Figure H - 9*, the normal flow of events in this use case is:

a) The IAP-SP delivers the *IAC Cancellation Request* to the IAC-issuing Jurisdiction using the Web Service operation submitIacCancellationRequest;

b) The IAC-issuing Jurisdiction performs offline processing to validate (but not 'action') the IAC Cancellation Request; and

c) The IAC-issuing Jurisdiction stores the IAC Cancellation Request for follow-on business processing (e.g. actioning or denial).

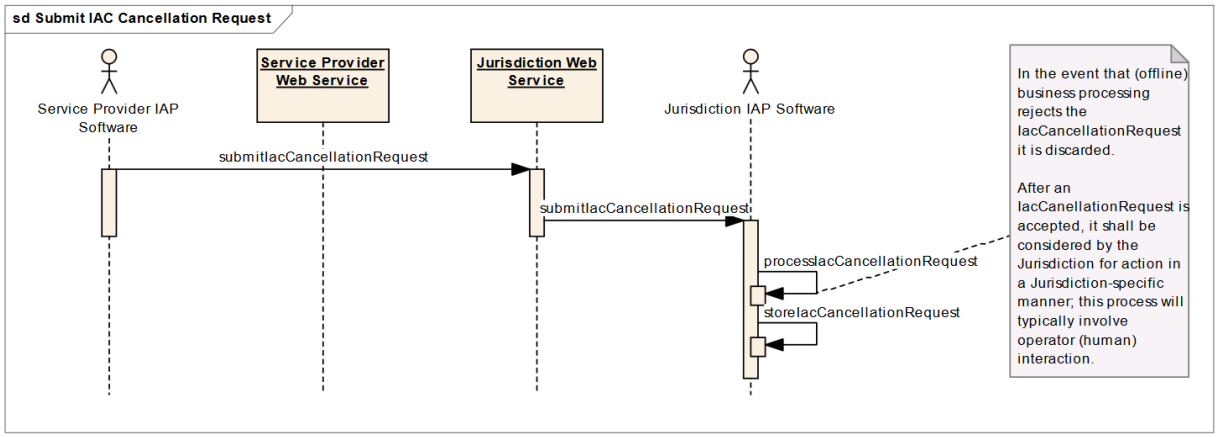


Figure H - 9. Service Provider Submits IAC Cancellation Request (Normal Flow)

H.3.6.3 Significant alternative flows are where the IAC-issuing Jurisdiction:

a) finds the IAC Cancellation Request to be invalid, this issue is resolved outside the scope of the B2B interface.

H.4 Specification

H.4.1 Standards and Interoperability

H.4.1.1 The B2B interface shall be implemented against the following standards and technologies:

a) XML Schema;

b) SOAP 1.1 [SOAP];

c) WSDL 1.1 [WSDL]; and

d) WS-Security 2004 [WSS].

H.4.1.2 The B2B interface shall support the IPv4 protocol.

H.4.2 Security

H.4.2.1 The B2B interface shall use the Internet as a transmission network.

H.4.2.2 All B2B interface transmissions shall use the HTTPS protocol (i.e. HTTP over TLS 1.2 or better) to ensure the confidentiality of data:

a) B2B interface clients shall not connect to B2B interface servers except via HTTPS;

b) B2B interface servers shall not accept B2B interface client connections except via HTTPS; and

c) B2B interface servers shall use 128-bit SSL certificate issued by a certification authority that verifies (at minimum) ownership of the domain name encoded within the subject distinguished name.

Note: Further information concerning accepted encryption protocols may be obtained from TCA.

H.4.2.3 All B2B interface transmissions shall use WS-Security coupled with PKI certificates to ensure message integrity and enable client authentication:

a) digital signatures shall be applied to the SOAP body of all Web Service requests, as per WS-Security;

b) digital signatures shall NOT be applied to the SOAP body of any Web Service responses[1];

[1] WS-Security is not permitted to be applied to Web Service responses for two reasons. Firstly, it is not required as server authentication is provided by the HTTPS (HTTP over SSL) protocol. Secondly, the Web Service response is formed after the Web Service operation has been completed and any failure by the Web Service client to process the response (e.g. verification of the digital signature) may cause the contents of the response to be lost.

c) digital signatures shall be formed using the SHA-1 digest algorithm and 1024-bit RSA encryption using signer's PKI certificate (binary security token);

d) digital signing certificates shall be ABN-DSC device (type 3) containing an ABN; and

e) WS-Security timestamps shall NOT be applied to Web Service requests or responses.

H.4.2.4 Upon receiving a Web Service request, the B2B interface server shall reject the request in accordance with H.4.2.5:

a) where it is not digitally signed in accordance with H.4.2.3;

b) where it is digitally signed, but where the digital signature fails verification (e.g. bad data, incorrect signature);

c) where it is digitally signed, but where the signer's digital certificate is not yet in force, expired, untrusted or does not contain an ABN. The B2B interface server must reject the request if the signer's digital certificate is checked for revocation and subsequently found to be revoked. However, it is not required that the B2B interface server check the signer's digital certificate for revocation;[2]

d) where the ABN contained within the signer's digital certificate does not match the ABN for the sender quoted within the (addressing header of the) Web Service request;

e) where the ABN contained within the signer's digital certificate does not represent an entity with which there is an established e-Business relationship;

f) where the request is not sufficiently well formed and valid to enable it to be correctly processed.

H.4.2.5 In circumstances requiring the rejection of a Web Service request associated with operation-independent processing, including the provisions of H.4.2.4, but excluding the provisions of H.4.3.4, the B2B interface server shall raise a SOAP fault as follows:

a) the faultcode element[3] should (where possible) be set to:

i) *iapws:SENDER_INVALID* – where processing has not occurred because the Web Service server software cannot determine or verify the identity (e.g. ABN) of the sender;

ii) *iapws:SENDER_UNKNOWN* – where processing has not occurred because the sender is not known as a trading partner;

iii) *iapws:SENDER_MISMATCH* – where processing has not occurred because the identity of the sender (e.g. ABN) is inconsistent with that quoted within the Web Service request;

[2] It is considered that certificate revocation will not be a significant issue within the IAP B2B environment due to the very limited number of trading partners (e.g. less than 20).

[3] The XML prefix 'soap' represents the XML namespace 'http://schemas.xmlsoap.org/soap/envelope/' and is equivalent to any alternate prefix defined for this XML namespace. The XML prefix 'iapws' represents the XML namespace 'http://www.tca.gov.au/schemas/iap/iapws/2006-04' and is equivalent to any alternate prefix defined for this XML namespace.

iv) *iapws:RECEIVER_UNKNOWN* – where the processing has not occurred because the receiver is not a trading partner represented by the B2B Interface server software;

v) *iapws:UNAVAILABLE* – where processing has not occurred due to a transient and known outage of the Web Service server software;

vi) *soap:Client* (or a qualified name starting with soap:Client) - where the processing error relates to the Web Service request itself, but where it is not possible or appropriate to assign a value as described above; and

vii) *soap:Server* (or a qualified name starting with soap:Server) – where the processing error relates to the processing of the Web Service request and not to the Web Service request itself, but where it is not possible or appropriate to assign a value as described above. Such circumstances are usually transitory;

b) the faultstring element shall be human readable string describing the cause of the fault; and

c) the detail element may be populated.

H.4.3 Reliable Web Service Operation Stereotype

H.4.3.1 For the set of *reliable*[4] Web Service operations (being *submitServiceProviderIac, replaceServiceProviderIac, submitNcr, submitPr, submitIacCancellationRequest* and *notifyIac*) and for the operation n*otifyRejection*[5] the B2B interface client shall:

a) assign a unique alphanumeric identifier to each unique request (note: for notifyRejection the request identifier shall be that taken from the original Web Service request that is being rejected). This request identifier is maintained across all attempts to send the request to the B2B interface server; and

b) attempt to re-send the request (i.e. by invoking the appropriate Web Service operation) using the same request identifier at periods of not less than one hour until such time that one of the following conditions is met:

i) a non-SOAP fault Web Service response issued by the B2B interface server is received by the client. This response will either explicitly reject or accept the request; in the latter case the response will include a receipt timestamp that may be used as the starting point for prescribed service level agreements (e.g. IAC approval); or

ii) a SOAP fault issued by the B2B interface server is received by the client, and this fault has a 'faultcode' value that is not soap:Server, that does not start with soap:Server or that is not iapws:UNAVAILABLE; or

iii) eight (8) consecutive attempts to send the request have occurred;

---

[4] Those Web Service operations that relate to the delivery of an XML document (e.g. IAC) and that require that the document be delivered exactly once (i.e. not less than once and not more than once).

[5] The operation notifyRejection is not formally a reliable operation as it does not contain an XML document, and is not subject to duplicate detection. However, it is similar to the reliable operations in that it requires the Web Service client to re-send the request in the event of failure.

c) where attempts to send the request pursuant to H.4.3.1b have failed, the sender shall endeavour to resolve this issue outside the scope of B2B interface; this is done by communicating with the intended recipient via Tier 2 data interchange to resolve the issue;

d) upon resolution of the issue referred to in H.4.3.1c, the Web Service client shall resend the original request via its Tier 1 B2B interface.

H.4.3.2 For the set of *reliable* Web Service operations the B2B interface server shall:

a) perform normal inbound request and outbound response processing as per other elements of this specification (e.g. security, logging);

b) where the server is capable of performing duplicate detection for request identifiers and the request identifier is a duplicate, form an acceptance response including the original date and time of receipt and by setting the response flag 'duplicateDetected' to true. Note that de-duplication shall only be performed against accepted Web Service requests (i.e. re-sends of rejected messages are not considered duplicates);

c) where the server is not capable of performing duplicate detection for request identifiers or where the request is deemed not to be a duplicate, exercise any optional online and synchronous request processing capabilities that may cause the request to be rejected (e.g. correlation of IAC identifiers, cross-checking of IAC state). In the event that any such processing causes the Web Service request to be rejected, form a rejection response in accordance with H.4.3.4; and

d) where the server decides to accept a Web Service request, form an acceptance response including the date and time of receipt and a duplicateDetected flag set to false. In addition, the server shall record the request identifier, date and time of receipt and associated details for future use (e.g. Web Service callback operations, request de-duplication).

H.4.3.3 For the set of reliable Web Service operations the B2B interface server shall validate the IAP document contained with the Web Service request (i.e. IAC, IAC Service Provider Section, Non-Compliance Report, Participants Report or IAC Cancellation Request) against the relevant IAP XML Schema. Where this XML Schema validation fails, the B2B interface server shall form a rejection response in accordance with H.4.3.4.

H.4.3.4 For the set of *reliable* Web Service operations the B2B interface shall form a rejection response according to the following:

a) the 'code' element shall be set to:

i) DOCUMENT_UNKNOWN – where the document to which the Web Service request refers cannot be found (e.g. the IAC referred to by an IAC *Service Provider Section*);

ii) DOCUMENT_INVALID – where the document within the Web Service request has failed validation against the relevant XML Schema;

iii) REQUEST_INCONSISTENT – where the document to which the Web Service request refers is in an inconsistent state for the request to be processed (e.g. is not in 'Interim Approved' state upon receipt of an IAC *Service Provider Section*); or

iv) REQUEST_DENIED – where the Web Service request is valid, but business processing has denied the request;

b) the 'message' element shall contain a human readable message elaborating on the rejection; and

c) zero or more 'comment' elements shall be added as appropriate (e.g. to enumerate XML Schema validation errors).

H.4.4 Jurisdiction Service

H.4.4.1 The Jurisdiction B2B interface server shall implement the Jurisdiction Web Service, incorporating the following operations:

a) submitServiceProviderIac (*refer H.4.4.2*);

b) replaceServiceProviderIac (*refer H.4.4.3*);

c) submitPr (*refer H.4.4.4*);

d) submitNcr (*refer H.4.4.5*);

e) submitIacCancellationRequest (*refer H.4.4.6*); and

f) ping (refer *H.4.4.7*).

H.4.4.2 Operation submitServiceProviderIac()

a) This operation is invoked by an IAP-SP to submit an IAC Service Provider Section to the IAC-issuing Jurisdiction;

b) Upon receipt of an IAC Service Provider Section (Part 3), the IAC-issuing Jurisdiction shall reconcile it against the IAC to which it refers; this processing may be performed online or offline, depending upon the capabilities of the IAC-issuing Jurisdiction. In the event that this reconciliation processing fails:

i) where online processing is being applied, a rejection Web Service response shall be formed and returned; and

ii) where offline processing is being applied, the Web Service request shall be rejected (after the event) by a callback to the IAP-SP Web Service operation *notifyRejection*; and

c) In the event that the IAC Service Provider Section (Part 3) is accepted, then BOTH of the following shall occur:

i) the IAC Service Provider Section (Part 3) shall be attached to the IAC, and the IAC state shall be changed to 'Approved' or 'Denied' (as appropriate); and

ii) the complete IAC shall be delivered to the IAP-SP by a callback to the IAP-SP Web Service operation *notifyIac*.

H.4.4.3 Operation replaceServiceProviderIac()

a) This operation is invoked by an IAP-SP to submit a replacement IAC Service Provider Section (Part 3) to the IAC-issuing Jurisdiction for an already-approved IAC;

b) Upon receipt of an IAC Service Provider Section (Part 3), the IAC-issuing Jurisdiction shall reconcile it against the IAC to which it refers; this processing may be performed online or offline, depending upon the capabilities of the IAC-issuing Jurisdiction. In the event that this reconciliation processing fails:

i) where online processing is being applied, a rejection Web Service response shall be formed and returned; and

ii) where offline processing is being applied, the Web Service request shall be rejected (after the event) by a callback to the IAP-SP Web Service operation *notifyRejection*; and

c) In the event that the IAC Service Provider Section is accepted, then BOTH of the following shall occur:

i) the already-approved IAC shall be cancelled. This requires that the complete IAC is delivered to the IAP-SP (i.e. in its cancelled state) by a callback to the IAP-SP Web Service operation *notifyIac*; and

ii) a new, pre-approved IAC Service Provider Section shall be created and shall contain the new IAC Service Provider Section (Part 3). The newly-approved, replacement IAC shall be delivered to the IAP-SP (i.e. in its approved state) by a callback to the IAP-SP Web Service operation *notifyIac*.

H.4.4.4 Operation submitPr()

a) This operation is invoked by an IAP-SP to submit a Participants Report to the IAC-issuing Jurisdiction; and

b) In the event that a Participants Report submitted successfully via this operation is rejected by offline processing within the IAC-issuing Jurisdiction, the IAC-issuing Jurisdiction shall resolve this issue outside the scope of the B2B interface.

H.4.4.5 Operation submitNcr()

a) This operation is invoked by an IAP-SP to submit a Non-Compliance Report to the IAC-issuing Jurisdiction; and

b) In the event that a Non-Compliance Report submitted successfully via this operation is rejected by offline processing within the IAC-issuing Jurisdiction, the IAC-issuing Jurisdiction shall resolve this issue outside the scope of the B2B interface.

H.4.4.6 Operation submitIacCancellationRequest()

a) This operation is invoked by an IAP-SP to submit an IAC Cancellation Request to the IAC-issuing Jurisdiction; and

b) In the event that an IAC Cancellation Request submitted successfully via this operation is rejected by offline processing within the IAC-issuing Jurisdiction, the IAC-issuing Jurisdiction shall resolve this issue outside the scope of the B2B interface.

H.4.4.7 Operation ping(). This is a purely synchronous operation and has no off-line processing requirement.

H.4.5 Service Provider Service

H.4.5.1 The Service Provider B2B interface server shall implement the Service Provider Web Service, incorporating the following operations:

a) notifyIac (refer H.4.5.2);

b) notifyRejection (refer H.4.5.3); and

c) ping (refer H.4.5.4).

H.4.5.2 Operation notifyIac()

a) This operation is invoked by an IAC-issuing Jurisdiction to notify an IAP-SP of a change- of-state for an IAC; and

b) In the event that an IAC submitted successfully via this operation is rejected by offline processing within the IAP-SP (e.g. inconsistent conditions), the IAP-SP shall resolve this issue outside the scope of the B2B interface.

H.4.5.3 Operation notifyRejection()

a) This operation is invoked by an IAC-issuing Jurisdiction to notify an IAP-SP that a previously accepted Web Service request has subsequently been rejected by offline processing; generally this operation will be used to notify rejection of an IAC Service Provider Section (Part 3).

H.4.5.4 Operation ping(). This is a purely synchronous operation and has no off-line processing requirement.

H.4.6 Logging

H.4.6.1 All messages, including those messages that contain a fault, shall be logged by recording the following details:

a) unique primary key (synthetic);

b) message disposition:

i) inbound request;

ii) outbound response;

iii) inbound response; and

iv) outbound request;

c) message action:

i) SOAP action or port and operation;

d) date and time of logging;

e) trading partner:

i) ABN; and

f) document information:

i) unique document identifier; and

ii) request id.

H.4.6.2 Logs represent raw data that may be required to support legal action or to build cases, in particular because of it being digitally signed. As such:

a) all logs should be supported by hardware that can tolerate at least one failure (e.g. highly available disk).

H.4.7 Non-Functional Requirements

H.4.7.1 The specification makes no quantitative requirement in relation to availability, scalability and performance. It is the responsibility of the integrator to satisfy themselves to the degree they believe necessary that their solution is adequate with respect to expected traffic loads.

H.4.7.2 For small server environments (smaller IAP-SPs and small Jurisdictions) a minimal solution would involve only a single server.

H.4.7.3 For larger environments it may be necessary to support HTTP load balancing across multiple machines to provide scalability and ensure higher availability.

H.4.8 Resource Discovery and Identity Management

H.4.8.1 The TCA web site shall provide up to date information for each IAC-issuing Jurisdiction and IAP-SP, including name, ABN, URL and supported version of the interface.

H.4.9 B2B Time Formats

H.4.9.1 Within the XML documents defined by the IAP XML Schemas, all elements and attributes of type date, time and dateTime shall be relative to an implicit time zone as shown in Table H-1.

Document	Field	Time Zone
offTheShelfConditions (Off-the-Shelf Conditions)	issuedDateTime conditionPeriod/fromDateTime conditionPeriod/toDateTime conditionInterval/fromTime conditionInterval/toTime validFromDateTime validToDateTime	Jurisdiction
iac (IAC) note: see also serviceProviderIac	issuedDateTime (all except Part 3) lapseDateTime commencementDateTime cessationDateTime	Jurisdiction
serviceProviderIac (IAC "Part 3")	issuedDateTime installationDateTime	IAP-SP
iacCancellationRequest (IAC Cancellation Request)	issuedDateTime	IAP-SP
nonComplianceReport	issuedDateTime	IAP-SP
(Non-Compliance Report)	ivuDateTime ivuNcaPeriod/fromDateTime ivuNcaPeriod/toDateTime	UTC
	jurisdictionDateTime jurisdictionNcaPeriod/fromDateTime jurisdictionNcaPeriod/toDateTime auditReferenceDateTime	Jurisdiction
participantsReport (Participants Report)	issuedDateTime	IAP-SP
	iapEntryDateTime iapExitDateTime reportPeriod/fromDateTime reportPeriod/toDateTime	Jurisdiction

Table H - 1. Non-exhaustive list of B2B Time formats

Note: The XML documents defined by the IAP XML Schemas are offTheShelfConditions (an Off-the-Shelf Conditions revision), iac (an IAC), serviceProviderIac (an IAP "Part 3"), iacCancellationRequest (an IAC Cancellation Request), nonComplianceReport (an NCR) and participantsReport (a PR).

H.4.9.2 Noting the provisions of 1 (above), within the XML documents defined by the IAP XML Schemas, all elements and attributes of type date, time and dateTime shall be encoded without any time zone offset field (e.g. 2005-12-03T11:54:00 rather than 2005-12-03T11:54:00+10:00, and 01:02:03 rather than 01:02:03+11:00).

H.4.9.3 Within the IAP Web Services headers, all elements and attributes of type date, time and dateTime shall be relative to the time zone of the IAP participant that populates the element or attribute in the event that the time zone offset field is not encoded.

Note: The relevant IAP Web Services header fields are requestDateTime and receiptDateTime, and these may be encoded with or without a time zone offset.

H.4.10 XML Data Compression

H.4.10.1 The IAP-SP may implement XML data compression for the Jurisdiction Web Service client and Service Provider Web Service server in accordance with H.4.10.2 through H.4.10.5.

Note: IAC-issuing Jurisdictions shall implement XML data compression for the Service Provider Web Service client and Jurisdiction Web Service server in accordance with H.4.10.2 through H.4.10.5. The IAP Participant Details Including B2B Configuration Parameters document shall be used to inform IAC-issuing Jurisdictions on whether to transmit compressed or uncompressed XML with each IAP-SP.

H.4.10.2 XML data compression shall apply to the following Jurisdiction Web Service operations:

a) *submitNcr* – the NCR document as defined by the XML Schema element *nonComplianceReport* shall be transmitted uncompressed using the element *nonComplianceReport*, or compressed using the element *compressedNonComplianceReport {http://www.tca.gov.au/schemas/iap/ncr/2007-02}*;

b) *submitPr* – the PR document as defined by the XML Schema element *participantsReport* shall be transmitted uncompressed using the element *participantsReport*, or compressed using the element *compressedparticipantsReport {http://www.tca.gov.au/schemas/iap/pr/2007-02}*;

c) *submitServiceProviderIac* – the IAC Service Provider Section (Part 3) document as defined by the XML Schema element *serviceProviderIac* shall be transmitted uncompressed using the element *serviceProviderIac*, or compressed using the element *compressedServiceProviderIac {http://www.tca.gov.au/schemas/iap/iac/2007-02}*;

d) *replaceServiceProviderIac* – the IAC Service Provider Section (Part 3) document as defined by the XML Schema element *serviceProviderIac* shall be transmitted uncompressed using the element *serviceProviderIac*, or compressed using the element *compressedServiceProviderIac {http://www.tca.gov.au/schemas/iap/iac/2007-02}*;

e) *submitIacCancellationRequest* – the IAC Cancellation Request document as defined by the XML Schema-defined element *iacCancellationRequest* shall be transmitted uncompressed using the element *iacCancellationRequest*, or compressed using the element *compressedIacCancellationRequest {http://www.tca.gov.au/schemas/iap/iac/2007-02}*.

H.4.10.3 XML data compression shall apply to the following Service Provider Web Service operation:

a) *notifyIac* – the IAC document as defined by the XML Schema element *iac* shall be transmitted uncompressed using the element *iac*, or compressed using the element *compressedIac {http://www.tca.gov.au/schemas/iap/iac/2007-02}*.

H.4.10.4 When invoking any Web Service operation listed in H.4.10.2 or H.4.10.3, a Web Service client that implements XML data compression shall:

a) isolate a standalone XML document that is valid with respect to the relevant XML Schema element;

b) compress that XML document into a byte stream using the GZIP compression algorithm (as defined in RFC 1952[6]);

c) encode that compressed byte stream using the BASE 64 algorithm (as defined in RFC 4648[6]); and

d) transmit that BASE 64 encoded byte stream within the relevant compressed Web Service request element.

Note: As an example, applying XML data compression to the notifyIac operation would require isolation of a standalone IAC document that is valid with respect to the XML Schema element iac. After being GZIP compressed and BASE 64 encoded, this document would be transmitted using the Web Service request element compressedIac, and the Web Service request element iac would not be populated {http://www.tca.gov.au/schemas/iap/iac/2007-02}.

XML data compression is performed prior to application of an XML digital signature (i.e. it is the compressed XML data that is digitally signed). Some Web Services toolkits will automatically BASE 64 encode the GZIP compressed data.

H.4.10.5 When hosting a Web Service operation listed in H.4.10.2 or H.4.10.3, a Web Service server that implements XML data compression shall determine whether XML data compression has been applied by the Web Service client by identifying whether the operations uncompressed Web Service request element or compressed Web Service request element has been populated. Where XML compression has been applied, the Web Service server shall:

a) recover the original standalone XML document by removing the BASE 64 encoding and GZIP compression applied by the Web Service client (as per H.4.10.4); and

b) process that standalone XML document as though it had been transmitted in uncompressed form.

Note: XML data decompression is performed after removal of the XML digital signature. Some Web Services toolkits will automatically BASE 64 decode the GZIP compressed data.

[6] Request For Comment (RFC 1952, 4648) repository maintained by the Internet Engineering Taskforce (IETF) Secretariat http://www.ietf.org/rfc.html (viewed on 30 January 2009).

H.5 XML Schemas Reference

H.5.1 XML Schema and Web Service Diagrams

H.5.1.1 This section contains UML class diagrams that reflect the structure and content of the IAP XML Schemas. However, it should be noted that these diagrams are considered illustrative, and are only provided as an aid to understanding the XML Schemas; these diagrams are not an exact reproduction of the XML Schemas and should not be used as the basis for design or development work.

H.5.2 XML Schema and Web Service Definitions

H.5.2.1 The B2B interface XML Schema definitions and Web Service definitions are defined in Annexes A and B of this Appendix, and for convenience in the following files attached to this specification:

a) iap_common_2006-09.xsd – defines common data types;

b) iap_conditions_2006-09.xsd – defines the data types for off-the-shelf and unique conditions;

c) iap_iac_2006-09.xsd – defines the data types for IACs;

d) iap_ncr_2006-09.xsd – defines the data types for NCRs;

e) iap_pr_2006-09.xsd – defines the data types for PRs;

f) iap_ws_2006-09.xsd – defines common types required to support the Jurisdiction and IAP-SP Web Service definitions;

g) iap_jurisdiction_2006-09.wsdl – defines the Jurisdiction Web Services interface;

h) iap_sp_2006-09.wsdl – defines the IAP-SP Web Services interface.

H.5.2.2 The XML Schema definitions and Web Service definitions are versioned using XML namespaces: a new namespace will be assigned to these definitions in the case that they are modified in any subsequent versions of this specification.

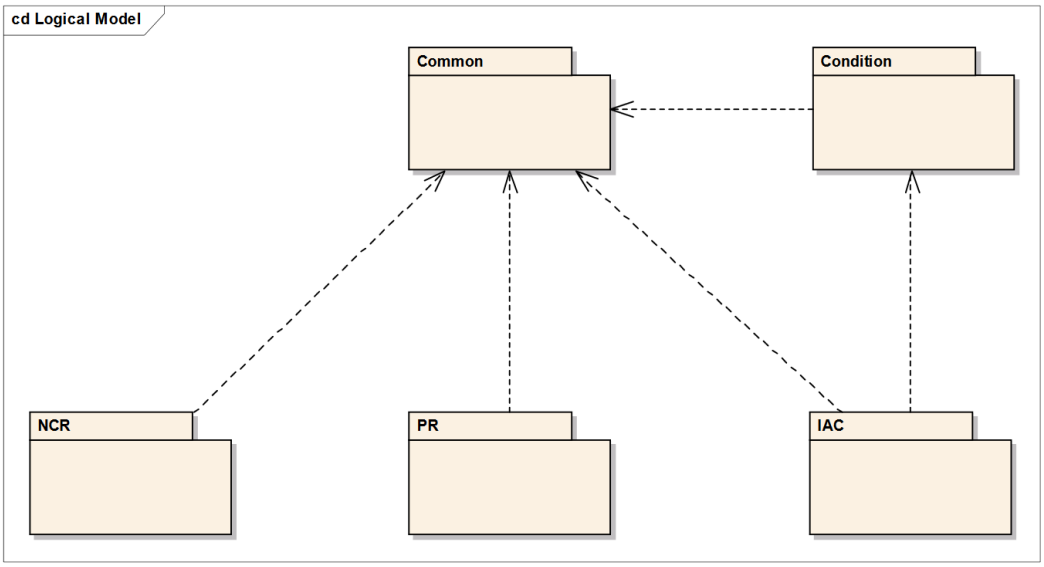


Figure H - 10. IAP Packages Logical Model

H.5.3 Common

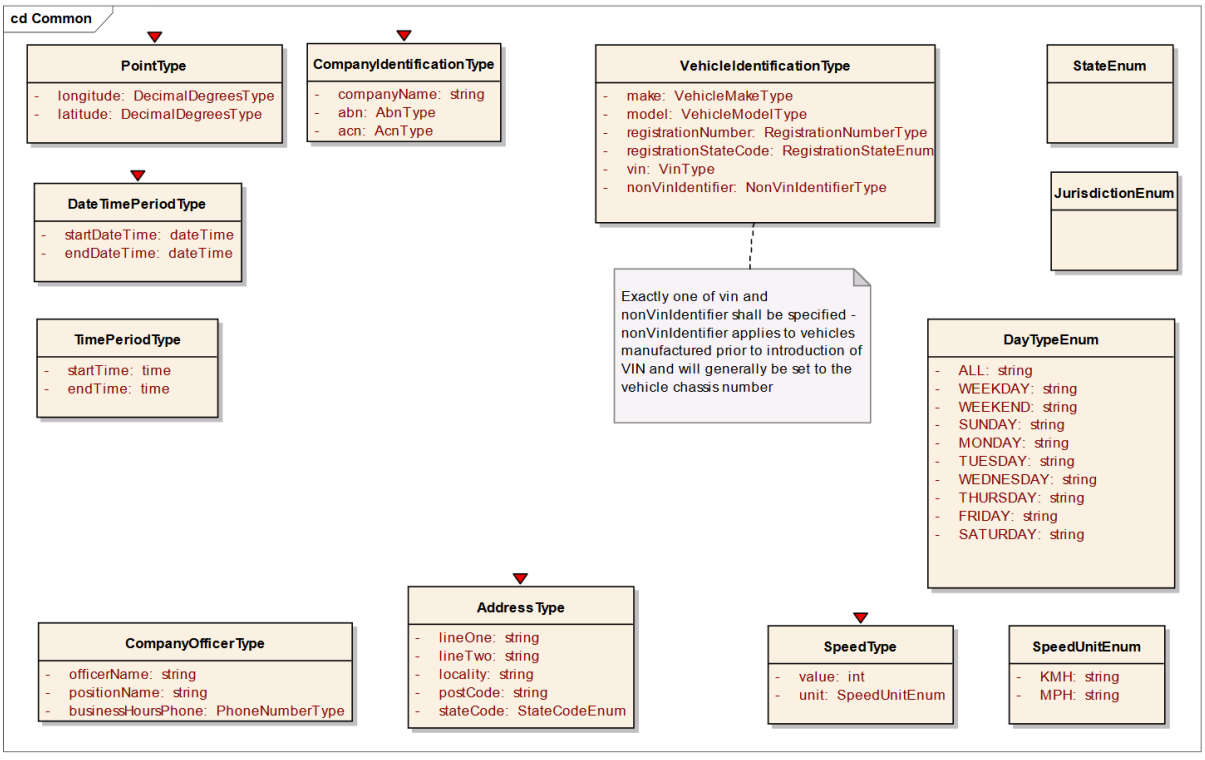


Figure H - 11. Common Schema Logical Model

H.5.4 Conditions

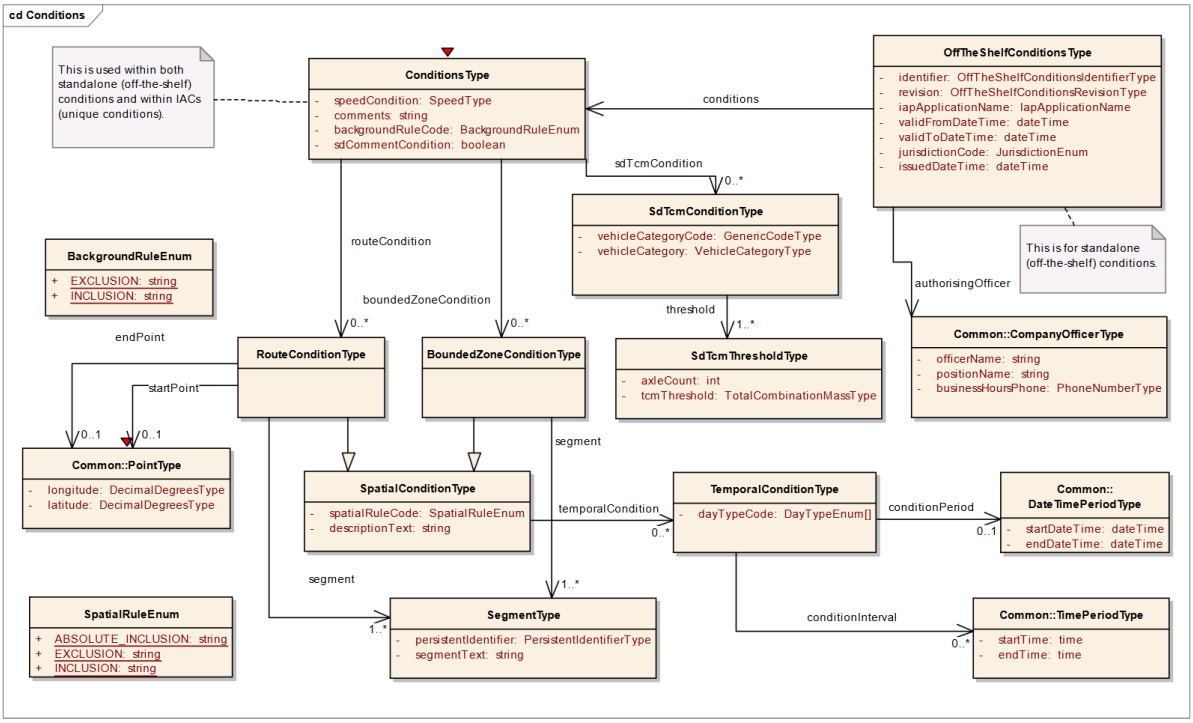
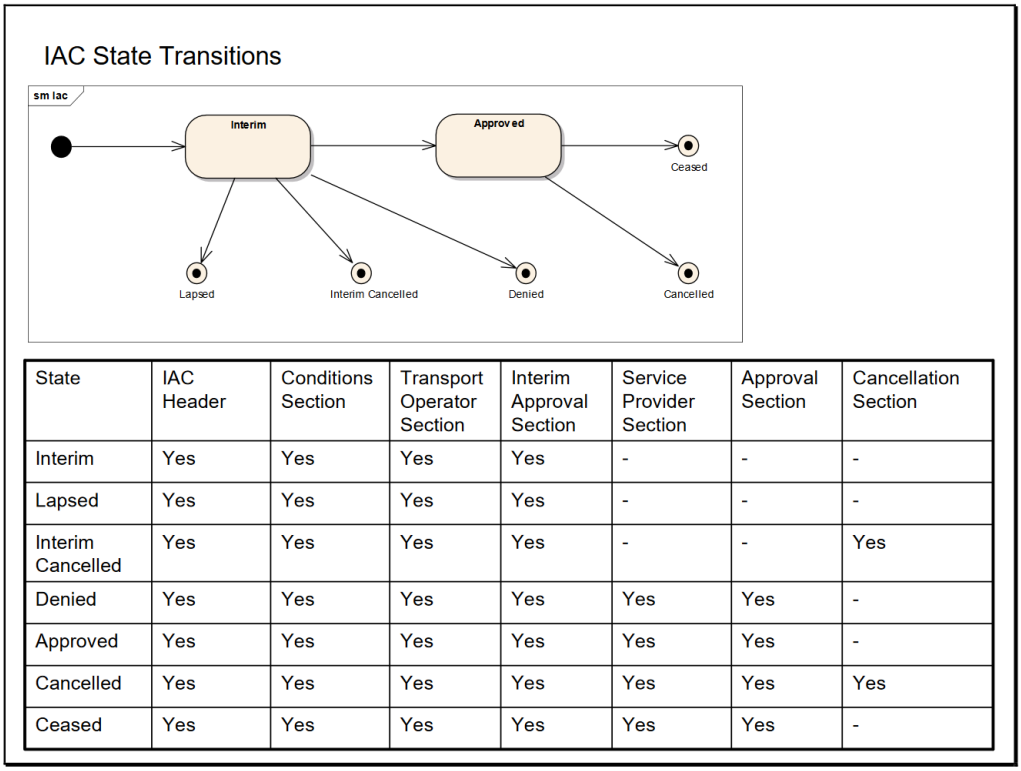


Figure H - 12. Conditions Schema Logical Model

H.5.4.1 Within the XML representation of IAP Conditions, times should be specified WITHOUT any time zone offset (e.g. 2005-12-03T11:54:00 rather than 2005-12-03T11:54:00+10:00). This is because times within IAP Conditions are relative to the issuing Jurisdiction, and cannot be ascribed an offset because they are not accompanied by a date (i.e. they may apply to either or both of the Jurisdiction's standard and daylight savings time zones).

H.5.5 IAC



State	IAC Header	Conditions Section	Transport Operator Section	Interim Approval Section	Service Provider Section	Approval Section	Cancellation Section
Interim	Yes	Yes	Yes	Yes	-	-	-
Lapsed	Yes	Yes	Yes	Yes	-	-	-
Interim Cancelled	Yes	Yes	Yes	Yes	-	-	Yes
Denied	Yes	Yes	Yes	Yes	Yes	Yes	-
Approved	Yes	Yes	Yes	Yes	Yes	Yes	-
Cancelled	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ceased	Yes	Yes	Yes	Yes	Yes	Yes	-

Figure H - 13. IAC State Transition Model

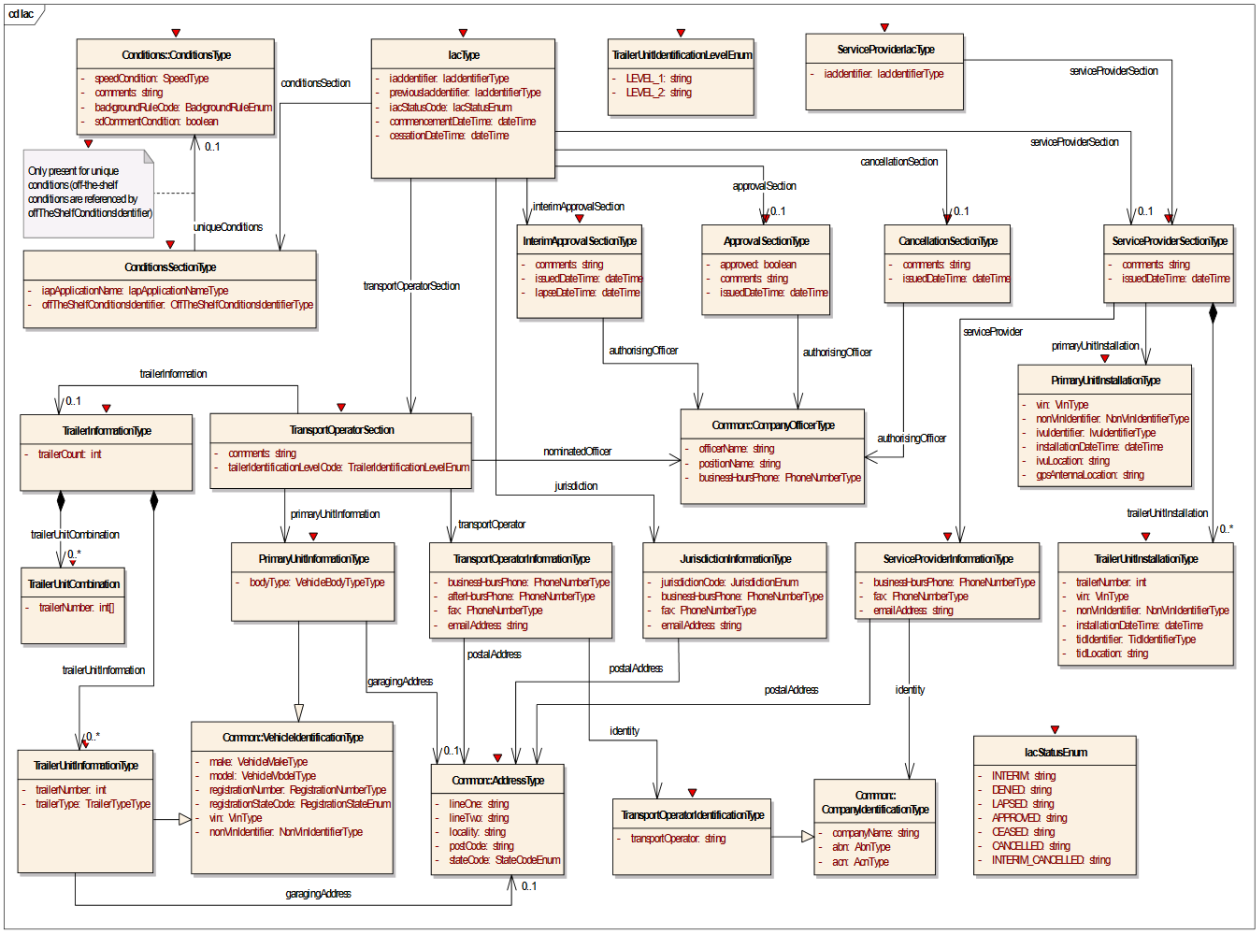


Figure H - 14. IAC Schema Logical Model

H.5.6 NCR

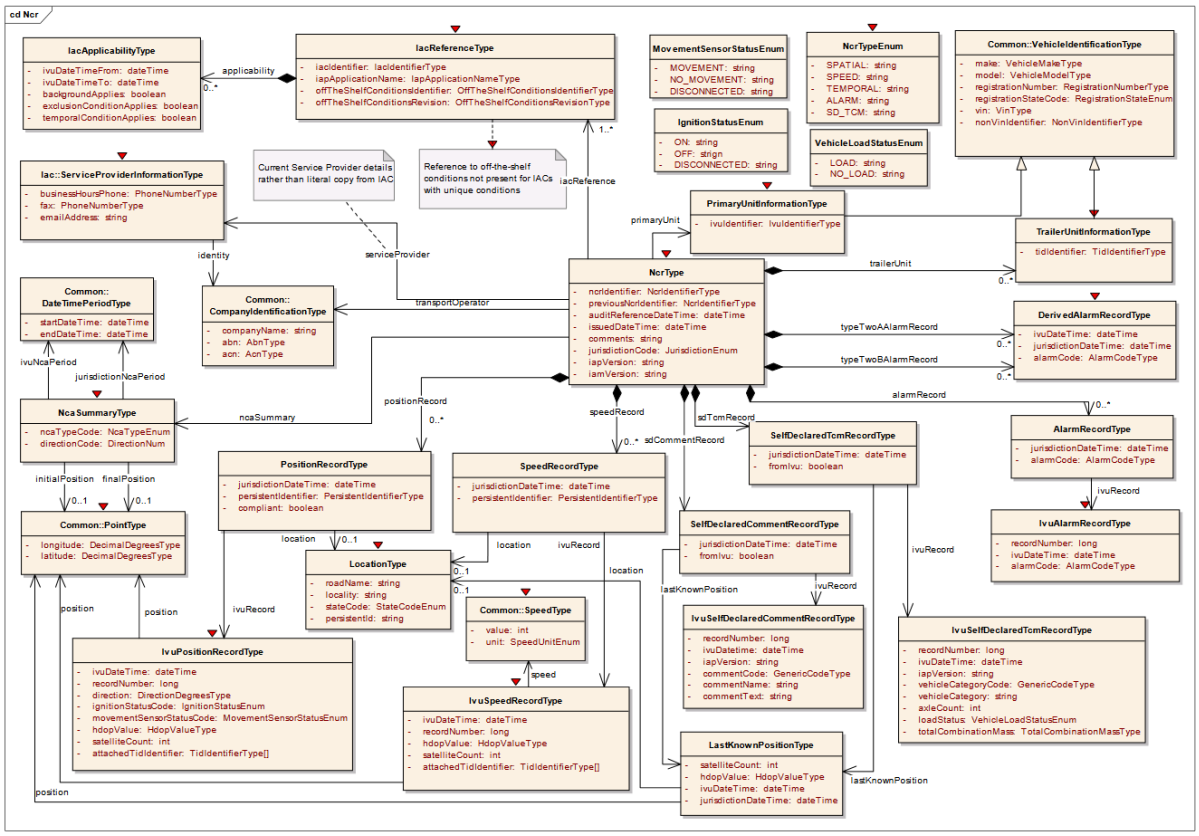


Figure H - 15. NCR Schema Logical Model

H.5.7 PR

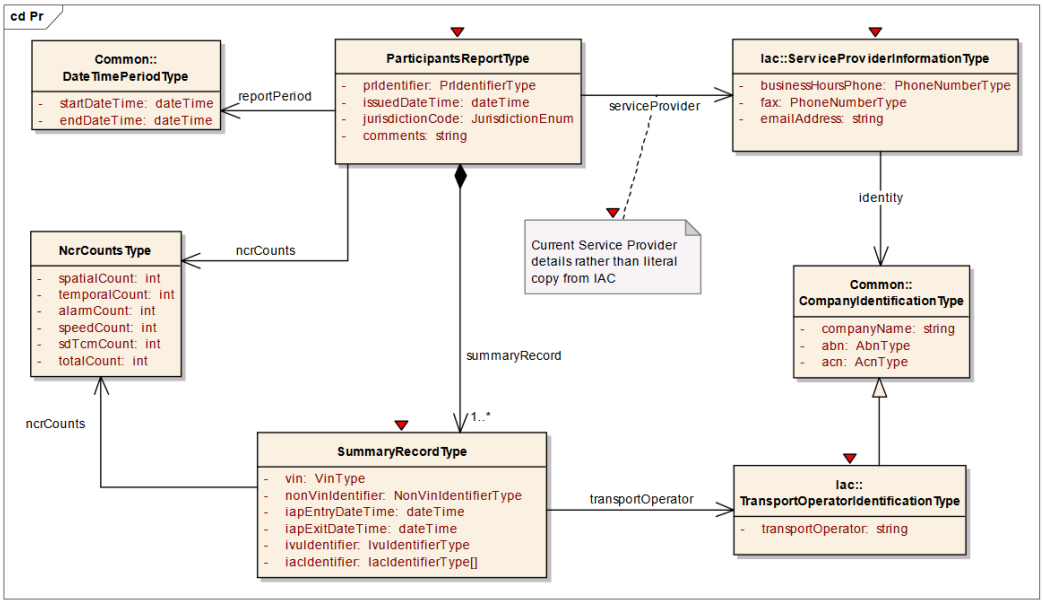


Figure H - 16. PR Logical Model

Annex A – WSDL

Web Service Support Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
   targetNamespace="http://www.tca.gov.au/schemas/iap/iapws/2007-02"
   xmlns:tns="http://www.tca.gov.au/schemas/iap/iapws/2007-02"
   xmlns:common="http://www.tca.gov.au/schemas/iap/common/2007-02"
   elementFormDefault="unqualified" version="2007-02" >


   <xs:annotation>
      <xs:appinfo>
         <xs:documentation>
            <name>iap_ws_2007-02.xsd</name>
            <version>2007-02</version>
            <description>Intelligent Access Program - WebService
               definition</description>
         </xs:documentation>
      </xs:appinfo>
   </xs:annotation>


   <xs:import namespace="http://www.tca.gov.au/schemas/iap/common/2007-02"
      schemaLocation="iap_common_2007-02.xsd"/>
   <xs:import namespace="http://www.tca.gov.au/schemas/iap/conditions/2007-02"
      schemaLocation="iap_conditions_2007-02.xsd"/>
   <xs:import namespace="http://www.tca.gov.au/schemas/iap/iac/2007-02"
      schemaLocation="iap_iac_2007-02.xsd"/>
   <xs:import namespace="http://www.tca.gov.au/schemas/iap/ncr/2007-02"
      schemaLocation="iap_ncr_2007-02.xsd"/>
   <xs:import namespace="http://www.tca.gov.au/schemas/iap/pr/2007-02"
      schemaLocation="iap_pr_2007-02.xsd"/>


   <xs:complexType name="AddressingHeaderType">
      <xs:sequence>
         <xs:element name="from" type="common:CompanyIdentificationType"/>
         <xs:element name="to" type="common:CompanyIdentificationType"/>
      </xs:sequence>
   </xs:complexType>


   <xs:complexType name="TransmittalHeaderType">
      <xs:sequence>
         <xs:element name="documentIdentifier" type="xs:string" />
         <xs:element name="requestIdentifier" type="xs:string"/>
         <xs:element name="requestDateTime" type="xs:dateTime"/>
      </xs:sequence>
   </xs:complexType>


   <xs:simpleType name="FaultCodeEnum">
      <xs:restriction base="xs:string">
         <xs:enumeration value="UNAVAILABLE" />
         <xs:enumeration value="SENDER_UNKNOWN" />
         <xs:enumeration value="SENDER_INVALID" />
         <xs:enumeration value="SENDER_MISMATCH" />
         <xs:enumeration value="RECEIVER_UNKNOWN" />
      </xs:restriction>
   </xs:simpleType>
```

```
<xs:simpleType name="RejectionCodeEnum">
   <xs:restriction base="xs:string">
      <xs:enumeration value="DOCUMENT_UNKNOWN" />
      <xs:enumeration value="DOCUMENT_INVALID" />
      <xs:enumeration value="REQUEST_INCONSISTENT" />
      <xs:enumeration value="REQUEST_DENIED" />
   </xs:restriction>
</xs:simpleType>


<xs:complexType name="AcceptanceType" >
   <xs:sequence>
      <xs:element name="receiptDateTime" type="xs:dateTime"/>
      <xs:element name="duplicateDetected" type="xs:boolean" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="RejectionType" >
   <xs:sequence>
      <xs:element name="code" type="xs:string" />
      <xs:element name="message" type="xs:string" />
      <xs:element name="comment" type="xs:string" minOccurs="0"
         maxOccurs="unbounded"/>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="AbstractRequestType" >
   <xs:sequence>
      <xs:element name="addressing" type="tns:AddressingHeaderType"/>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="AbstractTransmittalRequestType" >
   <xs:complexContent>
      <xs:extension base="tns:AbstractRequestType">
         <xs:sequence>
            <xs:element name="transmittal" type="tns:TransmittalHeaderType"/>
         </xs:sequence>
      </xs:extension>
   </xs:complexContent>
</xs:complexType>


<xs:complexType name="TransmittalResponseType">
   <xs:sequence>
      <xs:choice>
         <xs:element name="acceptance" type="tns:AcceptanceType" />
         <xs:element name="rejection" type="tns:RejectionType" />
      </xs:choice>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="RejectionRequestType">
   <xs:complexContent>
      <xs:extension base="tns:AbstractTransmittalRequestType" >
         <xs:sequence>
            <xs:element name="rejection" type="tns:RejectionType" />
         </xs:sequence>
      </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

```
    <xs:complexType name="RejectionResponseType" />


    <xs:complexType name="PingRequestType" >
       <xs:complexContent>
          <xs:extension base="tns:AbstractRequestType" />
       </xs:complexContent>
    </xs:complexType>


    <xs:complexType name="PingResponseType">
       <xs:sequence>
          <xs:element name="available" type="xs:boolean" />
       </xs:sequence>
    </xs:complexType>


</xs:schema>
```

Jurisdiction Web Service

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
   xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns:tns="http://www.tca.gov.au/schemas/iap/jurisdiction/2007-02"
   xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
   xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
   xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
   xmlns:iapws="http://www.tca.gov.au/schemas/iap/iapws/2007-02"
   xmlns:ns="http://www.tca.gov.au/schemas/iap/common/2007-02"
   targetNamespace="http://www.tca.gov.au/schemas/iap/jurisdiction/2007-02"
   name="JurisdictionWebService">


   <wsdl:types>
      <xs:schema elementFormDefault="unqualified"
         targetNamespace="http://www.tca.gov.au/schemas/iap/jurisdiction/2007-02"
         version="2007-02"
         xmlns:tns="http://www.tca.gov.au/schemas/iap/jurisdiction/2007-02"
         xmlns:common="http://www.tca.gov.au/schemas/iap/common/2007-02"
         xmlns:iapws="http://www.tca.gov.au/schemas/iap/iapws/2007-02"
         xmlns:pr="http://www.tca.gov.au/schemas/iap/pr/2007-02"
         xmlns:iac="http://www.tca.gov.au/schemas/iap/iac/2007-02"
         xmlns:iapcond="http://www.tca.gov.au/schemas/iap/iapConditions/2007-02"
         xmlns:ncr="http://www.tca.gov.au/schemas/iap/ncr/2007-02"
         xmlns:xs="http://www.w3.org/2001/XMLSchema">



         <xs:import namespace="http://www.tca.gov.au/schemas/iap/common/2007-02"
            schemaLocation="iap_common_2007-02.xsd"/>
         <xs:import namespace="http://www.tca.gov.au/schemas/iap/iapws/2007-02"
            schemaLocation="iap_ws_2007-02.xsd"/>
         <xs:import namespace="http://www.tca.gov.au/schemas/iap/ncr/2007-02"
            schemaLocation="iap_ncr_2007-02.xsd"/>
         <xs:import namespace="http://www.tca.gov.au/schemas/iap/iac/2007-02"
            schemaLocation="iap_iac_2007-02.xsd"/>
         <xs:import namespace="http://www.tca.gov.au/schemas/iap/pr/2007-02"
            schemaLocation="iap_pr_2007-02.xsd"/>
         <xs:import namespace="http://www.tca.gov.au/schemas/iap/conditions/2007-
            02" schemaLocation="iap_conditions_2007-02.xsd"/>

         <xs:complexType name="SubmitNcrType">
           <xs:complexContent>
              <xs:extension base="iapws:AbstractTransmittalRequestType">
                 <xs:choice>
                    <xs:annotation>
                       <xs:documentation>
                          WARNING: The element 'compressedNonComplianceReport' is
                          intended for future use and should not be implemented or
                          used operationally until notified by TCA.
                       </xs:documentation>
                    </xs:annotation>
                    <xs:element name="nonComplianceReport" type="ncr:NcrType" />
                    <xs:element name="compressedNonComplianceReport"
                       type="xs:base64Binary" />
                 </xs:choice>
              </xs:extension>
           </xs:complexContent>
         </xs:complexType>
```

```
<xs:complexType name="SubmitPrType">
   <xs:complexContent>
      <xs:extension base="iapws:AbstractTransmittalRequestType">
         <xs:choice>
            <xs:annotation>
               <xs:documentation>
                  WARNING: The element 'compressedParticipantsReport' is
                  intended for future use and should not be implemented or
                  used operationally until notified by TCA.
               </xs:documentation>
            </xs:annotation>
            <xs:element name="participantsReport"
               type="pr:ParticipantsReportType" />
            <xs:element name="compressedParticipantsReport"
               type="xs:base64Binary" />
         </xs:choice>
      </xs:extension>
   </xs:complexContent>
</xs:complexType>


<xs:complexType name="SubmitServiceProviderIacType">
   <xs:complexContent>
      <xs:extension base="iapws:AbstractTransmittalRequestType">
         <xs:annotation>
            <xs:documentation>
               WARNING: The element 'compressedServiceProviderIac' is intended
               for future use and should not be implemented or used
               operationally until notified by TCA.
            </xs:documentation>
         </xs:annotation>
         <xs:choice>
            <xs:element name="serviceProviderIac"
               type="iac:ServiceProviderIacType" />
            <xs:element name="compressedServiceProviderIac"
               type="xs:base64Binary" />
         </xs:choice>
      </xs:extension>
   </xs:complexContent>
</xs:complexType>


<xs:complexType name="ReplaceServiceProviderIacType">
   <xs:complexContent>
      <xs:extension base="iapws:AbstractTransmittalRequestType">
         <xs:annotation>
            <xs:documentation>
               WARNING: The element 'compressedServiceProviderIac' is
               intended for future use and should not be implemented or used
               operationally until notified by TCA.
            </xs:documentation>
         </xs:annotation>
         <xs:choice>
            <xs:element name="serviceProviderIac"
               type="iac:ServiceProviderIacType" />
            <xs:element name="compressedServiceProviderIac"
               type="xs:base64Binary" />
         </xs:choice>
       </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

```
        <xs:complexType name="SubmitIacCancellationRequestType">
           <xs:complexContent>
              <xs:extension base="iapws:AbstractTransmittalRequestType">
                 <xs:annotation>
                    <xs:documentation>
                       WARNING: The element 'compressedIacCancellationRequest' is
                       intended for future use and should not be implemented or used
                       operationally until notified by TCA.
                    </xs:documentation>
                 </xs:annotation>
                 <xs:choice>
                    <xs:element name="iacCancellationRequest"
                       type="iac:IacCancellationRequestType" />
                    <xs:element name="compressedIacCancellationRequest"
                       type="xs:base64Binary" />
                 </xs:choice>
              </xs:extension>
           </xs:complexContent>
        </xs:complexType>


        <xs:element name="submitNcr" type="tns:SubmitNcrType"/>
        <xs:element name="submitNcrResponse" type="iapws:TransmittalResponseType"/>


        <xs:element name="submitPr" type="tns:SubmitPrType"/>
        <xs:element name="submitPrResponse" type="iapws:TransmittalResponseType"/>

        <xs:element name="submitServiceProviderIac"
           type="tns:SubmitServiceProviderIacType"/>
        <xs:element name="submitServiceProviderIacResponse"
           type="iapws:TransmittalResponseType" />


        <xs:element name="replaceServiceProviderIac"
           type="tns:ReplaceServiceProviderIacType"/>
        <xs:element name="replaceServiceProviderIacResponse"
           type="iapws:TransmittalResponseType" />


        <xs:element name="submitIacCancellationRequest"
           type="tns:SubmitIacCancellationRequestType"/>
        <xs:element name="submitIacCancellationRequestResponse"
           type="iapws:TransmittalResponseType" />


        <xs:element name="ping" type="iapws:PingRequestType"/>
        <xs:element name="pingResponse" type="iapws:PingResponseType" />


     </xs:schema>
  </wsdl:types>


  <wsdl:message name="SubmitNcrRequest">
     <wsdl:part name="request" element="tns:submitNcr"/>
  </wsdl:message>
  <wsdl:message name="SubmitNcrResponse">
     <wsdl:part name="response" element="tns:submitNcrResponse"/>
  </wsdl:message>
```

```
<wsdl:message name="SubmitPrRequest">
   <wsdl:part name="request" element="tns:submitPr"/>
</wsdl:message>
<wsdl:message name="SubmitPrResponse">
   <wsdl:part name="response" element="tns:submitPrResponse"/>
</wsdl:message>


<wsdl:message name="SubmitServiceProviderIacRequest">
   <wsdl:part name="request" element="tns:submitServiceProviderIac"/>
</wsdl:message>
<wsdl:message name="SubmitServiceProviderIacResponse">
   <wsdl:part name="response" element="tns:submitServiceProviderIacResponse"/>
</wsdl:message>


<wsdl:message name="ReplaceServiceProviderIacRequest">
   <wsdl:part name="request" element="tns:replaceServiceProviderIac"/>
</wsdl:message>
<wsdl:message name="ReplaceServiceProviderIacResponse">
   <wsdl:part name="response" element="tns:replaceServiceProviderIacResponse"/>
</wsdl:message>


<wsdl:message name="SubmitIacCancellationRequestRequest">
   <wsdl:part name="request" element="tns:submitIacCancellationRequest"/>
</wsdl:message>
<wsdl:message name="SubmitIacCancellationRequestResponse">
   <wsdl:part name="response" element="tns:submitIacCancellationRequestResponse"/>
</wsdl:message>


<wsdl:message name="PingRequest">
   <wsdl:part name="request" element="tns:ping"/>
</wsdl:message>
<wsdl:message name="PingResponse">
   <wsdl:part name="response" element="tns:pingResponse"/>
</wsdl:message>


<wsdl:portType name="JurisdictionPortType">
   <wsdl:operation name="submitNcr">
      <wsdl:input message="tns:SubmitNcrRequest"/>
      <wsdl:output message="tns:SubmitNcrResponse"/>
   </wsdl:operation>
   <wsdl:operation name="submitPr">
      <wsdl:input message="tns:SubmitPrRequest"/>
      <wsdl:output message="tns:SubmitPrResponse"/>
   </wsdl:operation>
   <wsdl:operation name="submitServiceProviderIac">
      <wsdl:input message="tns:SubmitServiceProviderIacRequest"/>
      <wsdl:output message="tns:SubmitServiceProviderIacResponse"/>
   </wsdl:operation>
   <wsdl:operation name="replaceServiceProviderIac">
      <wsdl:input message="tns:ReplaceServiceProviderIacRequest"/>
      <wsdl:output message="tns:ReplaceServiceProviderIacResponse"/>
   </wsdl:operation>
   <wsdl:operation name="submitIacCancellationRequest">
      <wsdl:input message="tns:SubmitIacCancellationRequestRequest"/>
      <wsdl:output message="tns:SubmitIacCancellationRequestResponse"/>
   </wsdl:operation>
   <wsdl:operation name="ping">
      <wsdl:input message="tns:PingRequest"/>
      <wsdl:output message="tns:PingResponse"/>
   </wsdl:operation>
</wsdl:portType>
```

```
    <wsdl:binding name="JurisdictionBinding" type="tns:JurisdictionPortType">
       <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
       <wsdl:operation name="submitNcr">
          <soap:operation soapAction="submitNcr" style="document"/>
          <wsdl:input>
             <soap:body use="literal"/>
          </wsdl:input>
          <wsdl:output>
             <soap:body use="literal"/>
          </wsdl:output>
       </wsdl:operation>
       <wsdl:operation name="submitPr">
          <soap:operation soapAction="submitPr" style="document"/>
          <wsdl:input>
             <soap:body use="literal"/>
          </wsdl:input>
          <wsdl:output>
             <soap:body use="literal"/>
          </wsdl:output>
       </wsdl:operation>
       <wsdl:operation name="submitServiceProviderIac">
          <soap:operation soapAction="submitServiceProviderIac" style="document"/>
          <wsdl:input>
             <soap:body use="literal"/>
          </wsdl:input>
          <wsdl:output>
             <soap:body use="literal"/>
          </wsdl:output>
       </wsdl:operation>
       <wsdl:operation name="replaceServiceProviderIac">
          <soap:operation soapAction="replaceServiceProviderIac" style="document"/>
          <wsdl:input>
             <soap:body use="literal"/>
          </wsdl:input>
          <wsdl:output>
             <soap:body use="literal"/>
          </wsdl:output>
       </wsdl:operation>
       <wsdl:operation name="submitIacCancellationRequest">
          <soap:operation soapAction="submitIacCancellationRequest" style="document"/>
          <wsdl:input>
             <soap:body use="literal"/>
          </wsdl:input>
          <wsdl:output>
             <soap:body use="literal"/>
          </wsdl:output>
       </wsdl:operation>
       <wsdl:operation name="ping">
          <soap:operation soapAction="ping" style="document"/>
          <wsdl:input>
             <soap:body use="literal"/>
          </wsdl:input>
          <wsdl:output>
             <soap:body use="literal"/>
          </wsdl:output>
       </wsdl:operation>
    </wsdl:binding>

    <wsdl:service name="Jurisdiction">
       <wsdl:port name="JurisdictionPort" binding="tns:JurisdictionBinding">
          <soap:address location="https://tca.gov.au/iap/services/Jurisdiction" />
       </wsdl:port>
    </wsdl:service>

 </wsdl:definitions>
```

IAP-SP Web Service

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
   xmlns:tns="http://www.tca.gov.au/schemas/iap/provider/2007-02"
   xmlns:iapws="http://www.tca.gov.au/schemas/iap/iapws/2007-02"
   xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
   xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
   xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns:common="http://www.tca.gov.au/schemas/iap/common/2007-02"
   xmlns:cond="http://www.tca.gov.au/schemas/iap/conditions/2007-02"
   xmlns:iac="http://www.tca.gov.au/schemas/iap/iac/2007-02"
   xmlns:ncr="http://www.tca.gov.au/schemas/iap/ncr/2007-02"
   xmlns:pr="http://www.tca.gov.au/schemas/iap/pr/2007-02"
   targetNamespace="http://www.tca.gov.au/schemas/iap/provider/2007-
   02" name="ServiceProviderWebService">



   <wsdl:types>
      <xs:schema elementFormDefault="unqualified"
         xmlns:tns="http://www.tca.gov.au/schemas/iap/provider/2007-02"
         targetNamespace="http://www.tca.gov.au/schemas/iap/provider/2007-02"
         version="2007-02" xmlns:xs="http://www.w3.org/2001/XMLSchema">


         <xs:import namespace="http://www.tca.gov.au/schemas/iap/common/2007-02"
            schemaLocation="iap_common_2007-02.xsd"/>
         <xs:import namespace="http://www.tca.gov.au/schemas/iap/iapws/2007-02"
            schemaLocation="iap_ws_2007-02.xsd"/>
         <xs:import namespace="http://www.tca.gov.au/schemas/iap/ncr/2007-02"
            schemaLocation="iap_ncr_2007-02.xsd"/>
         <xs:import namespace="http://www.tca.gov.au/schemas/iap/iac/2007-02"
            schemaLocation="iap_iac_2007-02.xsd"/>
         <xs:import namespace="http://www.tca.gov.au/schemas/iap/pr/2007-02"
            schemaLocation="iap_pr_2007-02.xsd"/>


         <xs:complexType name="NotifyIacType">
            <xs:complexContent>
               <xs:extension base="iapws:AbstractTransmittalRequestType">
                  <xs:annotation>
                     <xs:documentation>
                        WARNING: The element 'compressedIac' is intended for
                        future use and should not be implemented or used
                        operationally until notified by TCA.
                     </xs:documentation>
                  </xs:annotation>
                  <xs:choice>
                     <xs:element name="iac" type="iac:IacType" />
                     <xs:element name="compressedIac" type="xs:base64Binary" />
                  </xs:choice>
               </xs:extension>
            </xs:complexContent>
         </xs:complexType>


         <xs:element name="notifyIac" type="tns:NotifyIacType"/>
         <xs:element name="notifyIacResponse" type="iapws:TransmittalResponseType"/>

         <xs:element name="notifyRejection" type="iapws:RejectionRequestType"/>
```

```
      <xs:element name="notifyRejectionResponse"
         type="iapws:RejectionResponseType"/>


      <xs:element name="ping" type="iapws:PingRequestType"/>
      <xs:element name="pingResponse" type="iapws:PingResponseType" />


   </xs:schema>
</wsdl:types>



<wsdl:message name="NotifyIacRequest">
   <wsdl:part name="request" element="tns:notifyIac"/>
</wsdl:message>
<wsdl:message name="NotifyIacResponse">
   <wsdl:part name="response" element="tns:notifyIacResponse"/>
</wsdl:message>


<wsdl:message name="NotifyRejectionRequest">
   <wsdl:part name="request" element="tns:notifyRejection"/>
</wsdl:message>
<wsdl:message name="NotifyRejectionResponse">
   <wsdl:part name="response" element="tns:notifyRejectionResponse"/>
</wsdl:message>


<wsdl:message name="PingRequest">
   <wsdl:part name="request" element="tns:ping"/>
</wsdl:message>
<wsdl:message name="PingResponse">
   <wsdl:part name="response" element="tns:pingResponse"/>
</wsdl:message>



<wsdl:portType name="ServiceProviderPortType">
   <wsdl:operation name="notifyIac">
      <wsdl:input message="tns:NotifyIacRequest"/>
      <wsdl:output message="tns:NotifyIacResponse"/>
   </wsdl:operation>
   <wsdl:operation name="notifyRejection">
      <wsdl:input message="tns:NotifyRejectionRequest"/>
      <wsdl:output message="tns:NotifyRejectionResponse"/>
   </wsdl:operation>
   <wsdl:operation name="ping">
      <wsdl:input message="tns:PingRequest"/>
      <wsdl:output message="tns:PingResponse"/>
   </wsdl:operation>
</wsdl:portType>



<wsdl:binding name="ServiceProviderBinding" type="tns:ServiceProviderPortType">
   <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
   <wsdl:operation name="notifyIac">
      <soap:operation soapAction="notifyIac" style="document"/>
      <wsdl:input>
          <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
```

```
            <soap:body use="literal"/>
         </wsdl:output>
      </wsdl:operation>
      <wsdl:operation name="notifyRejection">
         <soap:operation soapAction="notifyRejection" style="document"/>
         <wsdl:input>
            <soap:body use="literal"/>
         </wsdl:input>
         <wsdl:output>
            <soap:body use="literal"/>
         </wsdl:output>
      </wsdl:operation>
      <wsdl:operation name="ping">
         <soap:operation soapAction="ping" style="document"/>
         <wsdl:input>
            <soap:body use="literal"/>
         </wsdl:input>
         <wsdl:output>
            <soap:body use="literal"/>
         </wsdl:output>
      </wsdl:operation>
   </wsdl:binding>



   <wsdl:service name="ServiceProvider">
      <wsdl:port name="ServiceProviderPort" binding="tns:ServiceProviderBinding">
         <soap:address location="https://tca.gov.au/iap/services/ServiceProvider"/>
      </wsdl:port>
   </wsdl:service>



</wsdl:definitions>
```

Annex B – Schemas

Common Types Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:tns="http://www.tca.gov.au/schemas/iap/common/2007-02"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   targetNamespace="http://www.tca.gov.au/schemas/iap/common/2007-02"
   elementFormDefault="unqualified" version="2007-02" >


   <xs:annotation>
      <xs:appinfo>
         <xs:documentation>
            <name>iap_common_2007-02.xsd</name>
            <version>2007-02</version>
            <description>Intelligent Access Program - Common types</description>
         </xs:documentation>
      </xs:appinfo>
   </xs:annotation>


    <xs:simpleType name="LocationDegreesType">
      <xs:restriction base="xs:decimal">
         <xs:totalDigits value="8" />
         <xs:fractionDigits value="5" />
         <xs:maxInclusive value="180" />
         <xs:minInclusive value="-180" />
      </xs:restriction>
   </xs:simpleType>


   <xs:simpleType name="DirectionDegreesType">
      <xs:restriction base="xs:decimal">
         <xs:totalDigits value="4" />
         <xs:fractionDigits value="1" />
         <xs:maxExclusive value="360" />
         <xs:minInclusive value="0" />
      </xs:restriction>
   </xs:simpleType>


   <xs:simpleType name="HdopValueType">
      <xs:restriction base="xs:decimal">
         <xs:totalDigits value="3" />
         <xs:fractionDigits value="1" />
         <xs:maxExclusive value="100" />
         <xs:minInclusive value="0" />
      </xs:restriction>
   </xs:simpleType>


   <xs:simpleType name="TotalCombinationMassType">
      <xs:restriction base="xs:decimal">
         <xs:totalDigits value="4" />
         <xs:fractionDigits value="1" />
         <xs:minInclusive value="0" />
         <xs:maxExclusive value="1000.0" />
      </xs:restriction>
   </xs:simpleType>
```

```
<xs:simpleType name="GenericCodeType">
   <xs:restriction base="xs:int">
      <xs:minInclusive value="1" />
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="VehicleCategoryType">
    <xs:restriction base="xs:string">
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="PersistentIdentifierType">
    <xs:restriction base="xs:string">
       <xs:maxLength value="20"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="PhoneNumberType">
    <xs:restriction base="xs:string">
       <xs:maxLength value="20"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="VehicleBodyTypeType">
    <xs:restriction base="xs:string">
       <xs:maxLength value="20"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TrailerTypeType">
    <xs:restriction base="xs:string">
       <xs:maxLength value="20"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="VehicleMakeType">
    <xs:restriction base="xs:string">
       <xs:maxLength value="20"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="VehicleModelType">
    <xs:restriction base="xs:string">
       <xs:maxLength value="30"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="EngineNumberType">
    <xs:restriction base="xs:string">
       <xs:maxLength value="20"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="RegistrationNumberType">
    <xs:restriction base="xs:string">
       <xs:maxLength value="10"/>
   </xs:restriction>
</xs:simpleType>
```

```
<xs:simpleType name="VinType">
    <xs:restriction base="xs:string">
      <xs:maxLength value="17"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NonVinIdentifierType">
    <xs:restriction base="xs:string">
      <xs:maxLength value="25"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IvuIdentifierType">
    <xs:restriction base="xs:string">
      <xs:maxLength value="20"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="TidIdentifierType">
    <xs:restriction base="xs:string">
      <xs:maxLength value="20"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="StateEnum">
    <xs:restriction base="xs:string">
      <xs:enumeration value="NSW"/>
      <xs:enumeration value="VIC"/>
      <xs:enumeration value="QLD"/>
      <xs:enumeration value="SA"/>
      <xs:enumeration value="NT"/>
      <xs:enumeration value="ACT"/>
      <xs:enumeration value="WA"/>
      <xs:enumeration value="TAS"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="RegistrationStateEnum">
    <xs:restriction base="xs:string">
      <xs:enumeration value="NSW"/>
      <xs:enumeration value="VIC"/>
      <xs:enumeration value="QLD"/>
      <xs:enumeration value="SA"/>
      <xs:enumeration value="NT"/>
      <xs:enumeration value="ACT"/>
      <xs:enumeration value="WA"/>
      <xs:enumeration value="TAS"/>
      <xs:enumeration value="FIRS"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="JurisdictionEnum">
    <xs:restriction base="xs:string">
      <xs:enumeration value="NSW"/>
      <xs:enumeration value="VIC"/>
      <xs:enumeration value="QLD"/>
      <xs:enumeration value="SA"/>
      <xs:enumeration value="NT"/>
      <xs:enumeration value="ACT"/>
      <xs:enumeration value="WA"/>
      <xs:enumeration value="TAS"/>
      <xs:enumeration value="TCA"/>
   </xs:restriction>
</xs:simpleType>
```

```
<xs:simpleType name="DayTypeEnum">
   <xs:restriction base="xs:string">
      <xs:enumeration value="ALL"/>
      <xs:enumeration value="WEEKDAY"/>
      <xs:enumeration value="WEEKEND"/>
      <xs:enumeration value="SUNDAY"/>
      <xs:enumeration value="MONDAY"/>
      <xs:enumeration value="TUESDAY"/>
      <xs:enumeration value="WEDNESDAY"/>
      <xs:enumeration value="THURSDAY"/>
      <xs:enumeration value="FRIDAY"/>
      <xs:enumeration value="SATURDAY"/>
   </xs:restriction>
</xs:simpleType>


<xs:simpleType name="IacIdentifierType">
   <xs:annotation><xs:documentation>
      The format of this string is JNNNNNNNNNN, where:
       *   J represents the Jurisdiction and is one of:
         A   for ACT
         V   for Victoria
         Q   for Queensland
         N   for NSW
         W   for WA
         S   for SA
         Z   for NT
         T   for Tasmania
         X   for TCA
      *   NNNNNNNNNN is a Jurisdiction-assigned unique number.
   </xs:documentation></xs:annotation>
   <xs:restriction base="xs:string">
      <xs:pattern value="[a-zA-Z]{1}[0-9]{10}"/>
   </xs:restriction>
</xs:simpleType>


<xs:simpleType name="NcrIdentifierType">
   <xs:annotation><xs:documentation>
      The format of this string is SSSNNNNNNNNNNNNN, where:
      *   SSS is a TCA-assigned IAP-SP identifier
      *   NNNNNNNNNNNN is an IAP-SP-assigned unique number
   </xs:documentation></xs:annotation>
   <xs:restriction base="xs:string">
      <xs:pattern value="[a-zA-Z0-9]{3}[0-9]{12}"/>
   </xs:restriction>
</xs:simpleType>


<xs:simpleType name="PrIdentifierType">
   <xs:annotation><xs:documentation>
      The format of this string is SSSNNNNNNN, where:
       *   SSS is a TCA-assigned IAP-SP identifier
       *   NNNNNNN is an IAP-SP-assigned unique number
   </xs:documentation></xs:annotation>
   <xs:restriction base="xs:string">
      <xs:pattern value="[a-zA-Z0-9]{3}[0-9]{7}"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="AcnType">
   <xs:restriction base="xs:string">
      <xs:pattern value="[0-9]{9}"/>
   </xs:restriction>
</xs:simpleType>
```

```
<xs:simpleType name="AbnType">
   <xs:restriction base="xs:string">
      <xs:pattern value="[0-9]{11}"/>
   </xs:restriction>
</xs:simpleType>


<xs:simpleType name="IapApplicationNameType">
   <xs:restriction base="xs:string">
       <xs:maxLength value="50"/>
   </xs:restriction>
</xs:simpleType>


<xs:simpleType name="IamVersionType">
   <xs:restriction base="xs:string">
       <xs:maxLength value="15"/>
   </xs:restriction>
</xs:simpleType>


<xs:simpleType name="OffTheShelfConditionsIdentifierType">
   <xs:restriction base="xs:string">
       <xs:maxLength value="15"/>
   </xs:restriction>
</xs:simpleType>


<xs:simpleType name="OffTheShelfConditionsRevisionType">
   <xs:restriction base="xs:string">
       <xs:maxLength value="10"/>
   </xs:restriction>
</xs:simpleType>


<xs:complexType name="OffTheShelfConditionsReferenceType">
   <xs:sequence>
      <xs:element name="identifier"
         type="tns:OffTheShelfConditionsIdentifierType" />
      <xs:element name="revision" type="tns:OffTheShelfConditionsRevisionType"/>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="DateTimePeriodType">
   <xs:sequence>
      <xs:element name="startDateTime" type="xs:dateTime"/>
      <xs:element name="endDateTime" type="xs:dateTime"/>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="TimePeriodType">
   <xs:sequence>
      <xs:element name="startTime" type="xs:time"/>
      <xs:element name="endTime" type="xs:time"/>
   </xs:sequence>
</xs:complexType>
```

```
<xs:complexType name="VehicleIdentificationType">
   <xs:sequence>
      <xs:element name="make" type="tns:VehicleMakeType"/>
      <xs:element name="model" type="tns:VehicleModelType"/>
      <xs:element name="registrationNumber" type="tns:RegistrationNumberType"/>
      <xs:element name="registrationStateCode" type="tns:RegistrationStateEnum"/>
      <xs:choice>
          <xs:element name="vin" type="tns:VinType"/>
         <xs:element name="nonVinIdentifier" type="tns:NonVinIdentifierType" />
      </xs:choice>
   </xs:sequence>
</xs:complexType>


<xs:simpleType name="TrailerNumberListType">
   <xs:list itemType="xs:int"/>
</xs:simpleType>


<xs:simpleType name="SpeedUnitEnum">
   <xs:restriction base="xs:string">
      <xs:enumeration value="KMH"/>
      <xs:enumeration value="MPH"/>
   </xs:restriction>
</xs:simpleType>


<xs:simpleType name="SpeedValueType">
   <xs:restriction base="xs:decimal">
      <xs:totalDigits value="4" />
      <xs:fractionDigits value="1" />
      <xs:maxExclusive value="1000" />
      <xs:minInclusive value="0" />
   </xs:restriction>
</xs:simpleType>


<xs:complexType name="SpeedType">
   <xs:sequence>
      <xs:element name="unit" type="tns:SpeedUnitEnum" default="KMH" />
      <xs:element name="value" type="tns:SpeedValueType" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="AddressType">
   <xs:sequence>
      <xs:element name="lineOne" type="xs:string"/>
      <xs:element name="lineTwo" type="xs:string" minOccurs="0" />
      <xs:element name="locality" type="xs:string"/>
      <xs:element name="stateCode" type="tns:StateEnum"/>
      <xs:element name="postCode" type="xs:string"/>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="CompanyOfficerType">
   <xs:sequence>
      <xs:element name="officerName" type="xs:string"/>
      <xs:element name="positionName" type="xs:string"/>
      <xs:element name="businessHoursPhone" type="tns:PhoneNumberType" />
   </xs:sequence>
</xs:complexType>
```

```
   <xs:complexType name="CompanyIdentificationType">
      <xs:sequence>
         <xs:element name="companyName" type="xs:string"/>
         <xs:element name="abn" type="tns:AbnType"/>
         <xs:element name="acn" type="tns:AcnType" minOccurs="0"/>
      </xs:sequence>
   </xs:complexType>


   <xs:complexType name="PointType">
      <xs:sequence>
         <xs:element name="longitude" type="tns:LocationDegreesType"/>
         <xs:element name="latitude" type="tns:LocationDegreesType"/>
      </xs:sequence>
   </xs:complexType>


</xs:schema>
```

Conditions Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:tns="http://www.tca.gov.au/schemas/iap/conditions/2007-02"
   xmlns:common="http://www.tca.gov.au/schemas/iap/common/2007-02"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   targetNamespace="http://www.tca.gov.au/schemas/iap/conditions/2007-02"
   elementFormDefault="unqualified" version="2007-02" >


   <xs:annotation>
      <xs:appinfo>
         <xs:documentation>
            <name>iap_conditions_2007-02.xsd</name>
            <version>2007-02</version>
            <description>Intelligent Access Program - Conditions
               definition</description>
         </xs:documentation>
      </xs:appinfo>
   </xs:annotation>


   <xs:import namespace="http://www.tca.gov.au/schemas/iap/common/2007-02"
      schemaLocation="iap_common_2007-02.xsd"/>


   <xs:simpleType name="BackgroundRuleEnum">
      <xs:restriction base="xs:string">
         <xs:enumeration value="EXCLUSION"/>
         <xs:enumeration value="INCLUSION"/>
      </xs:restriction>
   </xs:simpleType>


   <xs:simpleType name="SpatialRuleEnum">
      <xs:restriction base="xs:string">
         <xs:enumeration value="ABSOLUTE_INCLUSION"/>
         <xs:enumeration value="EXCLUSION"/>
         <xs:enumeration value="INCLUSION"/>
      </xs:restriction>
   </xs:simpleType>


   <xs:complexType name="SpatialConditionType">
      <xs:annotation><xs:documentation>
         It is envisaged that additional extensions to this class will be included in
         subsequent versions of the schema, including CircularZoneConditionType (centre
         point and radius)and RectangularZoneConditionType (top-left and bottom-right
         points).
      </xs:documentation></xs:annotation>
      <xs:sequence>
         <xs:element name="spatialRuleCode" type="tns:SpatialRuleEnum"/>
         <xs:element name="descriptionText" type="xs:string"/>
         <xs:element name="temporalCondition" type="tns:TemporalConditionType"
            minOccurs="0" maxOccurs="unbounded">
            <xs:annotation><xs:documentation>
               If no temporal conditions are specified then this position condition
               applies to every hour of every day covered by the unique or off-the-
               shelf conditions.
            </xs:documentation></xs:annotation>
         </xs:element>
      </xs:sequence>
   </xs:complexType>
```

```
<xs:complexType name="RouteConditionType">
   <xs:complexContent>
      <xs:extension base="tns:SpatialConditionType">
         <xs:sequence>
            <xs:element name="startPoint" type="common:PointType" minOccurs="0"/>
            <xs:element name="endPoint" type="common:PointType" minOccurs="0" />
            <xs:element name="segment" type="tns:SegmentType"
               maxOccurs="unbounded"/>
         </xs:sequence>
      </xs:extension>
    </xs:complexContent>
</xs:complexType>


<xs:complexType name="BoundedZoneConditionType">
   <xs:complexContent>
      <xs:extension base="tns:SpatialConditionType">
         <xs:sequence>
            <xs:element name="segment" type="tns:SegmentType"
               maxOccurs="unbounded"/>
         </xs:sequence>
      </xs:extension>
    </xs:complexContent>
</xs:complexType>


<xs:complexType name="TemporalConditionType">
   <xs:sequence>
      <xs:element name="dayTypeCode" type="common:DayTypeEnum"
         maxOccurs="unbounded" />
      <xs:element name="conditionPeriod" type="common:DateTimePeriodType"
         minOccurs="0">
         <xs:annotation><xs:documentation>
            If no period is specified then this temporal condition applies to every
            day covered by the unique or off-the-shelf conditions.
         </xs:documentation></xs:annotation>
      </xs:element>
      <xs:element name="conditionInterval" type="common:TimePeriodType"
         minOccurs="0" maxOccurs="unbounded">
         <xs:annotation><xs:documentation>
            If no condition interval is specified then this temporal condition
            applies to every hour of every day that it covers (see conditionPeriod).
         </xs:documentation></xs:annotation>
      </xs:element>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="SegmentType">
   <xs:sequence>
      <xs:element name="persistentIdentifier"
         type="common:PersistentIdentifierType" />
      <xs:element name="segmentText" type="xs:string"/>
   </xs:sequence>
</xs:complexType>
```

```
    <xs:complexType name="ConditionsType">
       <xs:sequence>
          <xs:element name="speedCondition" type="common:SpeedType" minOccurs="0" >
             <xs:annotation><xs:documentation>
                 This is the maximum permitted speed.
             </xs:documentation></xs:annotation>
          </xs:element>
          <xs:element name="sdTcmCondition" type="tns:SdTcmConditionType"
             minOccurs="0" maxOccurs="unbounded" />
          <xs:element name="sdCommentCondition" type="xs:boolean" />
          <xs:element name="backgroundRuleCode" type="tns:BackgroundRuleEnum" />
          <xs:choice maxOccurs="unbounded">
             <xs:element name="boundedZoneCondition"
                type="tns:BoundedZoneConditionType" />
             <xs:element name="routeCondition" type="tns:RouteConditionType" />
          </xs:choice>
          <xs:element name="comments" type="xs:string" minOccurs="0"/>
       </xs:sequence>
    </xs:complexType>


    <xs:complexType name="SdTcmThresholdType">
       <xs:sequence>
          <xs:element name="axleCount" type="xs:int" />
          <xs:element name="tcmThreshold" type="common:TotalCombinationMassType" />
       </xs:sequence>
    </xs:complexType>


    <xs:complexType name="SdTcmConditionType">
       <xs:annotation><xs:documentation>
          TCM. An estimate of the total combination mass, entered to
          the nearest 0.1 tonnes.</xs:documentation></xs:annotation>
       <xs:sequence>
          <xs:element name="vehicleCategoryCode" type="common:GenericCodeType"/>
          <xs:element name="vehicleCategory" type="common:VehicleCategoryType"/>
          <xs:element name="threshold" type="tns:SdTcmThresholdType"
             maxOccurs="unbounded" />
       </xs:sequence>
    </xs:complexType>


    <xs:complexType name="OffTheShelfConditionsType">
       <xs:sequence>
          <xs:element name="identifier"
             type="common:OffTheShelfConditionsIdentifierType"/>
          <xs:element name="revision" type="common:OffTheShelfConditionsRevisionType"/>
          <xs:element name="iapApplicationName" type="common:IapApplicationNameType"/>
          <xs:element name="validFromDateTime" type="xs:dateTime"/>
          <xs:element name="validToDateTime" type="xs:dateTime" minOccurs="0" />
          <xs:element name="jurisdictionCode" type="common:JurisdictionEnum"/>
          <xs:element name="conditions" type="tns:ConditionsType"/>
          <xs:element name="authorisingOfficer" type="common:CompanyOfficerType" />
          <xs:element name="issuedDateTime" type="xs:dateTime" />
       </xs:sequence>
    </xs:complexType>


    <xs:element name="offTheShelfConditions" type="tns:OffTheShelfConditionsType"/>


</xs:schema>
```

IAC Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://www.tca.gov.au/schemas/iap/iac/2007-02"
   xmlns:tns="http://www.tca.gov.au/schemas/iap/iac/2007-02"
   xmlns:common="http://www.tca.gov.au/schemas/iap/common/2007-02"
   xmlns:iapcond="http://www.tca.gov.au/schemas/iap/conditions/2007-02"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   elementFormDefault="unqualified" version="2007-02" >


   <xs:annotation>
      <xs:appinfo>
         <xs:documentation>
            <name>iap_iac_2007-02.xsd</name>
            <version>2007-02</version>
            <description>Intelligent Access Program - Electronic IAC Form
               definition</description>
         </xs:documentation>
      </xs:appinfo>
   </xs:annotation>


   <xs:import namespace="http://www.tca.gov.au/schemas/iap/common/2007-02"
      schemaLocation="iap_common_2007-02.xsd"/>
   <xs:import namespace="http://www.tca.gov.au/schemas/iap/conditions/2007-02"
      schemaLocation="iap_conditions_2007-02.xsd"/>


   <xs:simpleType name="TrailerIdentificationLevelEnum">
      <xs:restriction base="xs:string">
         <xs:enumeration value="LEVEL_1"/>
         <xs:enumeration value="LEVEL_2"/>
      </xs:restriction>
   </xs:simpleType>


   <xs:complexType name="PrimaryUnitInstallationType">
      <xs:sequence>
         <xs:choice>
            <xs:element name="vin" type="common:VinType"/>
            <xs:element name="nonVinIdentifier" type="common:NonVinIdentifierType"/>
         </xs:choice>
         <xs:element name="ivuIdentifier" type="common:IvuIdentifierType"/>
         <xs:element name="installationDateTime" type="xs:dateTime"/>
         <xs:element name="ivuLocation" type="xs:string"/>
         <xs:element name="gpsAntennaLocation" type="xs:string"/>
      </xs:sequence>
   </xs:complexType>


   <xs:complexType name="TrailerUnitInstallationType">
      <xs:sequence>
         <xs:element name="trailerNumber" type="xs:int" />
         <xs:choice>
            <xs:element name="vin" type="common:VinType"/>
            <xs:element name="nonVinIdentifier" type="common:NonVinIdentifierType"/>
         </xs:choice>
         <xs:element name="tidIdentifier" type="common:TidIdentifierType"/>
         <xs:element name="installationDateTime" type="xs:dateTime"/>
         <xs:element name="tidLocation" type="xs:string"/>
      </xs:sequence>
   </xs:complexType>
```

```
<xs:simpleType name="IacStatusEnum">
   <xs:restriction base="xs:string">
      <xs:enumeration value="INTERIM"/>
      <xs:enumeration value="INTERIM_CANCELLED"/>
      <xs:enumeration value="LAPSED"/>
      <xs:enumeration value="DENIED"/>
      <xs:enumeration value="APPROVED"/>
      <xs:enumeration value="CEASED"/>
      <xs:enumeration value="CANCELLED"/>
   </xs:restriction>
</xs:simpleType>


<xs:complexType name="PrimaryUnitInformationType">
   <xs:complexContent>
      <xs:extension base="common:VehicleIdentificationType">
         <xs:sequence>
            <xs:element name="garagingAddress" type="common:AddressType"
               minOccurs="0"/>
            <xs:element name="bodyType" type="common:VehicleBodyTypeType"
               minOccurs="0"/>
         </xs:sequence>
      </xs:extension>
   </xs:complexContent>
</xs:complexType>


<xs:complexType name="TrailerUnitInformationType">
   <xs:complexContent>
      <xs:extension base="common:VehicleIdentificationType">
         <xs:sequence>
            <xs:element name="trailerNumber" type="xs:int"/>
            <xs:element name="garagingAddress" type="common:AddressType"
               minOccurs="0"/>
            <xs:element name="trailerType" type="common:TrailerTypeType"/>
         </xs:sequence>
      </xs:extension>
   </xs:complexContent>
</xs:complexType>


<xs:complexType name="TrailerInformationType">
   <xs:sequence>
      <xs:element name="trailerCount" type="xs:int"/>
      <xs:element name="trailerUnitInformation"
         type="tns:TrailerUnitInformationType" maxOccurs="unbounded"/>
      <xs:element name="trailerUnitCombination" type="common:TrailerNumberListType"
         maxOccurs="unbounded" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="ConditionsSectionType">
   <xs:sequence>
      <xs:element name="iapApplicationName" type="common:IapApplicationNameType"/>
      <xs:choice>
         <xs:element name="offTheShelfConditionsIdentifier"
            type="common:OffTheShelfConditionsIdentifierType"/>
         <xs:element name="uniqueConditions" type="iapcond:ConditionsType"/>
      </xs:choice>
   </xs:sequence>
</xs:complexType>
```

```
<xs:complexType name="TransportOperatorIdentificationType">
   <xs:complexContent>
      <xs:extension base="common:CompanyIdentificationType">
         <xs:sequence>
            <xs:element name="transportOperator" type="xs:string" />
         </xs:sequence>
      </xs:extension>
    </xs:complexContent>
</xs:complexType>


<xs:complexType name="TransportOperatorInformationType">
   <xs:sequence>
      <xs:element name="identity" type="tns:TransportOperatorIdentificationType"/>
      <xs:element name="postalAddress" type="common:AddressType"/>
      <xs:element name="businessHoursPhone" type="common:PhoneNumberType" />
      <xs:element name="afterHoursPhone" type="common:PhoneNumberType"
         minOccurs="0" />
      <xs:element name="fax" type="common:PhoneNumberType" minOccurs="0"/>
      <xs:element name="emailAddress" type="xs:string"
         minOccurs="0" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="TransportOperatorSectionType">
   <xs:sequence>
      <xs:element name="transportOperator"
         type="tns:TransportOperatorInformationType" />
      <xs:element name="nominatedOfficer" type="common:CompanyOfficerType"
         minOccurs="0" />
      <xs:element name="primaryUnitInformation"
         type="tns:PrimaryUnitInformationType"/>
      <xs:element name="trailerIdentificationLevelCode"
         type="tns:TrailerIdentificationLevelEnum"/>
      <xs:element name="trailerInformation" type="tns:TrailerInformationType"
         minOccurs="0"/>
      <xs:element name="comments" type="xs:string" minOccurs="0"/>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="ServiceProviderInformationType">
   <xs:sequence>
      <xs:element name="identity" type="common:CompanyIdentificationType" />
      <xs:element name="postalAddress" type="common:AddressType"/>
      <xs:element name="businessHoursPhone" type="common:PhoneNumberType" />
      <xs:element name="fax" type="common:PhoneNumberType" />
      <xs:element name="emailAddress" type="xs:string" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="ServiceProviderSectionType">
   <xs:sequence>
      <xs:element name="serviceProvider"
         type="tns:ServiceProviderInformationType" />
      <xs:element name="primaryUnitInstallation"
         type="tns:PrimaryUnitInstallationType"/>
      <xs:element name="trailerUnitInstallation"
         type="tns:TrailerUnitInstallationType" minOccurs="0"
         maxOccurs="unbounded"/>
      <xs:element name="comments" type="xs:string" minOccurs="0"/>
      <xs:element name="issuedDateTime" type="xs:dateTime" />
   </xs:sequence>
</xs:complexType>
```

```
<xs:complexType name="InterimApprovalSectionType">
   <xs:sequence>
      <xs:element name="lapseDateTime" type="xs:dateTime" />
      <xs:element name="comments" type="xs:string" minOccurs="0"/>
      <xs:element name="authorisingOfficer" type="common:CompanyOfficerType"
         minOccurs="0" />
      <xs:element name="issuedDateTime" type="xs:dateTime" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="ApprovalSectionType">
   <xs:sequence>
      <xs:element name="approved" type="xs:boolean" />
      <xs:element name="comments" type="xs:string" minOccurs="0"/>
      <xs:element name="authorisingOfficer" type="common:CompanyOfficerType" />
      <xs:element name="issuedDateTime" type="xs:dateTime" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="CancellationSectionType">
   <xs:sequence>
      <xs:element name="comments" type="xs:string" minOccurs="0"/>
      <xs:element name="authorisingOfficer" type="common:CompanyOfficerType" />
      <xs:element name="issuedDateTime" type="xs:dateTime" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="JurisdictionInformationType">
   <xs:sequence>
      <xs:element name="jurisdictionCode" type="common:JurisdictionEnum"/>
      <xs:element name="postalAddress" type="common:AddressType"/>
      <xs:element name="businessHoursPhone" type="common:PhoneNumberType" />
      <xs:element name="fax" type="common:PhoneNumberType" />
      <xs:element name="emailAddress" type="xs:string" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="IacType">
   <xs:sequence>
      <xs:element name="iacIdentifier" type="common:IacIdentifierType" />
      <xs:element name="previousIacIdentifier" type="common:IacIdentifierType"
         minOccurs="0" />
      <xs:element name="jurisdiction" type="tns:JurisdictionInformationType" />
      <xs:element name="iacStatusCode" type="tns:IacStatusEnum"/>
      <xs:element name="commencementDateTime" type="xs:dateTime"/>
      <xs:element name="cessationDateTime" type="xs:dateTime" minOccurs="0" />
      <xs:element name="conditionsSection" type="tns:ConditionsSectionType"/>
      <xs:element name="transportOperatorSection"
         type="tns:TransportOperatorSectionType"/>
      <xs:element name="interimApprovalSection"
         type="tns:InterimApprovalSectionType"/>
      <xs:sequence minOccurs="0" >
      <xs:element name="serviceProviderSection"
         type="tns:ServiceProviderSectionType"/>
         <xs:element name="approvalSection" type="tns:ApprovalSectionType"/>
      </xs:sequence>
      <xs:element name="cancellationSection" type="tns:CancellationSectionType"
         minOccurs="0" />
   </xs:sequence>
</xs:complexType>
```

```
   <xs:complexType name="ServiceProviderIacType">
      <xs:sequence>
         <xs:element name="iacIdentifier" type="common:IacIdentifierType" />
         <xs:element name="serviceProviderSection"
            type="tns:ServiceProviderSectionType"/>
      </xs:sequence>
   </xs:complexType>


   <xs:complexType name="IacCancellationRequestType">
      <xs:sequence>
         <xs:element name="iacIdentifier" type="common:IacIdentifierType" />
         <xs:element name="comments" type="xs:string" minOccurs="0"/>
         <xs:element name="authorisingOfficer" type="common:CompanyOfficerType" />
         <xs:element name="issuedDateTime" type="xs:dateTime" />
      </xs:sequence>
   </xs:complexType>


   <xs:element name="iac" type="tns:IacType" />


   <xs:element name="serviceProviderIac" type="tns:ServiceProviderIacType" />


   <xs:element name="iacCancellationRequest" type="tns:IacCancellationRequestType"/>


</xs:schema>
```

Non-Compliance Report Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema    xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns:common="http://www.tca.gov.au/schemas/iap/common/2007-02"
   xmlns:iapcond="http://www.tca.gov.au/schemas/iap/conditions/2007-02"
   xmlns:iac="http://www.tca.gov.au/schemas/iap/iac/2007-02"
   xmlns:tns="http://www.tca.gov.au/schemas/iap/ncr/2007-02"
   targetNamespace="http://www.tca.gov.au/schemas/iap/ncr/2007-02"
   elementFormDefault="unqualified" version="2007-02" >


   <xs:annotation>
      <xs:appinfo>
         <xs:documentation>
            <name>iap_ncr_2007-02.xsd</name>
            <version>2007-02</version>
            <description>Intelligent Access Program - Non Compliance Report
               definition</description>
         </xs:documentation>
      </xs:appinfo>
   </xs:annotation>


   <xs:import namespace="http://www.tca.gov.au/schemas/iap/common/2007-02"
      schemaLocation="iap_common_2007-02.xsd"/>
   <xs:import namespace="http://www.tca.gov.au/schemas/iap/conditions/2007-02"
      schemaLocation="iap_conditions_2007-02.xsd"/>
   <xs:import namespace="http://www.tca.gov.au/schemas/iap/iac/2007-02"
      schemaLocation="iap_iac_2007-02.xsd"/>


   <xs:simpleType name="AlarmCodeType">
      <xs:restriction base="xs:int">
         <xs:minInclusive value="1"/>
         <xs:maxInclusive value="99"/>
      </xs:restriction>
   </xs:simpleType>


   <xs:simpleType name="IgnitionStatusEnum" >
      <xs:restriction base="xs:string">
         <xs:enumeration value="ON" />
         <xs:enumeration value="OFF" />
         <xs:enumeration value="DISCONNECTED" />
      </xs:restriction>
   </xs:simpleType>


   <xs:simpleType name="MovementSensorStatusEnum" >
      <xs:restriction base="xs:string">
         <xs:enumeration value="MOVEMENT" />
         <xs:enumeration value="NO_MOVEMENT" />
         <xs:enumeration value="DISCONNECTED" />
      </xs:restriction>
   </xs:simpleType>


   <xs:simpleType name="NcaTypeEnum">
      <xs:annotation>
         <xs:documentation>Non compliance activity type</xs:documentation>
      </xs:annotation>
      <xs:restriction base="xs:string">
         <xs:enumeration value="SPATIAL"/>
         <xs:enumeration value="TEMPORAL"/>
         <xs:enumeration value="SPEED"/>
```

```
      <xs:enumeration value="ALARM"/>
      <xs:enumeration value="SD_TCM"/>
   </xs:restriction>
</xs:simpleType>

<xs:simpleType name="VehicleLoadStatusEnum">
   <xs:restriction base="xs:string">
      <xs:enumeration value="LOAD"/>
      <xs:enumeration value="NO_LOAD"/>
   </xs:restriction>
</xs:simpleType>

<xs:complexType name="LocationType">
   <xs:sequence>
      <xs:element name="persistentIdentifier"
         type="common:PersistentIdentifierType" />
      <xs:element name="roadName" type="xs:string"/>
      <xs:element name="locality" type="xs:string"/>
      <xs:element name="stateCode" type="common:StateEnum"/>
   </xs:sequence>
</xs:complexType>

<xs:complexType name="LastKnownPositionType">
   <xs:sequence>
      <xs:element name="ivuDateTime" type="xs:dateTime" />
      <xs:element name="position" type="common:PointType" />
      <xs:element name="satelliteCount" type="xs:int"/>
      <xs:element name="hdopValue" type="common:HdopValueType"/>
      <xs:element name="jurisdictionDateTime" type="xs:dateTime" />
      <xs:element name="location" type="tns:LocationType" minOccurs="0"/>
   </xs:sequence>
</xs:complexType>

<xs:complexType name="IvuPositionRecordType">
   <xs:sequence>
      <xs:element name="recordNumber" type="xs:long"/>
      <xs:element name="ivuDateTime" type="xs:dateTime" />
      <xs:element name="position" type="common:PointType" minOccurs="0" />
      <xs:element name="direction" type="common:DirectionDegreesType"/>
      <xs:element name="satelliteCount" type="xs:int"/>
      <xs:element name="hdopValue" type="common:HdopValueType"/>
      <xs:element name="ignitionStatusCode" type="tns:IgnitionStatusEnum" />
      <xs:element name="movementSensorStatusCode"
         type="tns:MovementSensorStatusEnum" />
      <xs:element name="tidIdentifer" type="common:TidIdentifierType" minOccurs="0"
         maxOccurs="unbounded" />
   </xs:sequence>
</xs:complexType>

<xs:complexType name="PositionRecordType">
   <xs:sequence>
      <xs:element name="ivuRecord" type="tns:IvuPositionRecordType" />
      <xs:element name="jurisdictionDateTime" type="xs:dateTime" />
      <xs:element name="location" type="tns:LocationType" minOccurs="0"/>
      <xs:element name="compliant" type="xs:boolean"/>
   </xs:sequence>
</xs:complexType>

<xs:complexType name="IvuSpeedRecordType">
   <xs:sequence>
      <xs:element name="recordNumber" type="xs:long"/>
      <xs:element name="ivuDateTime" type="xs:dateTime" />
```

```
      <xs:element name="position" type="common:PointType" minOccurs="0" />
      <xs:element name="speed" type="common:SpeedType"/>
      <xs:element name="satelliteCount" type="xs:int"/>
      <xs:element name="hdopValue" type="common:HdopValueType"/>
      <xs:element name="tidIdentifer" type="common:TidIdentifierType" minOccurs="0"
         maxOccurs="unbounded" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="SpeedRecordType">
   <xs:sequence>
      <xs:element name="ivuRecord" type="tns:IvuSpeedRecordType" />
      <xs:element name="jurisdictionDateTime" type="xs:dateTime" />
      <xs:element name="speedCondition" type="common:SpeedType"/>
      <xs:element name="location" type="tns:LocationType" minOccurs="0"/>
   </xs:sequence>
</xs:complexType>


<xs:simpleType name="SelfDeclaredCommentTextType">
   <xs:restriction base="xs:string">
      <xs:maxLength value="256"/>
   </xs:restriction>
</xs:simpleType>


<xs:complexType name="IvuSelfDeclaredCommentRecordType">
   <xs:sequence>
      <xs:element name="recordNumber" type="xs:long"/>
      <xs:element name="ivuDateTime" type="xs:dateTime" />
      <xs:element name="iapVersion" type="xs:string" />
      <xs:element name="commentCode" type="common:GenericCodeType" />
      <xs:element name="commentName" type="xs:string" />
      <xs:element name="commentText" type="tns:SelfDeclaredCommentTextType"
         minOccurs="0" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="SelfDeclaredCommentRecordType">
   <xs:sequence>
      <xs:element name="ivuRecord" type="tns:IvuSelfDeclaredCommentRecordType"/>
      <xs:element name="jurisdictionDateTime" type="xs:dateTime" />
      <xs:element name="fromIvu" type="xs:boolean"/>
      <xs:element name="lastKnownPostition" type="tns:LastKnownPositionType"
         minOccurs="0"/>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="IvuSelfDeclaredTcmRecordType">
   <xs:sequence>
      <xs:element name="recordNumber" type="xs:long" />
      <xs:element name="ivuDateTime" type="xs:dateTime" />
      <xs:element name="iapVersion" type="xs:string" />
      <xs:element name="vehicleCategoryCode" type="common:GenericCodeType"/>
      <xs:element name="vehicleCategory" type="common:VehicleCategoryType"/>
      <xs:element name="axleCount" type="xs:int"/>
      <xs:element name="loadStatus" type="tns:VehicleLoadStatusEnum"/>
      <xs:element name="totalCombinationMass" type="common:TotalCombinationMassType"
         minOccurs="0" />
   </xs:sequence>
</xs:complexType>
```

```
<xs:complexType name="SelfDeclaredTcmRecordType">
   <xs:sequence>
      <xs:element name="ivuRecord" type="tns:IvuSelfDeclaredTcmRecordType" />
      <xs:element name="jurisdictionDateTime" type="xs:dateTime" />
      <xs:element name="fromIvu" type="xs:boolean"/>
      <xs:element name="lastKnownPostition" type="tns:LastKnownPositionType"
         minOccurs="0"/>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="IvuAlarmRecordType">
   <xs:sequence>
      <xs:element name="recordNumber" type="xs:long"/>
      <xs:element name="ivuDateTime" type="xs:dateTime" />
      <xs:element name="alarmCode" type="tns:AlarmCodeType"/>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="AlarmRecordType">
   <xs:sequence>
      <xs:element name="ivuRecord" type="tns:IvuAlarmRecordType" />
      <xs:element name="jurisdictionDateTime" type="xs:dateTime" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="DerivedAlarmRecordType">
   <xs:sequence>
      <xs:element name="ivuDateTime" type="xs:dateTime" />
      <xs:element name="jurisdictionDateTime" type="xs:dateTime" />
      <xs:element name="alarmCode" type="tns:AlarmCodeType"/>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="NcaSummaryType">
   <xs:sequence>
      <xs:element name="ncaTypeCode" type="tns:NcaTypeEnum"/>
      <xs:sequence minOccurs="0">
         <xs:element name="ivuNcaPeriod" type="common:DateTimePeriodType"/>
         <xs:element name="jurisdictionNcaPeriod" type="common:DateTimePeriodType"/>
      </xs:sequence>
      <xs:sequence minOccurs="0">
         <xs:element name="initialPosition" type="common:PointType"/>
         <xs:element name="finalPosition" type="common:PointType"/>
      </xs:sequence>
   </xs:sequence>
</xs:complexType>


<xs:complexType name="PrimaryUnitInformationType">
   <xs:complexContent>
      <xs:extension base="common:VehicleIdentificationType">
         <xs:sequence>
            <xs:element name="ivuIdentifier" type="common:IvuIdentifierType"/>
         </xs:sequence>
      </xs:extension>
   </xs:complexContent>
</xs:complexType>
```

```
<xs:complexType name="TrailerUnitInformationType">
   <xs:complexContent>
      <xs:extension base="common:VehicleIdentificationType">
         <xs:sequence>
            <xs:element name="tidIdentifier" type="common:TidIdentifierType"/>
         </xs:sequence>
      </xs:extension>
    </xs:complexContent>
</xs:complexType>


<xs:complexType name="IacReferenceType">
   <xs:sequence>
      <xs:element name="iacIdentifier" type="common:IacIdentifierType" />
      <xs:element name="iapApplicationName" type="common:IapApplicationNameType"/>
      <xs:element name="offTheShelfConditions"
         type="common:OffTheShelfConditionsReferenceType" minOccurs="0" />
   </xs:sequence>
</xs:complexType>


<xs:complexType name="NcrType">
   <xs:sequence>
      <xs:element name="ncrIdentifier" type="common:NcrIdentifierType" />
      <xs:element name="previousNcrIdentifier" type="common:NcrIdentifierType"
         minOccurs="0" >
         <xs:annotation><xs:documentation>
            This element is used to indicate that this NCR represents a continuation
            of a previous NCR (used for spatial non-compliance that exceeds 72
            hours).
         </xs:documentation></xs:annotation>
      </xs:element>
      <xs:element name="auditReferenceDateTime" type="xs:dateTime" >
         <xs:annotation><xs:documentation>
            This is a date and time in the Jurisdiction's time zone that results
            from a deterministic algorithm being applied to the raw IVU records
            that caused the NCR to be issued - in other words the same value for
            this date and time will result no matter how many times the NCR is
            generated, and no matter when it is generated.
      </xs:documentation></xs:annotation>
      </xs:element>
      <xs:element name="iamVersion" type="common:IamVersionType" />
      <xs:element name="iapVersion" type="xs:string" >
         <xs:annotation><xs:documentation>
            This is the version of the specification governing the generation of
            this NCR.
         </xs:documentation></xs:annotation>
      </xs:element>
      <xs:element name="jurisdictionCode" type="common:JurisdictionEnum"/>
      <xs:element name="iacReference" type="tns:IacReferenceType"
         maxOccurs="unbounded" />
      <xs:element name="serviceProvider" type="iac:ServiceProviderInformationType"/>
      <xs:element name="transportOperator"
         type="iac:TransportOperatorIdentificationType"/>
      <xs:element name="primaryUnit" type="tns:PrimaryUnitInformationType"/>
      <xs:element name="trailerUnit" type="tns:TrailerUnitInformationType"
         minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="ncaSummary" type="tns:NcaSummaryType"/>
      <xs:element name="positionRecord" type="tns:PositionRecordType" minOccurs="0"
         maxOccurs="unbounded"/>
      <xs:element name="speedRecord" type="tns:SpeedRecordType" minOccurs="0"
         maxOccurs="unbounded"/>
      <xs:element name="selfDeclaredTcmRecord" type="tns:SelfDeclaredTcmRecordType"
         minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="selfDeclaredCommentRecord"
         type="tns:SelfDeclaredCommentRecordType" minOccurs="0"
```

```
            maxOccurs="unbounded"/>
         <xs:element name="alarmRecord" type="tns:AlarmRecordType" minOccurs="0"
            maxOccurs="unbounded"/>
         <xs:element name="typeTwoAAlarmRecord" type="tns:DerivedAlarmRecordType"
            minOccurs="0" maxOccurs="unbounded"/>
         <xs:element name="typeTwoBAlarmRecord" type="tns:DerivedAlarmRecordType"
            minOccurs="0" maxOccurs="unbounded"/>
         <xs:element name="comments" type="xs:string" minOccurs="0"/>
         <xs:element name="issuedDateTime" type="xs:dateTime" />
      </xs:sequence>
   </xs:complexType>


   <xs:element name="nonComplianceReport" type="tns:NcrType" />


</xs:schema>
```

Participants Report Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:common="http://www.tca.gov.au/schemas/iap/common/2007-02"
   xmlns:tns="http://www.tca.gov.au/schemas/iap/pr/2007-02"
   xmlns:iac="http://www.tca.gov.au/schemas/iap/iac/2007-02"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   targetNamespace="http://www.tca.gov.au/schemas/iap/pr/2007-02"
   elementFormDefault="unqualified" version="2007-02" >


   <xs:annotation>
      <xs:appinfo>
         <xs:documentation>
            <name>iap_pr_2007-02.xsd</name>
            <version>2007-02</version>
            <description>Intelligent Access Program - Participant Report
               definition</description>
         </xs:documentation>
      </xs:appinfo>
   </xs:annotation>


   <xs:import
      namespace="http://www.tca.gov.au/schemas/iap/common/2007-02"
      schemaLocation="iap_common_2007-02.xsd"/>
   <xs:import namespace="http://www.tca.gov.au/schemas/iap/iac/2007-02"
      schemaLocation="iap_iac_2007-02.xsd"/>


   <xs:complexType name="NcrCountsType">
      <xs:sequence>
         <xs:element name="spatialCount" type="xs:int"/>
         <xs:element name="temporalCount" type="xs:int"/>
         <xs:element name="speedCount" type="xs:int"/>
         <xs:element name="alarmCount" type="xs:int"/>
         <xs:element name="sdTcmCount" type="xs:int"/>
         <xs:element name="totalCount" type="xs:int"/>
      </xs:sequence>
   </xs:complexType>


   <xs:complexType name="SummaryRecordType">
      <xs:sequence>
         <xs:choice>
            <xs:element name="vin" type="common:VinType"/>
            <xs:element name="nonVinIdentifier" type="common:NonVinIdentifierType"/>
         </xs:choice>
         <xs:element name="transportOperator"
            type="iac:TransportOperatorIdentificationType"/>
         <xs:element name="iacIdentifier" type="common:IacIdentifierType"
            maxOccurs="unbounded" />
         <xs:element name="iapEntryDateTime" type="xs:dateTime" minOccurs="0" />
         <xs:element name="iapExitDateTime" type="xs:dateTime" minOccurs="0" />
         <xs:element name="ivuIdentifier" type="common:IvuIdentifierType"/>
         <xs:element name="ncrCounts" type="tns:NcrCountsType" />
      </xs:sequence>
   </xs:complexType>


   <xs:complexType name="ParticipantsReportType">
      <xs:sequence>
         <xs:element name="prIdentifier" type="common:PrIdentifierType"/>
         <xs:element name="jurisdictionCode" type="common:JurisdictionEnum"/>
         <xs:element name="reportPeriod" type="common:DateTimePeriodType"/>
```

```
            <xs:element name="serviceProvider" type="iac:ServiceProviderInformationType"/>
            <xs:element name="summaryRecord" type="tns:SummaryRecordType"
               minOccurs="0" maxOccurs="unbounded" />
            <xs:element name="ncrCounts" type="tns:NcrCountsType" />
            <xs:element name="comments" type="xs:string" minOccurs="0"/>
            <xs:element name="issuedDateTime" type="xs:dateTime" />
         </xs:sequence>
      </xs:complexType>


      <xs:element name="participantsReport" type="tns:ParticipantsReportType" />


</xs:schema>
```

tca®
Transport Certification Australia