Transport Certification Australia

Electronic Work Diary Functional and Technical Specification (Draft)

August 2013

Note:

This is a draft document and subject to change. The information within this document is intended for use in understanding the latest requirements for an Electronic Work Diary (EWD). Companies wishing to develop and/or operationally deliver an EWD should contact Transport Certification Australia.

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	Electronic Work Diary Functional and Technical Specification (Draft)
Document Number	TCA-S02-1.07
Version	1.3
Version Date	August 2013
Printing Instructions	Double Sided Colour

Document History

Version	Date	Description
1.1	February 2013	Completed draft for EWD Steering Committee
1.2	March 2013	Revisions accommodating commentary from EWD Steering Committee and stakeholders (internal and Project Management Committee)
1.3	August 2013	Final draft (alignment with Operation Pilot Final Report)

Contents

FIGURES

TABLES

APPENDICES

About Transport Certification Australia

Transport Certification Australia (TCA) is a national government body providing assurance in the use of telematics and other intelligent technologies, to support the current and emerging needs of Australian Governments and industry sectors.

TCA provides **assurance** in the use of information, communications and sensor solutions through identifying, delivering and deploying quality systems.

TCA provides three core services:

- Advice – founded on a demonstrated capability to design and deploy operational systems as enablers for reform
- Accreditation – in the type-approval and certification of telematics and intelligent technologies and services that give confidence to all stakeholders for their consideration of use
- Administration – of certified programs, such as the Intelligent Access Program (IAP), Intelligent Speed Compliance (ISC) Certified Telematics Services (CTS), and IAPm.

TCA's Members are:
Department of Infrastructure, Energy and Resources – Tasmania
Department of Infrastructure and Transport – Commonwealth
Department of Planning, Transport and Infrastructure – South Australia
Department of Transport – Northern Territory
Department of Transport and Main Roads – Queensland
Justice and Community Safety Directorate – Australian Capital Territory
Main Roads Western Australia – Western Australia
Roads and Maritime Services – New South Wales
VicRoads – Victoria

TCA is governed by a Board of Directors which consists of senior representatives from, and appointed by the head of, each Member organisation.

Transport Certification Australia

Level 12, 535 Bourke Street
Melbourne, Victoria 3000
P: (03) 8601 4600
F: (03) 8601 4611
E: tca@tca.gov.au

1 INTRODUCTION

1.1 Purpose

1.1.1 This Specification serves to describe the performance based functional and technical requirements of an Electronic Work Diary (EWD). This Specification describes the requirements for:

a) In-Vehicle Units (IVUs) Type-approval;

b) Electronic Work Diary Service Providers (EWD-SPs); and

c) User Interfaces (UIs) Type-approval.

1.1.2 This Specification is in line with the direction provided by the Australian Transport Council (now SCOTI) to develop a performance based specification for electronic heavy vehicle driver fatigue systems enhancing the use of in-vehicle telematics and adding value to the Intelligent Access Program (IAP).

1.1.3 This Specification is a draft document and subject to change. This Specification has been informed from the outcome of the Operational Pilot of EWDs (RMS 2013) and is subject to change by Transport Certification Australia (TCA) resulting from further consultation, review and policy settlement (NTC 2013). The information within this Specification is intended for use in understanding the requirements for an EWD. Companies wishing to develop and operationally deliver an EWD should contact TCA.

1.2 Scope

1.2.1 This document describes the following EWD requirements:

a) Requirements for IVU Type-approval: these are requirements that shall be met by Applicants intending to provide a Type-approved IVU for usage within an EWD;

b) Requirements for EWD-SPs: these are requirements that shall be met by an EWD-SP in fulfilling the EWD functional and technical requirements of an EWD-SP; and

c) Requirements for the UI Type-approval: these are requirements that shall be met by Applicants intending to provide a Type-approved User Interface for usage within an EWD. A condition of UI Type-approval is that it interfaces with its corresponding Type-approved IVU in a vehicle.

1.2.2 This Specification also serves to detail various obligations of other parties in the EWD. Specifically the Authorities, EWD System Manager and Record Keepers; particularly where these obligations relate to interacting with the EWD-SP.

1.3 Document overview

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

1.3.2 That is, Applicants for certification and, in an ongoing context EWD-SPs, are both encouraged to develop innovative ways of meeting the various functional and technical requirements of this Specification and to submit them for consideration. This will enable EWDs to draw upon the best in available technology as the environment 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.

1.3.3 Whilst the Specification articulates specific functions for each of the IVU and UI, the Applicant may consider these functions being performed by the other, subject to the performance and intent being met to the satisfaction of the EWD System Manager.

1.3.4 This Specification commences with this Introduction (Section 1). It is followed by Section 2, which presents an Overview of the EWD.

1.3.5 References applicable to this Specification are listed in Section 3.

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

a) IVU Type-approval;

b) EWD-SPs; and

c) UI Type-approval, respectively.

1.3.7 IVUs are to be Type-approved. The *Requirements for IVU Type-approval* describe the requirements for IVUs under the EWD. Requirements in this section are prefixed by an 'A'.

1.3.8 The performance of individual, installed IVUs will be monitored during operation in accordance with the *Requirements for EWD-SPs*. Requirements in this section are prefixed by a 'B'. The operation of an IVU and its transfer of data is dependent on a number of factors, such as installation, communication coverage, Global Positioning System (GPS) usage as well as the EWD-SP System's capabilities. The Requirements for EWD-SPs also describe the responsibilities and outputs expected of the EWD-SP, including the Remote Connection Access Framework and data interchange requirements between the various parties taking part in the EWD.

1.3.9 Requirements for the input of data from the Driver and display of information to the Driver and Authorised Officer are contained within the *Requirements for the UI Type-approval*. Requirements in this section are prefixed by a 'C'.

1.3.10 This Specification includes the following Appendices:

- Appendix A: Acronyms and definitions;
- Appendix B: Remote Connection Access Framework (RCAF) explanatory notes;
- Appendix C: Record format;
- Appendix D: Requirements for the provision of IVUs to the EWD System Manager;
- Appendix E: Requirements for the provision of UIs to the EWD System Manager;
- Appendix F: Data requirements;
- Appendix G: Authorised Officer Display example;
- Appendix H: Driver Fatigue Information; and
- Appendix I: Requirements for the Record Keeper.

1.4 Nomenclature

1.4.1 In this document:

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

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

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

d) all references to an IVU in this document shall be considered as a Type-approved IVU endorsed for EWD;

e) all references to a UI in this document shall be considered as a Type-approved UI interfacing with its corresponding Type-approved IVU in a vehicle endorsed for EWD; and

f) terms encased with angled brackets (i.e. <>) refer to fields within data records.

1.4.2 Requirements 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 Requirement.

1.4.4 To assist in understanding the purpose of some Requirements, additional commentary is provided in Blue and Bold, prior to the Requirement.

1.4.5 This Specification makes reference to the IAP Functional and Technical Specification (TCA 2013). Requirements and Appendices which have been created from or are substantially the same as Requirements and Appendices contained within the IAP Functional and Technical Specification (TCA 2013) have been referenced by an " * " as a suffix. For example 'IVU Identifier*'.

1.4.6 These comprise as follows:

a) When only a Requirement heading or Appendix heading exists, the same Requirements contained within the IAP Functional and Technical Specification (TCA 2013) apply with the term 'IAP' replaced with 'EWD';

b) When there are individual Requirements within the Requirement heading or Appendix heading, they are appended to or replace the corresponding Requirement contained within the IAP Functional and Technical Specification (TCA 2013); and

c) When a Requirement heading refers directly or implicitly to a UI, the same Requirements contained within the IAP Functional and Technical Specification (TCA 2013) apply with the term 'IVU' or 'SDID' as appropriate replaced with 'UI'.

2 OVERVIEW OF THE ELECTRONIC WORK DIARY

2.1 General

2.1.1 The participants, or key players in the EWD along with their broad interactions are (Figure 1):

a) Authority – As the context so requires it, references the EWD Regulatory Framework Owner, State Road Transport Authorities and/or the Police;

b) EWD System Manager - The body responsible for the certification and auditing of EWD-SPs and administering the technical and operational environment that interfaces with the EWD-SPs;

c) EWD-SPs - Bodies that provide telematics services (i.e. hardware, software and associated processes) and are certified for provision of EWD services;

d) Drivers - Drivers of heavy vehicles / operations using the EWD;

e) Transport Operators - Transport Operators of one or more heavy vehicles who have adopted the use of EWD;

f) Record Keepers - Bodies responsible for the record keeping task; and

g) Authorised Officers - A person who holds office under the law as an authorised officer and is authorised to review Driver Data Records.

2.1.2 The EWD includes four key elements:

a) In-Vehicle Unit (IVU);

b) User Interface (UI);

c) EWD-SP System; and

d) EWD Registry.

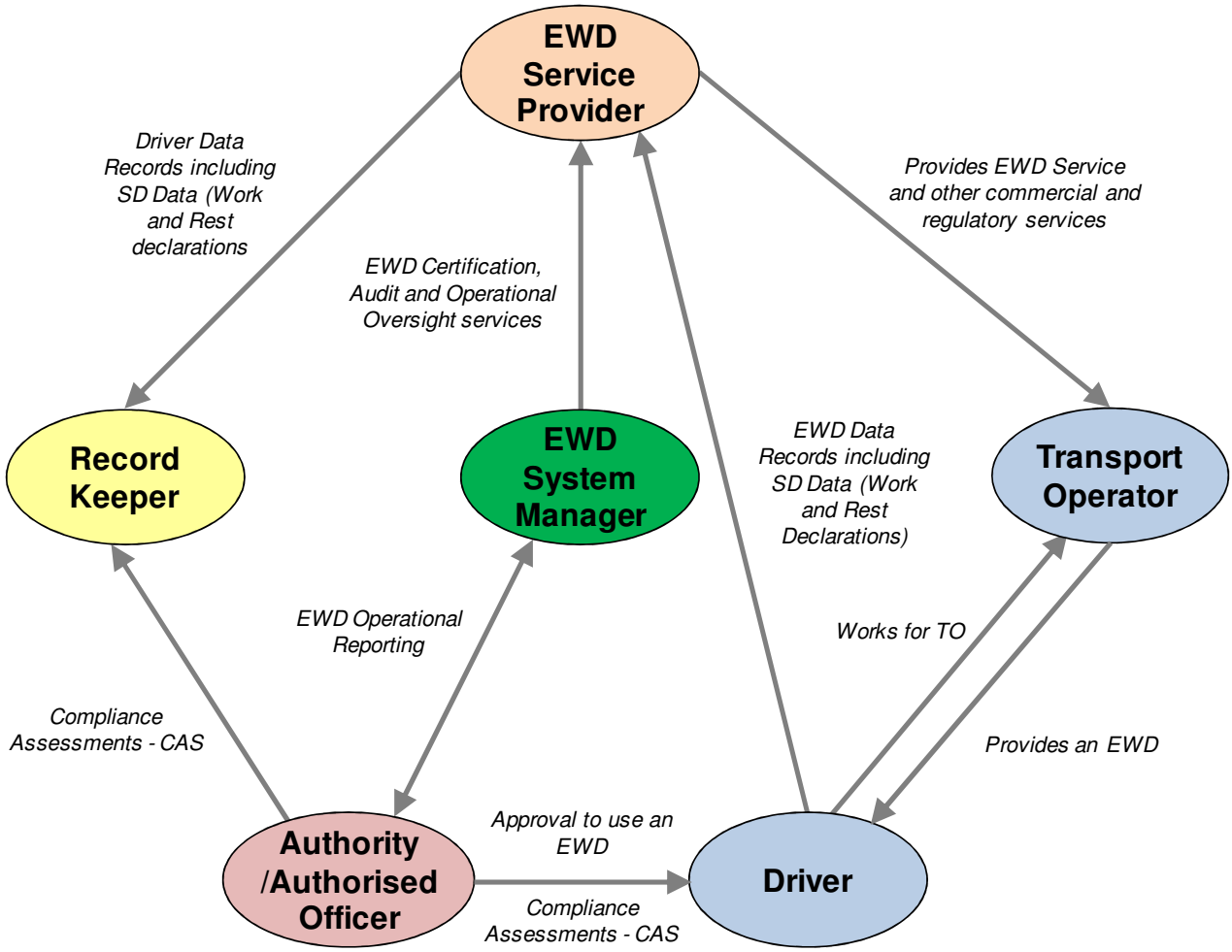

Figure 1: EWD key players

2.2 How the EWD operates

2.2.1 An electronic version of a written work diary is known as an EWD.

2.2.2 An EWD allows a Driver to identify and authenticate themselves and declare their periods of work and rest through the UI. This, along with other contextual information is captured using an IVU that utilises sensors to monitor parameters such as time and position. Wireless communications are typically used to transmit the data stored in the IVU to the EWD-SP System (also commonly referred to as a back office) operated by the EWD-SP.

2.2.3 Before a Driver can use an EWD they are required to register and have their identity confirmed.

2.2.4 The Driver and Transport Operator are required to support the use of an EWD through the installation of an IVU(s) and UI(s) within the heavy vehicle(s) that will be used by the Driver and the engagement / use of an EWD-SP.

2.2.5 Before a Driver can then use an EWD, the Driver must provide proof of identity to the EWD-SP. This process may be facilitated by the Transport Operator. The EWD-SP issues the Driver with a Driver Identification and Authentication method to access the EWD. The Driver Identification and Authentication method allows the Driver to identify and authenticate their identity to the IVU and is used to verify all work and rest declarations made by them, through the UI, much like a signature in a written work diary.

2.2.6 The IVU sends EWD Data Records (Driver periods of work and rest, along with contextual and technical information) to the EWD-SP System. The EWD-SP System includes the hardware and software (excluding the IVU and UI) used in the collection, testing, storage and reporting of EWD Data Records. The EWD-SP System functions under a Quality System approach.

2.2.7 One reporting activity of the EWD-SP System is to provide the Driver's Record Keeper with Driver Data Records. Some or all of the record keeping task may be assigned to the EWD-SP by the Record Keeper.

2.2.8 A second reporting activity of the EWD-SP System is to make the Driver Self Declared records and any Authorised Officer Annotation Records, accessible to the Driver.

2.2.9 A third reporting activity of the EWD-SP System is to exchange information through the Remote Connection Access Framework (RCAF). The architecture underpinning the RCAF is illustrated in Figure 2. The RCAF allows for the following:

a) The EWD-SP System to provide the EWD Registry a current listing of all Drivers who are utilising their (i.e. the EWD-SP's) EWD;

b) The exchange of Driver Data Records between relevant EWD-SP Systems (e.g. where a Driver uses EWDs from two different EWD-SPs); and

c) The Driver Data Records accessible for review by Authorised Officers at the roadside or through the Record Keeper. A roadside review is conducted by the Authorised Officer using the Driver's licence number. The Authorised Officer uses their electronic equipment referred to as the Compliance Assessment Software (CAS) to interrogate the EWD Registry. The EWD Registry holds the names of Drivers who are using EWDs and the details of the corresponding EWD-SP System(s) where the Driver's data records are stored. The Authorised Officer accesses the Driver's Data Records and undertakes the roadside review. The Record Keeper review is similar in process to that of the roadside review. The Authorised Officer lodges Authorised Officer Annotation Records through the review process.

2.2.10 The IVU and/or the EWD-SP System shall generate and provide to the Driver through the IVU/UI, Driver Fatigue Information aimed at assisting the Driver in managing their fatigue obligations.

2.2.11 The EWD-SP shall provide a facility for a Driver's Self Declared Records and Authorised Officer Annotation Records to be viewed away from the IVU and UI (i.e. outside of the vehicle) such as on a PC in a form that is readily accessible, easy to understand and may be printed.

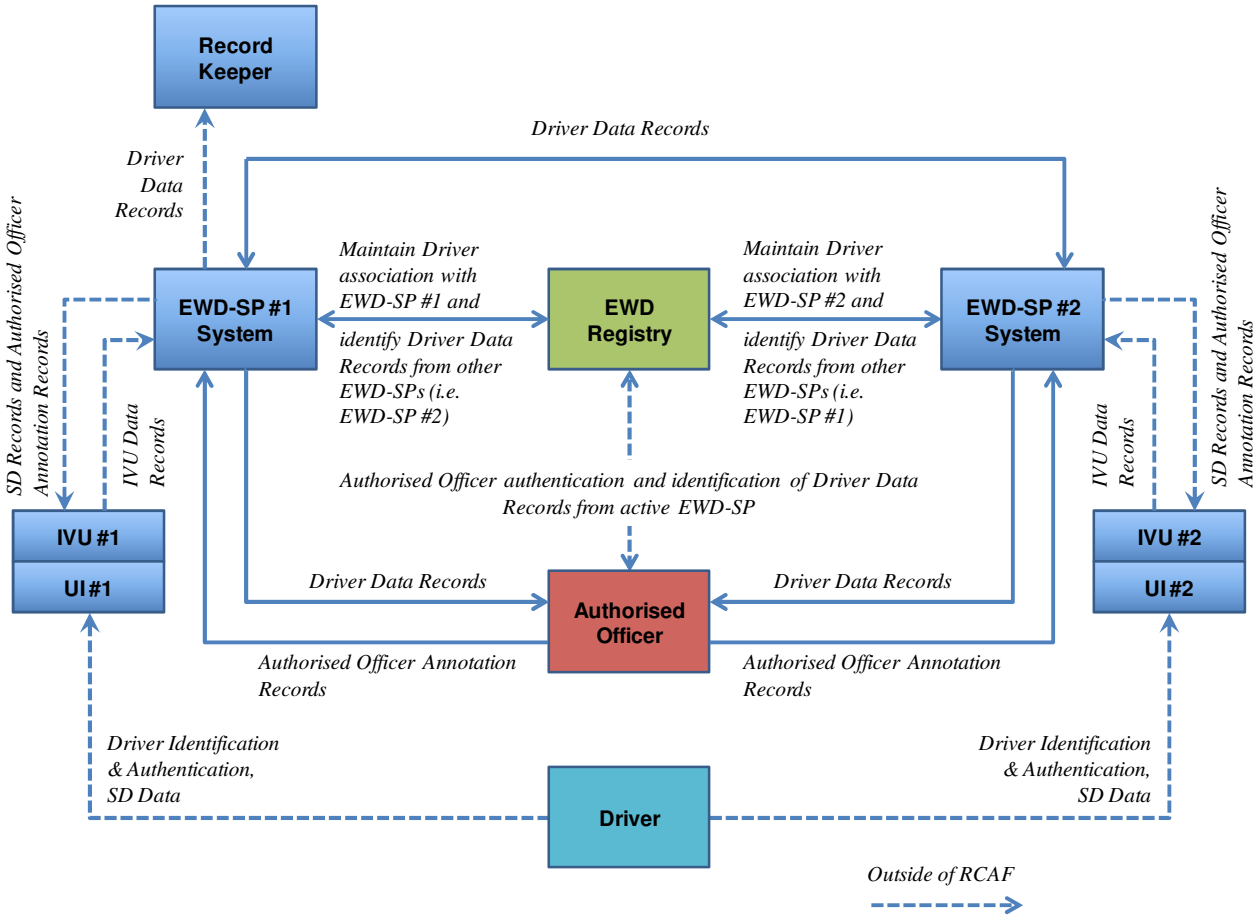

Figure 2: Remote Connection Access Framework (RCAF) architecture (Driver operating under two EWD-SPs / IVUs with EWD-SP #1 being responsible to inform the Driver's Record Keeper)

3 REFERENCES

3.1.1 Documents referenced in this Specification are listed below:

a) Department of Finance and Deregulation (DFD) 2009, National e-Authentication Framework, Commonwealth of Australia, Canberra, ACT.

b) Queensland Government (QG) 2006, Queensland Government Authentication Framework – Authentication Concepts, Version 1.0.3, Queensland Government, Brisbane, Queensland.

c) National Transport Commission (NTC) 2012, Heavy Vehicle National Law, Final Draft, viewed at 11 September 2012.

d) Transport Certification Australia (TCA) 2013, Intelligent Access Program Functional & Technical Specification Version 3.00, Transport Certification Australia, Melbourne, Victoria.

e) Roads and Maritime Services (RMS) 2013, Final Report Operational Pilot of Electronic Work Diaries and Speed Monitoring Systems, Roads and Maritime Services, Sydney, New South Wales.

f) National Transport Commission (NTC) 2013, Preparing Australia for Electronic Work Diaries Regulatory issues paper, National Transport Commission, Melbourne, Victoria.

4 REQUIREMENTS FOR IVU TYPE APPROVAL

A. REQUIREMENTS FOR IVU TYPE APPROVAL

PHYSICAL AND ENVIRONMENTAL CHARACTERISTICS

The rationale for connecting (or tethering) the IVU to the respective prime mover/rigid truck and the requirement of GNSS is presented in RMS 2013.

A.1 In-Vehicle Unit (IVU)*

A.1.1 The EWD Service Provider (EWD-SP) shall provide an In-Vehicle Unit (IVU) that:

a) collects, monitors and stores Global Positioning System (GPS) and other data required to be collected as part of an Electronic Work Diary (EWD);

b) transfers data via a communications device to the EWD-SP; and

c) receives data via a communications device from the EWD-SP.

A.2 IVU identifier*

The rationale for IVU security seals is part of the tamper evidence requirements presented in RMS 2013.

A.3 Security seals*

The Interoperable Interface has been included as an option to copy information locally from the IVU to a USB 2.0 (or higher) external mass storage device.

A.4 Level 3 and Level 4 IVUs

A.4.1 There are two categories of IVU:

a) Level 3 Type-approved; and

b) Level 4 Type-approved.

A.4.2 Level 3 Type-approved IVUs shall transfer IVU Data Records to the EWD-SP.

A.4.3 Level 3 Type-approved IVUs shall display Self Declaration (SD) Records and Authorised Officer Annotation Records via the User Interface (UI).

A.4.4 Level 4 Type-approved IVUs shall have an Interoperable Interface.

A.4.5 Level 4 Type-approved IVUs shall in addition to Level 3 Type-approved functionality, copy SD Records and Authorised Officer Annotation Records to a mass storage device connected to the Interoperable Interface in accordance with Appendix F.

A.5 Geodetic Datum

A.5.1 A Level 3 Type-approved IVU GPS receiver shall determine latitude/longitude in WGS84 or GDA94.

A.5.2 A Level 3 Type-approved IVU GPS receiver shall determine direction of travel of the vehicle in WGS84 or GDA94.

A.5.3 A Level 4 Type-approved IVU GPS receiver shall determine latitude/longitude GDA94.

A.5.4 A Level 4 Type-approved IVU GPS receiver shall determine direction of travel of the vehicle in GDA94.

A.6 Interoperable Interface

A.6.1 The Interoperable Interface shall be a Universal Serial Bus (USB) 2.0 (or greater) port.

A.6.2 The Interoperable Interface shall be capable of accepting a standard Type A USB plug.

A.7 User Interface (UI) capability

A.7.1 The IVU shall be capable of accepting data from the UI.

A.7.2 The IVU shall be capable of sending data to the UI.

A.8 IVU functionality

A.8.1 The UI shall provide a visual indication when the IVU is functioning in accordance with this Specification.

A.8.2 The UI shall provide a visual indication when the IVU is not functioning in accordance with this Specification.

A.8.3 In determining if the IVU is functioning, the EWD-SP shall consider, as a minimum:

a) communication with components of the IVU;

b) communication between the IVU and the UI;

c) capture, storage and transmission of data; and

d) connection of power, ignition and GPS antenna.

A.9 Driver Fatigue Information

A.9.1 The IVU (and/or the EWD-SP System) shall generate the Driver Fatigue Information detailed in Appendix H.

A.9.2 Where a Driver has conducted a period away from the EWD, and the calculation of Driver Fatigue Information in Appendix H is based upon, in at least some part, the period away from the EWD, the IVU shall:

a) generate the Driver Fatigue Information within Appendix H ignoring the counting periods that would encompass the period away from the EWD; and

b) generate a notice that the calculation does not take into consideration the periods of work or rest that occurred during the period away from the EWD.

Note: An example of a period away is when the Driver uses a WWD.

A.9.3 The IVU may provide other information to assist the Driver in managing their fatigue obligations.

The EWD-SP shall provide, to the EWD System Manager, evidence of compliance from an approved organisation that demonstrates the suitability for use of the IVU in heavy vehicles.

A.10 IVU suitability for use in vehicles*

The rationale for the requirement of GNSS (of which GPS is an approved type) is presented in RMS 2013.

A.11 IVU GPS capability*

The IVU shall be permitted to have non-EWD functionality as long as it does not interfere with the functionality of the IVU and EWD-SP System.

A.12 Non-EWD functionality in the IVU*

A.13 Documentation*

A.13.1 The EWD-SP shall document, to the satisfaction of the EWD System Manager:

a) the IVU and all their components, cabling and interfaces; and

b) how the IVU determines its functional state and what conditions generate a functional and not functional indication.

DATA COLLECTION AND RECORD GENERATION

The rationale for the data collected by the EWD is presented in RMS 2013.

A.14 Data*

A.14.1 The IVU shall collect the following data:

a) Driver Identification and Authentication data;

b) GPS Quality data;

c) Date and time;

d) Vehicle position data;

e) Vehicle direction of travel data;

f) Odometer data;

g) Distance travelled data;

h) Alarm status data; and

i) SD data;

A.14.2 The IVU shall process the collected data to produce the following IVU Data Records which are stored for transmission:

a) Position Records;

b) Type 1 Alarm Records; and

c) SD Records.

Note: Type 1 Alarm Records equate to Alarm Records within TCA 2013.

Each Driver shall have a unique way of identifying and authenticating their identity in alignment with government standards on electronic authentication (DFD 2009 and QG 2006).

A.15 Driver Identification and Authentication data

A.15.1 The IVU shall support a method of Driver Identification and Authentication that meets as a minimum the Identity Assurance Level 3 within the National e-Authentication Framework (NeAF).

Note:

a) Information about the NeAF may be obtained from the EWD System Manager.

b) The entry of Driver's Identification and Authentication data may take place through the UI, IVU or a combination of both.

A.15.2 The IVU shall only accept data from the UI upon the successful identification and authentication of a Driver.

A.15.3 The IVU shall use the Identification and Authentication method to generate, at a minimum, the Driver's SD Records with:

a) Driver's licence number;

b) Driver's name; and

c) Driver's licence issuing Jurisdiction.

GPS quality shall be measured to the satisfaction of the EWD System Manager.

A.16 GPS quality data*

The IVU shall measure and record the data and time.

A.17 Date and time data*

The IVU GPS receiver shall determine latitude/longitude position of the vehicle.

A.18 Vehicle position data*

The IVU GPS receiver shall accurately determine direction of travel of the vehicle.

A.19 Vehicle direction of travel data*

Drivers are required to record the odometer reading of the heavy vehicle they are working in at the time of their declaration. The EWD provides the opportunity to either declare the odometer or record the vehicle odometer electronically.

A.20 Odometer data

A.20.1 The IVU shall have the ability to:

a) accept the vehicle's odometer reading from the UI;

b) record the vehicle's odometer reading from the vehicle; or

c) some other way to capture the vehicle's odometer reading.

The rationale for Distance travelled is part of the tamper evidence requirements presented in RMS 2013.

A.21 Distance travelled data*

Note: Distance travelled equates conceptually to requirements under B.17 of TCA 2013.

The rationale for Alarm status data is part of the tamper evidence requirements presented in RMS 2013.

A.22 Alarm status data*

A.22.1 The connection of the UI shall be monitored in accordance with A.25.

A.22.2 For Level 4 Type-approved IVUs, the copying of SD Records to a connected mass storage device shall be reported upon in accordance with A.25.

To ensure that only information entered by the Driver of the vehicle is recorded, the IVU shall only accept information generated through the UI Type-approved to be used with the IVU. It shall not be possible to enter information into the IVU via a UI that has not been Type-approved to work with the IVU.

A.23 Self Declaration (SD) data*

A.23.1 The IVU shall have the capability of receiving, confirming receipt of and storing SD Data, only from a UI connected to it.

A.24 Position Records*

Activity which may be as a result of a (suspected) malfunction or tamper event shall be formulated into Type 1 Alarm Records.

A.25 Type 1 Alarm Records*

A.25.1 The IVU shall generate Type 1 Alarm Records including:

a) the UI is disconnected from the IVU;

b) the UI is reconnected to the IVU;

c) a connection to the Interoperable Interface is made; and

d) a connection to the Interoperable Interface is made and the previous 28 days of SD Records have been copied onto the mass storage device.

A.25.2 The EWD-SP shall use the Alarm Codes as provided by the EWD System Manager when generating Type 1 Alarm Records.

A.25.3 The format of the Type 1 Alarm Record is contained in Appendix C.

SD Records are generated by the Driver entering SD Data and the IVU collected data.

A.26 Self Declaration (SD) Records*

A.26.1 The IVU shall generate SD Records.

A.26.2 SD Records shall consist of the following data:

a) Record type (Activity or Commentary);

b) EWD Functional and Technical Specification version number;

c) The UTC date and time;

d) Date and time UTC offset - as used to render the UTC date and time as a local date and time to the Driver (relative to the Driver's base) (*refer part C.)*;

e) IVU ID;

f) Record number;

g) Driver's licence number

h) Drivers licence issuing Jurisdiction;

i) Driver's name;

j) Driver's base state;

k) Details of the Driver's base;

l) Work hours option - working under standard hours, solo hours of a bus, BFM hours, AFM hours or hours specified in a work/rest hours exemption;

m) BFM or AFM accreditation number;

n) Details of the Driver's record location (physical location of where the Driver Data Records are stored);

o) Work/rest status;

p) Use of the EWD;

q) The odometer reading at that time of the self declaration;

r) Distance Travelled data at the time of the self declaration;

s) The registration number shown on the numberplate of the heavy vehicle that the Driver drives at the time of the self declaration;

t) Two-up arrangement status;

u) If the Driver becomes a two-up Driver:

  i) The other Driver's name;

  ii) The other Driver's licence number;

  iii) Jurisdiction that issued the other Driver's licence;

  iv) The other Driver's work diary number (if using a WWD); and

  v) Jurisdiction that issued to the other Driver's work diary (if using a WWD).

v) Description of self declaration position;

w) Self declaration position (GPS position - latitude/longitude);

x) Date and time of last known non-void position (UTC);

y) Last known non-void position (GPS position - latitude/longitude);

z) Quality Records as set by EWD System Manager; and

aa) Comments (if any).

A.26.3 The <self declaration position> shall be populated from the most recent GPS recorded position where GPS recorded positions shall be determined at a frequency of at least once per second.

A.26.4 The <description of the self declaration position> shall be populated with a text description based upon the latitude and longitude of the current <self declaration position>.

A.26.5 The <description of the self declaration position> shall be accurately populated using the localities files of the IAM and describe the suburb that the <self declaration position> resides *(refer B.42)*.

A.26.6 The EWD-SP shall document, to the satisfaction of the EWD System Manager, how the <description of the self declaration position> is populated.

A.26.7 The format of the SD Record is contained in Appendix C.

A.27 Record numbering*

DATA STORAGE AND TRANSFER

Data collected by the IVU will need to be stored within the IVU until it is able to be transferred to the EWD-SP System. The IVU shall also have at least 28 days of SD Records and Authorised Officer Annotation Records of a successfully identified and authenticated Driver.

A.28 IVU Data Record storage capability*

A.28.1 The IVU shall be capable of storing at least 40,000 Position Records, Type 1 Alarm Records, SD Records and Authorised Officer Annotation Records combined.

Note:

a) SD Records comprise of both A.26.1 and A.32.1.

b) The record storage is dependent on the number and type of Applications or uses of the IVU.

The IVU will need to be able to store data in the event there is a power supply failure or power shutdown.

A.29 IVU external power supply failure/shut down*

Data or software within the IVU shall not be accessible or capable of being manipulated by any person, device or system (including the UI), other than that authorised by the EWD-SP.

A.30 Data security and confidentiality measures*

A.31 IVU communications capability*

A.31.1 The channel for the transmission of data between the IVU and the EWD-SP System and the EWD-SP System and the IVU shall be secure and guarantee standards for privacy and data integrity, at a level defined by the EWD System Manager.

A.32 Transfer of Data between EWD-SP System and IVU and IVU and EWD-SP System*

A.32.1 Upon successful identification and authentication of a Driver, the IVU shall receive the Driver's SD Records and Authorised Officer Annotation Records for the period up to the past (28 x 24 =) 672 hours from the EWD-SP System.

Note: the IVU may already contain some or all of the Driver's SD Records.

A.32.1 The transfer of Driver's SD Records and Authorised Officer Annotation Records from the EWD-SP System to the IVU shall be completed within 15 minutes of successful identification and authentication of the Driver provided that the IVU is in the communication coverage area offered by the EWD-SP and the vehicle is in operation.

A.32.2 The transfer of stored IVU Data Records from the IVU to the EWD-SP shall be performed at least once every 15 minutes provided that the IVU is in the communication coverage area offered by the EWD-SP and the vehicle is in operation.

A.32.3 An SD Activity Record and as applicable its associated SD Commentary Record shall be stored and transmitted together, never separated.

A.32.4 The EWD-SP shall have, to the satisfaction of the EWD System Manager, a sufficient transfer capability in its specified communications coverage between the EWD-SP System and the IVU and the IVU and the EWD-SP System.

Note: At a minimum, the transfer capability shall be designed to support:

a) the transfer of IVU Data Records from the IVU to the EWD-SP System;

b) the update of Driver identification and authentication details and any other such information from the EWD-SP System to the IVU for the Identification and Authentication method (refer A.15.2 and B.15.3);

c) the transfer of SD Records and Authorised Officer Annotation Records to the IVU (refer B.34.1); and

d) the population of the description of self declaration position within SD Records in the IVU;

A.32.5 SD Records stored in the IVU may only be deleted after:

a) a copy of the SD Record has been transferred from the IVU and successful receipt is confirmed by the EWD-SP; and

b) 672 hours (28 x 24) has elapsed since the date and time of their generation.

A.32.6 Position Records and Type 1 Alarm Records stored in the IVU shall only be deleted after such data is transferred from the IVU and successful receipt is confirmed by the EWD-SP.

For Level 4 Type-approved IVUs, data may be transferred to a mass storage device through the Interoperable interface of the IVU.

A.33 Copy of Data from the IVU to mass storage device (Level 4 Type-approved IVU only)

A.33.1 In addition to A.32, Level 4 Type-approved IVU's shall copy SD Records and Authorised Officer Annotation Records to the mass storage device.

A.33.2 Upon insertion of the mass storage device into the Interoperable Interface, the IVU shall, through the UI:

a) prompt for the Driver to identify and authenticate their identity;

b) upon successful identification and authentication, confirm the presence of the Driver's SD Records and Authorised Officer Annotation Records;

c) if no Driver's SD Records or Authorised Officer Annotation Records are present, communicate this to the Driver; and

d) if Driver's SD Records or Authorised Officer Annotation Records are present, copy up to the previous (28 x 24 =) 672 hours of SD Records and Authorised Officer Annotation Records within an EWD Data File to the mass storage device in accordance with Appendix F.

Note: The EWD Data File for copying to the mass storage device does not contain a Manifest Record, see Appendix F.

A.34 Removal of mass storage device from the Interoperable Interface (Level 4 Type-approved IVU only)

A.34.1 The IVU shall allow a request that the mass storage device be ejected.

A.34.2 The request that the mass storage device be ejected shall be from the IVU or UI or both.

A.34.3 The IVU, UI or both shall provide an indication that the mass storage device is safe to eject.

Note: the mass storage device shall be considered safe to eject when the IVU has completed copying SD Data Records and Authorised Officer Annotation Records.

A.34.4 Upon the request to eject the mass storage device, the IVU shall:

a) display a warning not to remove the mass storage device until the SD Records and Authorised Officer Annotation Records copying is complete;

b) write the remaining SD Records and Authorised Officer Annotation Records into the final EWD Data Files (refer Appendix F); and

c) stop any further activity on the mass storage device.

A.34.5 Upon successfully completing A.34.4, the IVU, UI or both shall provide an indication that all files have been successfully copied and it is now safe to remove the mass storage device from the IVU.

A.34.6 The eject process shall not be interrupted by the ignition status.

The transfer of data between the IVU to the EWD-SP System shall be secure and auditable.

A.35 IVU Data Records and Data Blocks*

A.36 Integrity and origin Data Blocks and IVU Data Records*

A.37 Integrity and origin of SD data*

PROVISION OF IVU FOR TYPE-APPROVAL

A.38 IVUs for type-approval

A.38.1 To facilitate Type-approval testing, two IVUs of the type (i.e. Level 3 or Level 4) to be approved shall be provided to the EWD System Manager as per Appendix D.

5 REQUIREMENTS FOR EWD-SPS

B. REQUIREMENTS FOR EWD-SPS

IN-VEHICLE UNIT (IVU) INSTALLATION, OPERATION AND MAINTENANCE

An IVU shall be Type-approved by the EWD System Manager prior to vehicle installation.

B.1 Type-approved IVUs*

B.1.1 The EWD-SP shall not provide an IVU to a Transport Operator if the Transport Operator's physical areas of operation are not within the specified communications coverage for which the EWD-SP is certified.

Note: The specified communications coverage shall be provided to the EWD System Manager by the applicant seeking certification as an EWD-SP.

The EWD-SP shall be responsible for the installation, operation and maintenance of the IVU and UI.

B.2 Installation of IVUs*

B.3 Operation of IVUs*

B.4 Maintenance of IVUs*

B.4.1 In the event that an IVU does not function in accordance with this Specification the EWD-SP shall:

a) complete the resolution process within seven working days of becoming aware of the malfunction subject to the reasonable cooperation of the Transport Operator; and

b) ensure IVU Data Records held by the IVU are transferred to the EWD-SP System within 21 days of the record generation subject to the reasonable cooperation of the Transport Operator.

B.5 Documentation*

USER INTERFACE (UI) INSTALLATION, OPERATION AND MAINTENANCE

B.6 Installation of UIs*

B.7 Operation of UIs*

B.8 Maintenance of UIs*

B.8.1 In the event that an UI does not function in accordance with this Specification the EWD-SP shall complete the resolution process within seven working days of becoming aware of the malfunction subject to the reasonable cooperation of the Transport Operator.

B.9 Documentation*

CERTIFICATION OF EWD-SPs

An EWD-SP shall be certified on the basis of the Type-approval of their IVU and UI and the certification of their EWD-SP System.

B.10 Certification of EWD-SPs*

B.11 EWD-SP Identifier

B.11.1 An EWD-SPs shall have a unique EWD-SP Identifier.

B.11.2 The EWD-SP Identifier shall be a trigraph assigned by the EWD System Manager.

B.11.3 Each EWD-SP Identifier shall map to at most one EWD-SP.

B.11.4 Each ABN shall map to at most one EWD-SP.

EWD-SP SYSTEM

The EWD-SP System application will be considered as a function of the number IVUs and UIs the EWD-SP has the capacity to support in accordance with this Specification.

B.12 EWD-SP System*

B.12.1 The EWD-SP System shall achieve the minimum performance of:

a) 99.5% uptime and availability of data over any period of (28 x 24 =) 672 hours; and

b) no greater than 1 hour downtime or unavailability of data in any 24 hour period.

The EWD-SP is responsible for the operation of their EWD-SP System in accordance with this Specification. Maintenance and continuity of the EWD-SP System shall be consistent with the need for Driver Data Records to be available for compliance assessment continuously and without significant delay or unavailability.

B.13 Maintenance and continuity of the EWD-SP System*

B.13.1 The EWD-SP shall have sufficient equipment and resources available such that, in the event of a component becoming inoperable that does not impact the performance of the EWD-SP System specified in B.12.1 and B.30, the EWD-SP System can be returned to its certified operational state within three working days.

B.13.2 The EWD-SP shall document, to the satisfaction of the EWD System Manager, their plan for recovery from 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.

REGISTRATION OF DRIVERS FOR EWD USAGE

B.14 Driver approval by Authority

B.14.1 The Authority will approve Drivers for EWD usage.

B.14.2 The Authority will issue a Driver with a completed EWD Driver Authorisation Form.

B.14.3 The EWD Driver Authorisation Form will contain as a minimum:

a) the Driver's identity;

b) the Driver's licence number and licence issuing Jurisdiction; and

c) the Authority's EWD usage approval for the Driver.

B.15 Driver Registration

B.15.1 Drivers must be registered within the EWD-SP System and the EWD Registry prior to using an EWD.

B.15.2 The Driver will provide the EWD-SP with the EWD Driver Authorisation Form.

B.15.3 The EWD-SP shall only register Drivers for EWD usage that present with a complete and consistent EWD Driver Authorisation Form.

B.15.4 Drivers that have previously been de-registered shall be required to present a new EWD Driver Authorisation Form prior to being registered by the EWD-SP.

B.15.5 After receipt of the EWD Driver Authorisation Form from the Driver, the EWD-SP shall check the document for completeness and plausibility of information provided and consistency of that information with any material previously lodged by the Driver or Transport Operator with the EWD-SP.

B.15.6 If any such incompleteness or inconsistency is detected the EWD-SP shall return the EWD Driver Authorisation Form to the Driver with a notation indentifying the conflict, to enable the Driver to resolve any anomalies with the Authority.

B.15.7 If the EWD Driver Authorisation Form is complete and consistent, then the EWD-SP shall register the Driver by:

a) updating the EWD Registry with the relevant Driver details (*refer B.38)*; and

b) issue the Driver with their Driver Identification and Authentication method.

Note: the Driver Identification and Authentication method may require liaising with the relevant Transport Operator.

B.15.8 The Driver identification and authentication details within the Driver Identification and Authentication method shall be populated with the details contained in the EWD Driver Authorisation Form.

B.15.9 The EWD-SP shall maintain documentation of registered Drivers for EWD usage including:

a) the EWD Driver Authorisation Form;

b) The personnel performing the registration; and

c) The details of the registration.

B.16 Driver De-registration

B.16.1 The EWD-SP shall implement a de-registration process through which a Driver's registration to access the EWD will be revoked.

B.16.2 Drivers who no longer have the authority to use an EWD shall be de-registered.

B.16.3 Drivers de-registration shall include, within three working days, the deregistration from:

a) Driver Identification and Authentication method; and

b) EWD-SP System *(refer B.46)*.

B.16.4 Drivers de-registration shall include (91 x 24 =) 2,184 hours after the date of de-registration, removal of the Driver details from the EWD Registry (*refer B.38*).

B.16.5 The EWD-SP shall maintain documentation of deregistered Drivers for a period of one year after the date of de-registration.

Drivers using an EWD will need to identify and authenticate with the EWD. Whilst the method of identification and authentication is performance based, the information captured through this process is prescribed to ensure interoperability.

B.17 Identification and Authentication

B.17.1 The EWD-SP shall provide a unique Identification and Authentication method to the Driver *(refer A.15.1).*

B.17.2 The Identification and Authentication method shall be used to identify and authenticate the Driver's identity for use with, as a minimum, the UI and by association the IVU.

B.17.3 The method of ensuring the Driver Identification and Authentication method is current shall be documented to the satisfaction of the EWD System Manager.

B.17.4 The method of ensuring the status of Drivers identification and authentication is up to date shall be documented to the satisfaction of the EWD System Manager.

B.18 EWD-SP Driver capacity

B.18.1 The EWD-SP shall have sufficient capability and capacity to support, in accordance with this Specification, the number of Drivers for which it has been certified.

B.18.2 The EWD-SP shall immediately notify the EWD System Manager when it has in service 80% of the number of Drivers for which it has been certified.

AUTHORISED OFFICER EWD USAGE

Authorised Officers will have access to Driver Data Records as part of their compliance and enforcement functions on-road and in the back-office. The back-office processes are detailed in Appendix I.

B.19 Authorised Officers

B.19.1 An Authorised Officer will have remote access to Driver Data Records as part of their on-road compliance and enforcement function.

B.19.2 The Authorised Officer will use the Compliance Assessment Software (CAS) to perform B.19.1

B.20 Authorised Officer Annotation Records

B.20.1 The Authorised Officer will, through CAS, generate an Authorised Officer Annotation Record when they access a Driver's Driver Data Records.

B.20.2 The Authorised Officer will, through CAS, generate an Authorised Officer Annotation Record when they elect to provide commentary.

B.20.3 The Authorised Officer Annotation Record shall be transferred to the Driver's Data Records stored in the EWD-SP System.

B.20.4 An Authorised Officer Annotation Record shall consist of the following data:

a) Record type;

b) EWD Functional and Technical Specification version number;

c) The UTC date and time;

d) Date and time UTC offset (derived from time zone of the intercept location);

e) Terminal ID;

f) Record number;

g) Drivers licence number;

h) Drivers licence issuing Jurisdiction;

i) Number of days of Drivers Data Records requested; and

j) Authorised Officer annotation text (variable length structured data).

Note: The process above is detailed within the Remote Connection Access Framework (refer B.41).

DATA HANDLING

B.21 Data collection*

B.22 Data processing*

B.22.1 EWD Data Records comprise:

a) Position Records;

b) Type 1 Alarm Records;

c) SD Records;

d) Authorised Officer Annotation Records; and

e) Type 2 Alarm Records.

B.22.2 Driver Data Records are a subset of the EWD Data Records.

B.22.3 Driver Data Records comprise:

a) SD Records;

b) Authorised Officer Annotation Records; and

c) Position Records that commence with the first occurrence of a Driver's SD Record and cease with one of the following:

i) an SD Record from the Driver where the <use of the EWD> contains 1, 2 or 3 from C.12.1;

ii) a period where the vehicle is not in operation of greater than 72 hours;

iii) the EWD-SP has detected, through the RCAF, the Driver has generated a more recent SD Record using another IVU (where applicable); and

iv) some other event that demonstrates the Driver is no longer associated with the vehicle.

B.22.4 If IVU Data Records are collected in WGS84, the EWD-SP shall convert them to GDA94 prior to storage or provision via the RCAF and any further processing for consistency with the IAM and EWD in general *(refer B.27)*.

The EWD-SP shall test records and generate appropriate Type 2 Alarm Records. This provides an indication of the operational status of the IVU and malfunctioning, tampering and attempted tampering.

B.23 Data testing*

B.24 Driver Fatigue Information

B.24.1 The EWD-SP system (and/or the IVU) shall generate the Driver Fatigue Information detailed in Appendix H.

B.25 Type 2 Alarms and Type 2 Alarm Records*

B.25.1 The EWD-SP shall:

a) continuously monitor for evidence of malfunction, tampering or attempted tampering with the IVU hardware, software and data, assessing the nature of Type 1 Alarm Records and Type 2 Alarms, together with all other information and evidence available from the vehicle and from inspection and investigation.

b) The EWD-SP shall immediately report to the Authority in accordance with B.4.

B.25.2 The EWD-SP shall check for the presence of Type 1 Alarm Records.

B.25.3 The EWD-SP shall check for the presence of Type 2 Alarms in accordance with B.23.

B.25.4 The EWD-SP shall generate Type 2 Alarm Records from Type 2 Alarms.

B.25.5 The format of Type 2 Alarm Records is contained within Appendix C.

The EWD-SP shall demonstrate an auditable trail of the generation of data and as such shall back up and archive data.

B.26 Data backup and archiving*

REMOTE CONNECTION ACCESS FRAMEWORK – REFERENCE

The Remote Connection Access Framework (RCAF) provides for remote access interoperability for multiple stakeholders and permits:

- **An EWD-SP to determine if a Driver has relevant Driver Data Records with another EWD-SP;**
- **Authorised Officers to locate with which EWD-SP a Driver's Driver Data Records are stored; and**
- **Authorised Officers to lodge Authorised Officer Annotation Records.**

Central to this functionality is the EWD Registry. The EWD Registry holds the referencing address with the EWD-SP of the Driver Data Records but does not hold actual Driver Data Records. EWD-SPs ensure that Drivers using their EWDs are registered in the EWD Registry and keep the registration updated by noting when they have last received Driver Data Records. EWD-SPs frequently check the EWD Registry for updates of the Drivers using their EWD and if required, will download records from other EWD-SPs.

An Authorised Officer uses the Driver's licence number and State of issue to search the EWD Registry and obtain where the Driver Data Records are stored. An Authorised Officer then undertakes the roadside assessment using the Compliance Assessment Software (CAS).

B.27 Driver identification for RCAF interoperability and transfer of records

B.27.1 The EWD-SP shall ensure interoperable Driver identification for the purpose of achieving:

a) RCAF usage for other EWD-SPs and Authorised Officers; and

b) the transfer of records as defined in Appendix F.

B.27.2 A Driver shall have unique driver ID.

B.27.3 The EWD-SP shall use the information from the EWD Driver Authorisation Form to create the driver ID.

B.27.4 The driver ID shall be of the form "<licence issuing Jurisdiction><licence number>".

Note: For example "VIC1234567", "NSW12341234", "SA12341234".

B.27.5 The licence issuing Jurisdiction shall be at least one of: VIC, NSW, ACT, QLD, NT, SA, WA or TAS.

B.27.6 The driver ID shall be a maximum of 16 characters.

Note: driver ID for RCAF Interoperability and organisation of records for transfer is not the same as the Driver Identification and Authentication method provided to the Driver to access the EWD.

B.28 Management of the RCAF architecture

B.28.1 The RCAF architecture will be managed by the EWD System Manager.

B.29 Management of the EWD Registry

B.29.1 The EWD Registry will be managed by the EWD System Manager and/or Authority.

B.30 EWD-SP System RCAF Interface and data availability with RCAF

B.30.1 The EWD-SP System shall interface with the RCAF in accordance with B.36.

B.30.2 The EWD-SP System RCAF Interface, shall achieve the minimum performance of:

a) 99.5% uptime and availability of data over any period of (28 x 24 =) 672 hours; and

b) no greater than 1 hour downtime or unavailability of data in any 24 hour period.

Note: Refer B.36

B.30.3 The EWD-SP shall document, to the satisfaction of the EWD System Manager, how they shall meet the minimum performance levels of B.30.2.

B.31 Basic concepts and entities

Note: RCAF explanatory notes are in Appendix B.

B.31.1 Within the scope of the RCAF Interface, EWD-SPs shall be uniquely identified primarily by a trigraph assigned by the EWD System Manager (the "EWD-SP Identifier"), and secondarily by their ABN (i.e., each ABN shall map to at most one EWD-SP).

Note: Refer to B.11.

B.31.2 A Driver shall be considered active with respect to an EWD-SP where that EWD-SP has collected a Driver Data Record for that Driver within the past (91 x 24 =) 2,184 hours, or where that EWD-SP has authenticated that Driver within the past (91 x 24 =) 2,184 hours.

B.31.3 Driver Data Records shall be considered recent where they have an internal record date and time that falls within (91 x 24 =) 2,184 hours of the current date and time.

B.31.4 An SD Commentary Record shall be considered recent where the SD Activity Record that it pertains to is considered recent.

B.32 Connectivity and interoperability

B.32.1 Communication between EWD-SPs, the EWD Registry and Compliance Assessment Software (CAS) shall occur using RESTful Web Services.

Note: in the context of this Specification, the term RESTful Web Services implies the use of standard HTTP method names (e.g., GET, PUT, POST, DELETE) and variable, resource-oriented URLs.

B.32.2 All communication between EWD-SPs, the EWD Registry and CAS instances shall occur over the public internet using HTTPS (i.e., HTTP running over TLS 1.x or SSL 3.0).

Note: the use of TLS or SSL provides confidentiality, in addition to both server and client authentication.

B.32.3 The EWD-SP shall host a server capability on the public internet that accepts connections from other EWD-SPs, and CAS instances or their proxies.

B.32.4 When acting as a server, the EWD-SP shall allow access to variable suffix URLs as defined in this Specification.

Note: RESTful Web Services rely upon dynamically constructed URLs to identify fine-grained resources. This requirement should be brought to the attention of network engineers as some firewalls may require careful configuration.

B.32.5 The EWD-SP shall have a client capability to connect via the public internet to the EWD Registry, and to other EWD-SPs.

B.32.6 The EWD-SP shall provision the connection between the EWD-SP System and the EWD Registry using EWD Registry details as provided by the EWD System Manager. These details shall include the EWD Registry ABN, and EWD Registry URL(s).

B.32.7 When acting as a server, the EWD Registry and the EWD-SP shall each support HTTP request and response compression through use of the Content-Encoding and Accept-Encoding HTTP headers. The EWD Registry and the EWD-SP shall each:

a) accept HTTP request bodies that are GZIP encoded, as indicated by a “Content-Encoding: gzip” header; and

b) be able to GZIP encode HTTP response bodies where the associated HTTP request contains an “Accept-Encoding: gzip” header.

B.32.8 The EWD-SP shall ensure that the EWD System Manager has the following details:

a) EWD-SP name;

b) EWD-SPABN; and

c) base URL of the form https://<hostname>/<path> (for construction of RESTful Web Service URLs).

Note: These details are subsequently discovered by other EWD-SPs through the EWD Registry.

Within the RCAF, all communication will require a trusted form of authentication. This ensures that information is only shared with appropriate entities.

B.33 Authentication

B.33.1 When acting as a server, the EWD-SP and EWD Registry shall authenticate to clients using an SSL server certificate:

a) issued by a well-known and trusted Certification Authority;

b) supporting at least 128-bit encryption; and

c) having a Subject Common Name consistent with the hostname component of the URLs exposed to HTTP clients.

B.33.2 When acting as a server, the EWD-SP and EWD Registry shall require client-authentication TLS or SSL before allowing access to any URL defined within this Specification.

B.33.3 When acting as a server, the EWD-SP shall authenticate other EWD-SPs (as clients). The EWD-SP shall:

a) trust the VeriSign Gatekeeper Type 3 Operational Certification Authority (OCA); and

b) ensure that the ABN encoded within the client’s certificate appears within the set of EWD-SPs discovered using the EWD Registry.

B.33.4 When acting as a server, the EWD-SP shall authenticate CAS and Authorised Officers (as clients). The EWD-SP shall:

a) trust the CAS self-signed certificate generated by EWD System Manager; and

b) require and process an EWD Authentication Token (*refer B.34*).

B.33.5 When acting as a client, the EWD-SP shall authenticate itself using client-authentication TLS or SSL and a Gatekeeper Type 3 certificate that encodes its ABN.

In addition to the correct systems (i.e. EWD-SP, CAS, EWD Registry), Authorised Officers need to be authenticated prior to being able to obtain Driver Data Records.

B.34 EWD Authentication Tokens

B.34.1 The details of the EWD Authentication Token shall be provided by the EWD System Manager.

For interoperability purposes, the interface to the EWD Registry and EWD-SP is fully prescribed.

B.35 EWD Registry RCAF Interface

B.35.1 The EWD Registry shall support the "GET /providers" operation; this operation returns a list of all known EWD-SPs.

Security	EWD-SP clients must be authenticated using a Gatekeeper Type 3 Certificate, the ABN from which must match a known EWD-SP.
Request Headers	None
Request Body	None
Response Code	200 – OK
Response Headers	Content-Type – text/csv
Response Body	Multiple lines of the following fields (separated by commas), with each line terminated by a carriage return, a line feed, or both: • provider-id – unique EWD-SP Identifier (e.g., XYZ); • provider-abn – EWD-SP's current ABN. This should be used as the basis for authenticating EWD-SP calls: the ABN is extracted from the client's Gatekeeper certificate and mapped to an EWD-SP Identifier; • provider-name – the company name of the EWD-SP; and • provider-url - the base URL from which all other URLs will be constructed (e.g., https://someprovider.com.au/ewd/rest).

B.35.2 The EWD Registry shall support the "PUT /drivers/{driver-id}" operation. This operation establishes an association between the EWD-SP (the authenticated client) and the specified Driver, and also advertises the most recently received Driver Data Records held by the authenticated client for the specified Driver.

Security	EWD-SP clients must be authenticated using a Gatekeeper Type 3 Certificate, the ABN from which must match a known EWD-SP.
Request Headers	Content-Type – text/csv
Request Body	A single line of the following fields (separated by commas) terminated by a carriage return, a line feed, or both: • driver-id – unique Driver identifier. Must match the value within

	the URL; • provider-id – the identifier associated with the authenticated client (an EWD-SP); • driver-records-key – a "password" required to download this Driver's Driver Data Records from the EWD-SP; this should vary per-Driver; and • driver-records-last-modified – the date and time at which the most recent Driver Data Record was receipted by the EWD-SP. This value is in ISO 8601 format (e.g., 2012-10-31T13:52:16Z). The purpose of this value is for other EWD-SPs to detect that new Driver Data Records are available; it is NOT directly used in downloading of those new Driver Data Records.
Response Code	204 – No Content – on success 400 – Bad Request – if the data contained errors (e.g., there was a mismatch between the driver-id in the data and in the URL).
Response Headers	None
Response Body	None

B.35.3 The EWD Registry shall support the "POST /drivers/updated" operation. This operation allows an EWD-SP to perform a "bulk update" of the most recently received Driver Data Records for multiple Drivers:

a) Drivers described in the request body, but not yet registered with the EWD Registry for the calling EWD-SP, are registered in a manner equivalent to invoking "PUT /drivers/{driver-id}";

b) Drivers described in the request body, and that are registered with the EWD Registry for the calling EWD-SP, are updated in a manner equivalent to invoking "PUT /drivers/{driver-id}";

c) Drivers not described in the request body, and that are registered with the EWD Registry for the calling EWD-SP, are not affected within the EWD Registry; and

d) This is an atomic operation; all updates occur, or no updates occur.

Note: Atomic in this context means just that: either every Driver specified within the request body has their details updated in the EWD Registry, or none of the Drivers do.

Security	EWD-SP clients must be authenticated using a Gatekeeper Type 3 Certificate, the ABN from which must match a known EWD-SP.
Request Headers	Content-Type – text/csv
Request Body	Multiple lines of the following fields (separated by commas), with each line terminated by a carriage return, a line feed, or both: • driver-id – unique Driver identifier; • provider-id – the identifier associated with the authenticated client (an EWD-SP); • driver-records-key – a "password" required to download this Driver's Driver Data Records from the EWD-SP; this should vary per-Driver; and • driver-records-last-modified – the date and time at which the most recent Driver Data Record was receipted by the EWD-SP. This value is in ISO 8601 format (e.g., 2012-10-31T13:52:16Z). The purpose of this value is for other EWD-SPs to detect that new

	Driver Data Records are available; it is NOT directly used in downloading of those new Driver Data Records.
Response Code	204 – No Content – on success 400 – Bad Request – if the data contained errors (e.g., there was a mismatch between the EWD-SP Identifier and the authenticated EWD-SP).
Response Headers	None
Response Body	None

B.35.4 The EWD Registry shall support the "DELETE /drivers/{driver-id}" operation. This operation removes the association between the EWD-SP (the authenticated client) and the specified Driver.

Security	EWD-SP clients must be authenticated using a Gatekeeper Type 3 Certificate, the ABN from which must match a known EWD-SP.
Request Headers	None
Request Body	None
Response Code	204 – No Content – in the case the operation succeeded. 404 – Not Found – in the case that the Driver is not associated with the EWD-SP.
Response Headers	None
Response Body	None

B.35.5 The EWD Registry shall support the "GET /drivers" and "GET /drivers/shared":

a) "/drivers" is only called by EWD-SPs, and returns a list of all Drivers associated with the EWD-SP (the authenticated client); and

b) "/drivers/shared" is only called by EWD-SPs, and returns a list of Drivers that are associated with the EWD-SP (the authenticated client) and at least one other EWD-SP.

Security	EWD-SP clients must be authenticated using a Gatekeeper Type 3 Certificate, the ABN from which must match a known EWD-SP. CAS must be authenticated using a self-signed certificate provided by the EWD System Manager, and additionally Authorised Officer credentials (using a mechanism outside the scope of this Specification).
Request Headers	If-Modified-Since – if specified, only return the requested list of Drivers if it has changed since the specified date and time, or if any entry within the list has changed since the specified date and time. Note that the entire list is returned if any change has occurred, not just the changed entries. The value specified should be exactly as returned in the Last-Modified response header of a previous GET operation. This value must be in HTTP date format (e.g., Fri, 05 Oct 2012 06:11:25 GMT)
Request Body	None
Response Code	200 – OK 204 – No Content – if there are no matching Drivers. 304 – Not Modified – if no data has changed since If-Modified-Since.

Response Headers	Last-Modified – the date and time at which the last change was made to the list, including to any entry within the list. Retain this value for subsequent GET operations. This header should be returned for response codes 200 and 304, and must be in HTTP date format. Content-Type – text/csv
Response Body	The following fields (separated by commas), with each line separated by a carriage return, a line feed, or both: • driver-id –Driver identifier; • provider-id – the EWD-SP Identifier; • driver-records-key – a "password" required to download this driver's Driver Data Records from this EWD-SP; and • driver-records-last-modified – the date and time at which the most recent Driver Data Records was receipted by the EWD-SP. This value is in ISO 8601 format (e.g., 2012-10-31T13:52:16Z). When called by an EWD-SP, the first record for each Driver pertains to the authenticated EWD-SP.

B.36 EWD-SP System RCAF Interface

B.36.1 EWD-SPs shall support the "GET /drivers/{driver-id}/records?key={key}" operation for the purposes of obtaining recent Driver Data Records for the specified Driver. This operation is only called by other EWD-SPs, and so only returns those Driver Data Records collected by or lodged with the called (server) EWD-SP.

Security	EWD-SP clients must be authenticated using a Gatekeeper Type 3 Certificate, the ABN from which must match a known EWD-SP.
Request Parameters	key – the driver-specific "password" as published by the called EWD-SP in the Driver's record within the EWD Registry.
Request Headers	If-Modified-Since – If not specified, then all recent Driver Data Records are returned. If specified, then only Driver Data Records received by the EWD-SP since the date and time are returned (i.e., a partial set is returned). If there are no such Driver Data Records, then the response code 304 is returned. The value specified in this parameter should be taken from the Last-Modified response header of the previous GET operation and is specified in HTTP date format (e.g., Fri, 05 Oct 2012 06:11:25 GMT). Accept-Encoding – if specified should be gzip (indicating the response should be compressed).
Request Body	None
Response Code	200 – OK 204 – No Content – in the case where there are no Driver Data Records to return and If-Modified-Since was not specified. 304 – Not Modified – in the case where If-Modified-Since was specified, and there are no new Driver Data Records. 403 – Forbidden – in the case that the request parameter "key" is incorrect, or that the request comes from an EWD-SP that does not have an association with the specified Driver. 404 – Not Found – in the case that the Driver is not known to the EWD-SP.
Response Headers	Last-Modified – the date and time when the most recently-received

	Driver Record for this Driver was received by the EWD-SP. This value should be stored for use in later requests (in the If-Modified-Since request header), and for comparison to the value returned from a “GET /drivers” request to the EWD Registry. This header should be returned for response codes 200, 204 and 304, and is specified in HTTP date format (e.g., Fri, 05 Oct 2012 06:11:25 GMT). Content-Type – application/octet-stream – this is specified rather than text/plain so that no software frameworks alter the “carriage-return line-feed” separator characters. Content-Encoding – if specified gzip
Response Body	As specified in Appendix C.

Note: the If-Modified-Since and Last-Modified headers both pertain to the date and time at which Driver Data Records were received (stored) within the EWD-SPs System, and not to the date and time within each Driver Data Record. This heuristic ensures that newly received Driver Data Records are exchanged irrespective of their order of collection.

B.36.2 EWD-SPs shall support the “PUT /drivers/{driver-id}/annotation/{record-date-time}?key={key}”. This operation allows Authorised Officers to lodge Authorised Officer Annotation Records, and optionally to retrieve recent Driver Data Records for review:

a) The request body shall always contain an Authorised Officer Annotation Record, and the “record-date-time” path component shall be derived from the UTC date and time in that Authorised Officer Annotation Record (e.g., a record date and time of “2012-10-12 13:42:52” would map to a record-date-time value of 20121012134252); and

b) The operation shall return recent Driver Data Records held by the EWD-SP, irrespective of which EWD-SP collected those records. The number of days of recent Driver Data Records required is specified within the Authorised Officer Annotation Record *(refer Appendix C)*.

B.36.3 This operation shall be idempotent (as are all operations within this Specification): multiple invocations of this operation with the same data shall all report success, but the Authorised Officer Annotation Record shall be lodged exactly once.

Security	CAS must be authenticated using a self-signed certificate provided by the EWD System Manager, and additionally a signed EWD Authentication Token.
Request Parameters	key – the driver-specific “password” as published by the called EWD-SP in the Driver’s record within the EWD Registry.
Request Headers	X-WSSE – this header provides the EWD Authentication Token, and is used to authenticate the calling Authorised Officer. Content-Type – application/octet-stream – this is specified rather than text/plain so that no software frameworks alter the “carriage-return line-feed” separator characters. Content-Encoding – if specified, should be gzip (indicating the request is compressed).
Request Body	As specified in Appendix C.

Response Code	200 – OK – on success (in the case where 0 days Driver Data Records are to be returned). 204 – No Content – on success (in the case where more than 0 days Driver Data Records are to be returned, but no Driver Data Records are available). 400 – Bad Data – in the case that the submitted data is incorrectly formatted or otherwise invalid. 403 – Forbidden – in the case that the request parameter "key" is incorrect, or that the EWD Authentication Token was missing or invalid. 404 – Not Found – in the case that the Driver is not known to the EWD-SP.
Response Headers	Content-Type – application/octet-stream – this is specified rather than text/plain so that no software frameworks alter the "carriage-return line-feed" separator characters. Content-Encoding – if specified gzip
Response Body	Only provided where recent Driver Data Records are returned as requested within the Authorised Officer Annotation Record being lodged *(refer Appendix C)*.

Note: Authorised Officers will typically invoke this method (via CAS) twice per road-side intercept: once at the commencement (to obtain Driver Data Records), and once at the conclusion to record any outcome.

REMOTE CONNECTION ACCESS FRAMEWORK – USAGE

The success of the RCAF requires EWD-SPs to keep the EWD Registry current.

B.37 EWD-SP Discovery of Other EWD-SPs

B.37.1 Each EWD-SP shall reconcile the list of other EWD-SPs by calling "GET /providers" on the EWD Registry at intervals of 15 minutes.

An EWD-SP shall ensure the list of Drivers is current so that other EWD-SPs can determine if they need the EWD-SP Driver Data Records.

B.38 EWD-SP Maintenance of Driver Associations (with Self)

B.38.1 Each EWD-SP must explicitly register an association between itself and any Driver holding a current Driver Identification and Authentication method issued by itself, or that is active with respect to itself; this is achieved by calling "PUT /drivers/{driver-id}" or "POST /drivers/updated" on the EWD Registry (*refer B.35.2 and B.35.3*);

B.38.2 When updating it's association with a specific Driver in accordance with B.38.1, the EWD-SP shall specify a "key" to be used by other EWD-SPs and Authorised Officers to access that Driver's Data Records:

a) an independent key shall be provided for each Driver; and

b) the key shall comprise 12 randomly generated printable, non-whitespace characters.

B.38.3 Each EWD-SP must explicitly remove its association with any Driver that no longer holds a current Driver Identification and Authentication method issued by itself, and that is no longer active with respect to itself; this is achieved by calling "DELETE /drivers/{driver id}" (*refer 22.4*).

Note: the EWD-SP must not call DELETE /drivers/{driver id} until the driver is no longer active with respect to it, thus ensuring that any recent Driver Data Records are available to other EWD-SPs if required.

B.38.4 Each EWD-SP shall reconcile its Driver associations with those recorded in the EWD Registry at intervals of approximately 24 hours:

a) Valid associations that do not appear in the EWD Registry shall be added in accordance with B.38.1; and

b) Invalid associations that appear in the EWD Registry shall be removed in accordance with B.38.3.

B.38.5 If the EWD-SP Driver association reconciliation fails, the EWD-SP shall retry in 1 hour.

EWD-SPs need to keep current with listings and activity of Drivers who are associated with them and other EWD-SPs. These Drivers may be creating Driver Data Records across multiple EWDs and as such will require EWD-SPs to download records from other EWD-SPs to ensure they maintain a complete 90 days worth of Driver Data Records.

B.39 EWD-SP Discovery of Driver Associations (with other EWD-SPs) and Driver Data Records

B.39.1 Each EWD-SP shall call "POST /drivers/updated" *(refer B.35.3)* on the EWD Registry at intervals of approximately 3 minutes:

a) Each such call shall include details of all Driver's that have not yet been registered with the EWD Registry in accordance with B.38.1;

b) Each such call shall include details of all Driver's for which Driver Data Records have been received since the date and time currently known to the EWD Registry (essentially since the prior call of this operation); and

Note: This does not include records obtained from another EWD-SP.

c) Where this operation would have an empty request body (i.e., no Drivers meet the above criteria), the call shall not be made.

B.39.2 Each EWD-SP shall call "GET /drivers/shared" on the EWD Registry at intervals of approximately 5 minutes.

B.40 EWD-SP exchange of recent Driver Data Records

B.40.1 The EWD-SP shall attempt to download recent Driver Data Records for a given Driver from another EWD-SP where:

a) the Driver is active with respect to the calling EWD-SP (i.e., the calling EWD-SP has collected a Driver Data Record for the Driver in the past 2,184 hours, or the Driver has authenticated to the calling EWD-SP within the past 2,184 hours); and

b) the EWD Registry indicates (through the response to "GET /drivers/shared") that the called EWD-SP has Driver Data Records received more recently than those already held by the calling EWD-SP.

B.40.2 EWD-SPs shall not continuously poll other EWD-SPs for new Driver Data Records; the availability of new Driver Data Records will be advertised through the EWD Registry.

B.40.3 EWD-SPs shall not continuously obtain new Driver Data Records for Drivers that are not currently active.

To ensure that Authorised Officers review of Driver Data Records is transparent to all entities, prior to be able to download Driver Data Records, Authorised Officers will lodge an Authorised Officer Annotation Record. Authorised Officers may lodge further Authorised Officer Annotation Records with comments about the intercept, compliance or directions provided.

B.41 Authorised Officer Annotation

B.41.1 Authorised Officers shall lodge an Authorised Officer Annotation Record with an EWD-SP as a pre-requisite to obtaining Driver Data Records; this is enforced by the design of the PUT /drivers/{driver-id}/annotation operation.

B.41.2 The Authorised Officer Annotation Record is a variable-length record that includes a date and time specified with respect to the Driver's base time zone.

B.41.3 The format of the Authorised Officer Annotation Record is provided within Appendix C.

IAM

To ensure that all entities are using consistent information for translation of GPS coordinates into locations, a map is prescribed.

B.42 IAM*

B.42.1 The EWD-SP shall use the Administrative Boundaries LOCALITY and LOCALITY_POLYGON files of the IAM dataset to determine the <description of the self declaration position>.

B.42.2 The EWD System Manager will be responsible for the supply of the IAM to the EWD-SP, including the supply of updated versions. The IAM will be supplied in one of two formats:

a) DVD; or

b) via the internet as a published Web Feature Service (WFS).

Note: The EWD System Manager aims to release updates for the IAM on a quarterly basis.

DATA INTERCHANGE

Outside of the RCAF, information is required to be exchanged between EWD-SPs, with the EWD System Manager, Authority, Record Keepers and Drivers.

B.43 Provision of Records

B.43.1 EWD Data Records shall be transferred to the EWD System Manager within EWD Data Files in accordance with Appendix F.

B.43.2 Driver Data Records shall be transferred to the Record Keeper within EWD Data Files in accordance with Appendix F.

B.43.3 An EWD Data File shall contain one or more EWD Data Records.

B.43.4 An EWD Data File shall contain one Manifest Record.

B.43.5 The Manifest Record shall be the last record within the EWD Data File.

B.43.6 A Manifest Record shall consist of:

a) Record type;

b) EWD Functional and Technical Specification version number;

c) End UTC date and time;

d) End date and time UTC offset;

e) IVU ID;

f) Number of records;

g) Driver's licence number;

h) Driver's licence issuing Jurisdiction;

i) Start date and time;

j) Start date and time UTC offset; and

k) Random sequence of characters.

B.43.7 The EWD-SP shall populate the Manifest Record in accordance with Appendix F.

B.43.8 The format of the Manifest Record is contained within Appendix C.

B.44 Data interchange – Tier 3

B.44.1 Tier 3 data interchange shall be used by the EWD-SP to communicate and transfer data to the EWD System Manager.

B.44.2 Tier 3 data interchange shall be used by the EWD-SP to communicate to the Authority.

B.44.3 Tier 3 data interchange shall be supported using secure email, FTPS, registered mail and secure web portal.

B.44.4 For the purposes of Tier 3 data interchange via secure email, the EWD-SP shall:

a) utilise an EWD specific email address within its organisation (e.g. ewd@serviceprovidername.com.au);

b) sign transmitted emails;

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.44.5 Secure email shall be digitally signed using the S/MIME secure email format.

B.44.6 Secure email shall not be encrypted.

B.44.7 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 the Certification Authority for which the EWD-SP has sought and gained approval from the EWD System Manager.

B.44.8 For the purposes of Tier 3 data interchange via FTPS, the EWD-SP shall:

a) implement FTPS using SSL and associated security infrastructure;

b) use FTPS for communication with the EWD System Manager for data interchanges as outlined in Appendix D and Appendix E; and

c) provide details of its implementation for the approval of the EWD System Manager.

B.44.9 For the purposes of Tier 3 data interchange via registered mail, the EWD-SP shall appropriately register and file copies of such communications.

B.44.10 For the purposes of Tier 3 data interchange via a secure web portal, the EWD-SP shall:

a) access the secure web portal via an up-to-date web browser or via the EWD-SP System;

b) use the secure web portal for reporting to the Authority and the EWD System Manager (as applicable) malfunctions and possible tampering in relation to the IVU, EWD-SP System and Quality System;

c) use the secure web portal for other activities as they are made available; and

d) provide details of its implementation for the approval of the EWD System Manager.

B.44.11 The Authority and the EWD System Manager will be responsible for the implementation of their Tier 3 data interchange requirements.

B.44.12 EWD-SP requests for approval by the EWD System Manager shall be submitted as a Tier 3 data interchange, with supporting information appropriate for the approval request.

B.44.13 Any EWD System Manager response approving or rejecting a request for approval will be provided as a Tier 3 data interchange.

B.44.14 No verbal communication or representations will be binding between the EWD-SPs and the EWD System Manager and the Authority.

B.45 Data interchange – Tier 4

B.45.1 In the case where the EWD-SP is not keeping Driver Data Records on behalf of the Record Keeper, the EWD-SP and Record Keeper shall agree and implement a Tier 4 Data Interchange capability for exchange of Driver Data Records.

Note: the exact nature of the Tier 4 Data Interchange is not prescribed by this Specification, including whether Driver Data Records are "pushed" or "pulled" from the EWD-SP to Record Keeper.

B.45.2 The Tier 4 Data Interchange capability shall ensure confidentiality, including authentication of the EWD-SP and Record Keeper.

B.45.3 The Tier 4 Data Interchange capability shall ensure that Driver Data Records are received and stored within the Record Keeper in accordance with Appendix F.

B.45.4 The EWD-SP shall ensure Driver Data Records are available through Tier 4 data interchange within 24 hours after receipt of the relevant records, including those collected by other EWD-SPs in the 28 day period prior to any Driver Data Record collected by the EWD-SP.

B.45.5 The EWD-SP shall document, to the satisfaction of the EWD System Manager, their chosen Tier 4 Data Interchange with each Record Keeper.

B.46 Data interchange – Tier 5

B.46.1 Tier 5 data interchange shall be used by the EWD-SP to transfer data to the Driver.

B.46.2 The EWD-SP shall provide a facility for a Driver's SD Records and Authorised Officer Annotation Records to be:

a) viewed away from the IVU and UI in a form that is reasonably capable of being understood by the Driver;

b) available in a form that may be printed by the Driver and reasonably capable of being understood by the Driver; and

c) readily accessible by the Driver.

Note: An example of a facility that may be viewed away from the IVU and UI is a facility on a PC or smart phone.

EWD-SP QUALITY SYSTEM

EWD-SPs will require a robust quality system to ensure that information is suitable to support the intended use of the EWD.

B.47 General*

B.48 Internal and external audits*

B.49 Information security*

B.50 Data access controls*

B.51 Reporting*

EWD-SP QUALITY MONITORING STATION

B.52 EWD Quality Monitoring Station*

AUDIT AND REVIEW OF EWD-SP

The EWD-SP shall be reviewed and audited by the EWD System Manager to determine compliance with this Specification.

B.53 General*

B.54 IVU audit*

B.55 UI audit*

B.56 EWD-SP data audit*

B.57 Position Audit*

RESTRICTION ON POST-CERTIFICATION CHANGE – EWD-SP

To ensure that the EWD-SP's EWD Service continues to be in accordance with this Specification, any change to the EWD-SPs hardware and service shall be approved by the EWD System Manager.

B.58 EWD-SP restriction on post-certification change*

6 REQUIREMENTS FOR THE TYPE APPROVAL OF THE USER INTERFACE (UI)

C. PART C: REQUIREMENTS FOR THE TYPE-APPROVAL OF THE USER INTERFACE (UI)

PHYSICAL AND ENVIRONMENTAL CHARACTERISTICS

C.1 User Interface (UI)*

C.1.1 The UI is used by the Driver to self declare data into the IVU. The UI is inclusive of the hardware, software and cabling and connection leading up to, but not including, the IVU.

Note: the UI can include greater functionality than the requirements specified in this Specification. .

C.1.2 The EWD-SP shall provide the User Interface (UI).

C.2 UI Identifier*

The rationale for UI security seals is part of the tamper evidence requirements presented in RMS 2013.

C.3 Security seals*

As a Driver needs the ability to declare, confirm and annotate SD data, the UI provides this capability directly to the IVU.

C.4 UI capability

C.4.1 The UI shall allow Drivers to enter data.

C.4.2 The UI shall be capable of providing visual indication to the Driver.

C.4.3 The UI shall be capable of accepting data from the IVU.

C.4.4 The UI shall be capable of sending data to the IVU.

C.5 UI tethering

C.5.1 The UI shall be electronically or physically tethered to the IVU.

C.5.2 Removal of the UI from the IVU shall create a Type 1 Alarm Record *(refer A.25)*.

C.6 UI functionality

C.6.1 The UI shall provide a visual indication when the UI is functioning in accordance with this Specification.

C.6.2 The UI shall provide a visual indication when the UI is not functioning in accordance with this Specification.

C.6.3 In determining if the UI is functioning, the EWD-SP shall consider, as a minimum:

a) communication with components of the UI;

b) communication between the IVU and the UI; and

c) capture, storage and transmission of data.

The EWD-SP shall provide, to the EWD System Manager, evidence of compliance from an approved organisation that demonstrates the suitability for use of the UI in heavy vehicles.

C.7 UI suitability for use in vehicles*

C.8 Non-EWD functionality in the UI*

C.9 Documentation*

C.9.1 The EWD-SP shall document, to the satisfaction of EWD System Manager:

a) the UI components and interface; and

b) how the UI determines its functional state and what conditions generate a functional and not functional indication.

DATA ENTRY

C.10 Entering SD Data

C.10.1 The UI shall permit the entry of SD Data.

C.10.2 The UI shall permit the confirmation of SD Data.

C.10.3 The UI shall permit the annotation of SD Data.

C.10.4 The UI shall ensure successful Driver identification and authentication before:

a) permitting the entry of SD data; and

b) undertaking the Driver specific functions of the IVU in accordance with this Specification.

C.10.5 A single successful identification and authentication shall be required to enter and confirm an SD Data work declaration.

C.10.6 A single successful identification and authentication shall be required to enter and confirm an SD Data rest declaration.

C.10.7 The Driver Identification and Authentication method shall be such that it shall be required to be re-entered if no SD Data is entered for a continuous period of three minutes.

The declaration of work and rest by a Driver is defined in the Heavy Vehicle National Law (NTC 2012). The declaration through the UI of SD Data is made and this generates an SD Activity Record. If a Driver elects to annotate the SD Data entered, this is done through the UI of SD Data and this generates an SD Commentary Record. The SD Activity Record is not altered or deleted.

C.11 SD Data

C.11.1 SD Data shall be entered and automatically populated in accordance with Table 1.

C.11.2 Driver confirmation of SD Data may be necessary prior to generation of a SD Activity Record in accordance with Table 1.

C.11.3 Driver annotation of SD Data generates an SD Commentary Record in accordance with Table 1.

Table 1: SD Data

SD Data	Entered and/or Automatically Populated	Driver confirmation necessary prior to generation of SD Activity Record	Driver annotation of SD data generates SD Commentary Record
Date	Automatically by the IVU	YES	YES
Time of declaration	Automatically by the IVU	YES	YES
Date and time UTC offset	Entered (or as a minimum confirmed) by the Driver	YES	NO
Driver's licence number	Automatically by the Identification and Authentication method	YES	Cannot be Annotated
Driver's licence issuing Jurisdiction	Automatically by the Identification and Authentication method	YES	Cannot be Annotated
Driver's name	Automatically by the Identification and Authentication method	YES	Cannot be Annotated
Driver's Base state	Entered (or as a minimum confirmed) by the Driver	YES	YES
Driver's Base Address	Entered (or as a minimum confirmed) by the Driver	YES	YES
Driver's Base Latitude	Populated by the EWD-SP	NO	N/A
Driver's Base Longitude	Populated by the EWD-SP	NO	N/A
Work hours option	Entered by the Driver	YES	NO
Accreditation number (BFM and AFM only)	Entered by the Driver	YES	NO
Record Keeper Address	Populated by the EWD-SP	YES	YES
Record Keeper Address State	Populated by the EWD-SP	YES	YES
Work/Rest status	Entered by the Driver	YES	NO
Use of the EWD	Entered by the Driver	YES	NO
Odometer reading at the time of declaration	Entered by the Driver or automatically by the IVU	YES	NO – if declared by Driver YES – if captured or generated by the IVU
Registration number of the heavy vehicle	Automatically by the IVU	YES	YES
Registration Jurisdiction of the heavy vehicle	Automatically by the IVU	YES	YES
Two-up arrangement status	Entered by the Driver	YES	NO

SD Data	Entered and/or Automatically Populated	Driver confirmation necessary prior to generation of SD Activity Record	Driver annotation of SD data generates SD Commentary Record
Other Driver's licence number	Other Driver's Identification and Authentication method	YES	Cannot be Annotated
Other Driver's license issuing Jurisdiction	Other Driver's Identification and Authentication method	YES	Cannot be Annotated
Other Driver's name	Other Driver's Identification and Authentication method	YES	Cannot be Annotated
Other Driver's work diary number	Other Driver's Identification and Authentication method or manually entered	YES	Cannot be Annotated
Other Driver's work diary issuing Jurisdiction	Other Driver's Identification and Authentication method or manually entered	YES	Cannot be Annotated
Description of self declaration position	Automatically by the IVU	YES	YES
Location state	Automatically by the IVU	YES	YES
Self declaration position latitude	Automatically by the IVU	NO	N/A
Self declaration position longitude	Automatically by the IVU	NO	N/A
Comment text	Entered by the Driver	NO	N/A

A Driver may stop using a vehicle, may start recording work and rest in a WWD or may perform local hours. It is necessary that the Driver declares this disassociation with the EWD.

C.12 Use of the EWD

C.12.1 The SD Data <use of the EWD> shall generate the SD Record field in accordance with Table 2.

Table 2: Use of the EWD

Use of the EWD	Description
0	When the Driver is continuing to use their EWD
1	When the Driver is moving to an WWD after this declaration
2	When the Driver is moving to 100km (local) work after this declaration
3	When the Driver is discontinuing the use of the vehicle

C.12.2 The UI shall be capable of displaying the SD data of the most recent SD Activity Record generated, unless a SD Commentary Record was also generated which would take precedence.

Note: The display of the SD Data allows the Driver to transcribe the information to a WWD should the driver be leaving the EWD.

C.12.3 The IVU shall not permit the Driver to declare a <work/rest status> of 1 (work) in combination with a <use of the EWD> status of 2 (moving to 100km (local) work).

The EWD caters for Drivers under a Two-up driving arrangement. A Driver's use of the UI to enter SD Data will occur after they identify and authenticate themselves.

C.13 Provision for Driver under a Two-up driver arrangement

C.13.1 The IVU shall allow a Driver to work under a two-up driving arrangement.

Note: a change to two-up driving arrangement shall not, in itself, trigger an SD Commentary Record.

C.13.2 When a Driver first declares that they are changing from a solo to two-up driving arrangement, the IVU shall request the second Driver to use their Driver Identification and Authentication method.

C.13.3 The use of the second Driver's Identification and Authentication method shall populate the second Driver's details within the first Driver's SD Activity or SD Commentary Record.

C.13.4 The second Driver's details shall include the Driver's name, licence number and licence issuing Jurisdiction.

Note: It is allowable for the IVU to facilitate simultaneous declarations by both Drivers involved in a two-up arrangement, thus requiring a total of two authentications (one per driver).

C.13.5 The details of the second Driver shall remain populated within subsequent SD Activity Records generated by the first Driver until the first Driver changes their two-up driving arrangement to solo.

C.13.6 The IVU shall allow the Driver to declare they are changing their second Driver whilst remaining under a two-up arrangement.

C.13.7 If a Driver does declare they are changing their second Driver, the IVU shall request the new second Driver's Identification and Authentication method.

C.13.8 The IVU shall allow a Driver to declare that they are driving under a solo driving arrangement by setting the <two-up arrangement status> within the SD Activity or SD Commentary Record to a 0.

C.13.9 Where both Drivers are using the vehicles IVU to make declarations under a two-up driving arrangement, Position Records generated by the IVU shall be allocated to both Drivers as part of their Driver Data Records *(refer A.24).*

Note: The provision of two-up driving arrangement allows for two Drivers to be interacting with the IVU at one time.

DATA DISPLAY

C.14 UTC date and time display

C.14.1 The IVU or UI shall, using the Driver base location, derive an offset to apply to the UTC date and time.

C.14.2 The UI shall display the date and time as a local date and time (i.e. the date and time at the Driver base location) using the UTC date and time and the derived offset.

C.14.3 The UI shall display date and time in whole minutes.

C.14.4 The UI shall display date and time rounded down to the nearest minute.

Note: For example 19:43:01 or 19:43:59 would be displayed as 19:43 or 7:43 PM.

C.15 Driver Fatigue display

C.15.1 The UI shall display Driver Fatigue Information (refer to A.9).

C.15.2 In displaying Driver Fatigue Information, the UI shall provide a notification that the Driver Fatigue Information is provided as advice.

C.16 Authorised Officer display

C.16.1 The UI shall be capable of displaying a Driver's SD Records and Authorised Officer Annotation Records.

C.16.2 When requested, the UI shall display the last 28 days of a Driver's SD Records and Authorised Officer Annotation Records.

Note: this requirement shall require the capability to transfer data from the EWD-SP System to the IVU (refer A.32).

C.16.3 Where there exists a SD Commentary Record, the UI shall display the SD Commentary Record and not the preceding SD Activity Record.

C.16.4 For each SD Record, the UI shall display the:

a) Driver's name;

b) Driver's licence number and the Jurisdiction where the licence was issued;

c) Vehicle Registration;

d) Address of Driver base;

e) Address of Record location (physical location of where the Driver Data Records are stored);

f) Time and date of the declaration (rendered in the Driver's base local time);

g) Work/rest status (work, rest);

h) Period of the work/rest;

Note: the period for the most recent work/rest activity shall be blank.

i) Use of the EWD status;

j) Description of self declaration position;

k) Odometer;

l) Work hours option;

m) BFM or AFM accreditation number;

n) If the Driver becomes a two-up Driver,

i) the other Driver's name;

ii) the other Driver's Driver licence number; and

iii) the other Driver's work diary number; and

o) Comments (if any).

C.16.5 For each Authorised Officer Annotation Record, the UI shall display the:

a) Date and time (rendered in the Drivers base local time); and

b) Authorised Officer Annotation text.

C.16.6 The IVU shall display records in Arial font and be no smaller than 12 font.

C.16.7 The IVU shall display records in reverse chronological order with the most recent record at the top of the screen.

C.16.8 An example of the Authorised Officer display is contained within Appendix G.

DATA TRANSFER

C.17 SD Record Transfer

C.17.1 The UI shall provide a visual indication of the date and time that the last Driver's SD Record was generated.

C.17.2 The UI shall provide a visual indication of the date and time that the last Driver's SD Record was transferred to the EWD-SP System.

PROVISION OF UI FOR TYPE-APPROVAL

C.18 UIs for Type-approval

C.18.1 To facilitate Type-approval testing, two UIs to be type-approved shall be provided to the EWD System Manager as per Appendix D.

Appendix A Acronyms and Definitions*

Term	Definition
ABN	Australian Business Number.
AFM	Advanced Fatigue Management providing the most flexible work and rest hours option for applicable regulated heavy vehicle Drivers.
Applicant	A party which has applied for certification as an EWD-SP.
Authentication	The verification of someone's or something's declared identity.
Authority	As the context so requires it, references the EWD Regulatory Framework Owner, State Road Transport Authorities and/or the Police.
Authorised Officer	A person who holds office under the law as an authorised officer
BFM	Basic Fatigue Management providing more flexible work and rest hours option for applicable regulated heavy vehicle Drivers.
Certification	The formal confirmation that an Applicant has satisfied all the requirements for appointment as an EWD-SP.
driver ID	The EWD-SP shall ensure interoperable Driver identification for the purpose of achieving RCAF usage for other EWD-SPs and Authorised Officers and the organisation of records for data transfer defined in Appendix F.
EWD	An EWD is an approved electronic system for recording work and rest.
EWD Data	The electronic data collected by the EWD-SP within the EWD.
EWD Functional & Technical Specification	The Specification defining the functional and technical requirements which a party applying for certification as an EWD-SP must satisfy with respect to its hardware, software and systems.
EWD Reference System	The reference system used by the EWD System Manager for GPS quality testing of IVUs.
EWD Registry	The electronic storage of Drivers' identities and record address used within the Remote Connection Access Framework.
EWD Regulatory Framework Owner	The entity responsible for managing legislation and policy implementation governing the EWD.
EWD Service Provider (EWD-SP)	A party which is certified by the EWD System Manager as suitable to provide EWD Services.
EWD Services	The services that an EWD-SP provides in accordance with this Specification.
EWD System Manager	The manager responsible for certification, re-certification, audit and operations of the EWD-SPs and associated technical ICT EWD aspects.
EWD Vehicle	A vehicle operating with an EWD.
EWD-SP System	The EWD-SP's hardware and software, excluding the IVU and UI used in the collection, processing, testing, storage and reporting of EWD Data.

Term	Definition
GDA94	The Geocentric Datum of Australia 1994 (GDA94) is a coordinate system for Australia that is compatible with coordinates produced by the Global Positioning System (GPS). GDA94 supersedes the Australian Geodetic Datum coordinate systems AGD66 and AGD84.
Global Positioning System (GPS)	A form of GNSS controlled by the US Department of Defense.
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.
Driver Identification and Authentication method	The method used by the Driver to identify and authenticate their identity to the IVU.
In-Vehicle Unit (IVU)	A Type-approved telematics unit installed, operated and maintained by the EWD-SP which monitors parameters.
IVU Data	The raw data collected by the IVU.
IVU Data Records	Position, Type 1 Alarm and SD Records generated by the IVU.
Level 3 Type-approved IVU	A Type-approved IVU with no ability to record SD Records to a mass storage device.
Level 4 Type-approved IVU	A Type-approved IVU with the ability to record SD Records to a mass storage device.
Local time	Time at a particular locale.
NeAF	National electronic Authentication Framework – an Australian Government standard for identity authentication.
Position Record	A record generated and stored in the IVU.
Quality Monitoring Station (QMS)	Equipment used by the EWD-SP and the EWD System Manager to provide a log of the output of a Type-approved IVU and UI with respect to its accuracy and integrity.
Remote Connection Access Framework (RCAF)	A system which allows for exchange of Driver Data Records between EWD-SPs, and for Authorised Officers to both obtain Driver Data Records (in the context of a road-side intercept) and lodge an Authorised Officer Annotation Record.
SD Data	Data which is self declared by the Driver.
SD Record	A record generated and stored in the IVU whenever a Driver self declares SD Data.
Self Declaration	The self declaration of data by the Driver of a heavy vehicle.
SSL	Secure Sockets Layer is an IT cryptographic communications protocol, predominantly used to provide secure communications on the internet.
Standard hours	The Basic work and rest limit option for applicable regulated heavy vehicle Drivers.
Tamper	Conduct towards any system (including without limitation, the IVU) which is intended to prevent the system from functioning correctly.
Transport Operator (TO)	A Transport Operator of one or more vehicles.

Term	Definition
Type 1 Alarm Record	A record generated and stored in the IVU as a result of testing IVU data against pre-defined criteria. Type 1 Alarm Records equate to Alarm Records within (TCA 2013).
Type 2 Alarm	An EWD-SP System response resulting from testing data transmitted from the IVU against pre-defined criteria. Type 2 Alarms equates to Alarms within (TCA 2013).
Type 2 Alarm Record	A record generated and stored in the EWD-SP System as a result of testing IVU data against pre-defined criteria.
User Interface (UI)	A Type-approved interface unit installed, operated and maintained by the EWD-SP.
UTC	Coordinated Universal Time – the standard time used internationally to regulate clocks and time.
Vehicle position	The latitude and longitude position of a vehicle, in decimal degrees to 0.00001 degrees (GDA94).
WGS84	The World Geodetic System 1984 (WGS84) is a coordinate system for the world that is compatible with coordinates produced by the Global Positioning System (GPS). WGS84 was last updated in 2004 and supersedes the World Geodetic Systems coordinate systems WGS72, WGS66 and WGS60.
Work hours option	Option under the National Heavy Vehicle Law which defines the maximum work and rest limits (standard hours, solo hours of a bus, BFM hours, AFM hours or hours specified in a work/rest hours exemption).
Working day	Any period of 24 consecutive hours, commencing and ending at any time but interruptible by Saturdays, Sundays and Public Holidays.
WWD	Written Work Diary means a written work diary issued to the Driver of a fatigue-regulated heavy vehicle by the Authority.
XML	Extensible Markup Language is a programming language which facilitates the sharing of documents and data across different systems, particularly systems connected via the internet.

Appendix B Remote Connection Access Framework (RCAF) explanatory notes

B.1 Architectural overview

The RCAF allows for exchange of Driver Data Records between EWD-SPs, and for Authorised Officers to both obtain Driver Data Records (in the context of a road-side intercept) and lodge an Authorised Officer Annotation Record.

This architecture has been designed to accommodate the following architectural quality attributes:

- *Simplicity* – the architecture is simple and predicated on simple, commodity technologies. It should be feasible for EWD-SPs to implement the architecture with minimal cost and risk;
- *Scalability* – the architecture should scale to tens of thousands of Drivers, assuming that only a small percentage of those Drivers operate vehicles fitted by multiple EWD-SPs during any period of approximately 28 days; and
- *Privacy* – the architecture exposes only the bare minimum of an EWD-SP's commercial activity to other EWD-SPs (i.e., its competitors), does not allow Driver Data Records to touch the EWD Registry, and minimises the visibility of Driver Data Records to EWD-SPs where the Driver is not actively operating vehicles fitted with their equipment.

B.2 Use cases

B.2.1 EWD-SP discovers other EWD-SPs

Each EWD-SP requires a list of other EWD-SPs for the purposes of authentication prior to the exchange of any information. The list of EWD-SPs is maintained in the RCAF by periodically (e.g., every 15 minutes) communicating with the EWD Registry; and

The result list of EWD-SPs is subsequently reconciled against the list already held by the EWD-SP; new EWD-SPs are added, and those no longer known by the EWD Registry removed; there may be some "housekeeping" associated with the removal of an EWD-SP (e.g., the removal of associations with Drivers within the EWD-SP's own system).

B.2.2 EWD-SP maintains Driver associations (with Self)

Each EWD-SP must ensure that the EWD Registry accurately reflects all current (and only current) associations between the EWD-SP and Drivers. This involves registering and deleting associations within the EWD Registry. As the RCAF is a distributed system, the EWD-SP must periodically reconcile the associations.

The association between EWD-SP and Driver within the EWD Registry should be removed when there is no longer any relationship between the EWD-SP and the Driver.

B.2.3 EWD-SP discovers Driver associations and Driver Data Records with other EWD-SPs

Once an EWD-SP has registered an association with a given Driver, the EWD-SP will commence collection of Driver Data Records for that Driver; this results in the Driver becoming active with the EWD-SP. As Driver Data Records are collected by the EWD-SP from the IVU, the EWD-SP is required to announce the availability of those Driver Data Records to other EWD-SPs: the other EWD-SPs can then download those Driver Data Records as required for forwarding to the Record Keeper, and for performing EWD-related processing within their back-office and IVUs.

It is important to understand that EWD-SPs only announce the availability of Driver Data Records collected by their own IVUs, or lodged directly with them by an Authorised Officer; EWD-SPs do not announce the availability of Driver Data Records downloaded from other EWD-SPs.

B.2.4 EWD-SP obtains Driver Data Records from another EWD-SP

Each EWD-SP must obtain recent Driver Data Records collected by another EWD-SP for Drivers that are active with respect to itself (e.g., to provide to the Record Keeper). Every 5 minutes the EWD-SP invokes a request through the RCAF. As a result, the EWD-SP may identify Drivers that are active with respect to itself, and that have recent Driver Data Records with another EWD-SP:

EWD-SPs should not, and do not need to, continuously poll other EWD-SPs for new Driver Data Records; the availability of new Driver Data Records will be advertised through the EWD Registry.

EWD-SPs should not, and do not need to, continuously obtain new Driver Data Records for Drivers that are not currently active.

B.2.5 Authorised Officer reviews Driver Data Records

This section describes how the RCAF supports the review of Driver Data Records by an Authorised Officer using the Compliance Assessment Software (CAS). CAS enables to Authorised Officer to interface to the RCAF and review Driver Data Records for compliance.

Having interacted with the EWD Registry, an Authorised Officer obtains the recent Driver Data Records for the Driver from the EWD-SP as the RCAF does not store Driver Data Records as part of the privacy and security framework of the EWD. This operation takes as input an Authorised Officer Annotation Record, the purpose of which is to act as an audit record, and returns as output recent Driver Data Records (for the number of days specified within the Authorised Officer Annotation Record). In making this call, the Authorised Officer authenticates to the EWD-SP.

The road-side intercept then proceeds, with the Authorised Officer able to analyse the Driver Data Records. At the conclusion of the review, the Authorised Officer may generate a second Authorised Officer Annotation Record.

Appendix C Record Format*

C.1 Format*

The format of each record shall be provided by the EWD System Manager.

C.2 SD Record*

The format of the SD Record shall be provided by the EWD System Manager.

C.3 Position Record*

The format of the Position Record shall be provided by the EWD System Manager.

C.4 Type 1 Alarm Record*

The format of the Type 1 Alarm Record shall be provided by the EWD System Manager.

C.5 Type 2 Alarm Record*

The format of the Type 2 Alarm Record shall be provided by the EWD System Manager.

C.6 Authorised Officer Annotation Record

The format of the Authorised Officer Annotation Record shall be provided the EWD System Manager.

C.7 Manifest Record*

The format of the Manifest Record shall be provided by the EWD System Manager.

Appendix D Requirements for the provision of IVUs to the EWD System Manager*

Appendix E Requirements for the provision of UIs to the EWD System Manager*

Appendix F Data requirements*

F.1 General requirements

This appendix describes a mechanism for storing EWD Data Records in files, and organising those files into a directory structure. This storage mechanism is used in a number of contexts within the EWD architecture.

F.1.1.1 EWD Data Records shall be transferred in EWD Data Files; each EWD Data File shall contain one or more EWD Data Records.

F.1.1.2 An EWD Data File shall contain EWD Data Records in the format described in Appendix C**.**

F.1.1.3 With the exception of EWD Data Files copied to the mass storage device, each EWD Data File shall contain one Manifest Record.

F.1.1.4 The Manifest Record shall be the last record in the EWD Data File.

F.1.1.5 If (and only if) directed to do so, EWD Data Files shall be compressed.

F.1.1.6 If (and only if) directed to do so, EWD Data Files shall be digitally signed to form an EWD Signature File:

a) Where the EWD Data File is compressed, the digital signature shall be of the uncompressed (i.e., original) file;

b) The EWD Signature File shall contain a BASE 64 encoded Cryptographic Message Syntax (CMS) digital signature of the EWD Data File.

c) The EWD Signature File shall be stored alongside (i.e., in the same directory) as the signed (i.e., original) file.

F.1.1.7 EWD Data Files, and (where relevant) EWD Signature Files shall be stored in a directory structure that is organised by driver ID (*refer B.27*) or by IVU ID *(refer A.2)*:

F.2 Application to copy SD Records and Authorised Officer Annotation Records to a mass storage device*

F.2.1.1 SD and Authorised Officer Annotation Records shall be copied in a directory structure (supplied by EWD System Manager).

F.3 Application to transfer EWD Data Records to the EWD System Manager*

F.3.1.1 EWD Data Files shall be transferred in the directory structure under the driver ID and under the IVU ID (as appropriate).

F.4 Application to transfer Driver Data Records to a Record Keeper*

F.4.1.1 EWD Data Files shall be transferred in the directory structure under the drivers ID and under the IVU ID.

F.4.1.2 Each EWD Data File shall contain all Driver Data Records generated by, or annotated to, the EWD-SP System on a given UTC date for a specific Driver.

F.4.1.3 Each EWD Data File shall contain Driver Data Records received by the EWD-SP System during the arbitrary period of time that has elapsed since the prior EWD Data File was created:

a) A new EWD Data File shall not (and cannot) be created until at least one EWD Record has been received since the creation of the previous EWD Data File;

b) Where EWD Data Records have been received, a new EWD Data File shall be created at least once per UTC date; and

c) New EWD Data Files should not be created more than once every 15 minutes.

F.4.1.4 The <UTC start date and time> and <start date and time UTC offset> within each EWD Data File's Manifest Record shall be:

a) where a previous EWD Data File has been created for that Driver, the UTC date and time and offset when the last Driver Data Record within that previous EWD Data File was received by the EWD-SP; or

b) where no previous EWD Data File has been created for that Driver, the UTC date and time "19700101000000" (i.e., midnight on 1st January 1970).

F.4.1.5 The <UTC end date and time> and <end date and time UTC offset> within each EWD Data File's Manifest Record (and so the date and time component of the EWD Data File's name) shall coincide with the UTC date and time and UTC offset when the last Driver Data Record within the EWD Data File was received by the EWD-SP.

Note: the UTC offset referenced in F.4.1.4 and F.4.1.5 shall be the UTC offset at the location of the EWD-SP.

F.4.1.6 Each EWD Data File shall be digitally signed by the EWD-SP in accordance with F.1.1.6, and using a Gatekeeper Type 3 certificate.

Appendix G Authorised Officer Display Example

Driver: John Smith		**Licence number: 123456789**						**Issuing state: VIC**			**Registration: XWY123**	
Date and time	Work /Rest	Period	Use of the EWD	Hours option	Accred number	Odometer	Location	Other Driver's				
								Name	Licence no	Licence state	Work diary number	Comment
Sun 30 Sep 2012 17:19	Rest		0	BFM Solo	12345678	456670	Benalla					
Sun 30 Sep 2012 14:25	Work	2h 54m	0	BFM Solo	12345678	456525	Seymour					
Sun 30 Sep 2012 13:58	Rest	0h 27m	0	BFM Solo	12345678	456525	Seymour					
Sun 30 Sep 2012 11:00	Work	2h 58m	0	BFM Solo	12345678	456325	Brunswick					
Sun 30 Sep 2012 9:45	Rest	1h 15m	0	BFM Solo	12345678	456325	Brunswick					
Sun 30 Sep 2012 9:43	Reviewed Driver work diary at Brunswick and found non-compliance requiring John to stand down for 1 hour – Officer 1234											
Sun 30 Sep 2012 9:32	Work	0h 13m	0	BFM Solo	12345678	456320	Brunswick					

Appendix H Driver Fatigue Information

H.1 Information provided to the Driver

H.1.1.1 Information provided by the EWD-SP to the Driver through the IVU/UI shall include as a minimum (and as updated from time to time):

a) the time of the next required rest break and the minimum period of rest that must be taken before commencing work for the Driver's current work hours option;

b) where the rest required is a 7 hour rest break, whether the rest must also include night rest; and

c) where the rest to be taken is night rest and whether the rest required to be taken is one or more night rests.

Appendix I Requirements for the Record Keeper

I.1 Data backup and archiving

I.1.1.1 The Record Keeper shall document and have in place, appropriate procedures for daily backup of Driver Data Records and any supporting applications required to support the receipt or backup of Driver Data Records.

I.1.1.2 The Record Keeper shall test its procedures for Driver Data Record retrieval from backup storage:

a) for partial Driver Data Record retrieval, no less frequently than once every three months; and

b) for full Driver Data Record retrieval, no less frequently than once every 12 months.

I.1.1.3 Full system backups of Driver Data Records, applications and operating system shall be performed before and after any hardware or software changes.

I.1.1.4 The Record Keeper shall document and have in place, appropriate procedures for the archiving and retrieval of Driver Data Records.

I.1.1.5 The Record Keeper shall maintain weekly archives of all Driver Data Records, for a period of three years from the date received.

I.1.1.6 The Record Keeper shall, at the expiration of the respective periods referred to in I.1.1.5 destroy the archived Driver Data Records.

I.1.1.7 All archived Driver Data Records shall be stored at two separate places:

a) One copy shall be kept at a location that allows for immediate access; and

b) One copy shall be kept at a secure off-site facility (within five working days of archiving the Driver Data Records).

I.1.1.8 The Record Keeper shall perform a Driver Data Record retrieval of the archived Driver Data Records within five working days of being requested to do so by the EWD System Manager.

I.1.1.9 The Record Keeper shall test its procedures for archive retrieval no less frequently than once every 3 months and shall document its test results.

I.2 Data interchange – Tier 4

I.2.1.1 In the case where the EWD-SP is not keeping Driver Data Records on behalf of the Record Keeper, the Record Keeper and EWD-SP shall agree and implement a Tier 4 Data Interchange capability for exchange of Driver Data Records.

I.2.1.2 The Tier 4 Data Interchange capability shall ensure confidentiality, including authentication of the EWD-SP and Record Keeper.

I.2.1.3 The Tier 4 Data Interchange capability shall ensure that Driver Data Records are received and stored within the Record Keeper in accordance with Appendix F.

I.2.1.4 The Record Keeper shall document, to the satisfaction of the EWD System Manager, their chosen Tier 4 Data Interchange with each Record Keeper.

I.3 Data access controls

I.3.1.1 The Record Keeper shall adopt a risk-based data access control policy, and monitor for compliance with the policy.

For example: the Australian Government Information Security Manual contains a suitable risk-based data access control policy.

I.3.1.2 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.

Note: To minimise unauthorised access to user data, the Record Keeper, where possible, store a hashed version of the data rather than the actual data, e.g. password details.

I.3.1.3 The Record Keeper shall periodically review the access rights of users against their job roles to ensure that access does not continue after it becomes inappropriate.

I.4 Information security

I.4.1.1 The Record Keeper shall be required to implement an Information Security Management System (ISMS) necessary for the on-going operation of the system.

I.4.1.2 The ISMS shall provide assurance that the risks to evidentially-significant information will be managed appropriately by the users of the system.

I.4.1.3 The ISMS shall be in alignment with AS/NZS 27001 and implement control mechanisms in accordance with AS/NZS 27002. The ISMS shall include, as a minimum, the management of:

a) physical and environmental security;

b) access control, especially access from privileged users and the mechanisms to provide controlled access to functions and information based upon a user's legitimate tasks on a need-to-know basis;

c) network and communications security; and

d) incident detection and management.

I.4.1.4 The Record Keeper's system external interfaces shall be protected against intrusion and attack, including, without limitation, the use of effective and up-to-date firewall and anti-virus and intrusion detection software.

I.4.1.5 The Record Keeper shall ensure that its ISMS meets the confidentiality requirements of the relevant state based legislated privacy principles.

I.4.1.6 The Record Keeper shall monitor and review the information security practices in general, against documented objectives and targets.

I.5 Authorised Officers

I.5.1.1 An Authorised Officer will have access to Driver Data Records stored by the Record Keeper as part of their compliance and enforcement function.

I.5.1.2 The Authorised Officer will use the Compliance Assessment Software (CAS) to perform I.5.1.1.

I.5.1.3 The Authorised Officer will provide the Record Keeper a completed form that will contain the summary details of the compliance and enforcement function performed.

I.6 Record Keeper Audit

I.6.1.1 The Record Keeper shall make available their record keeping system for audit of compliance in accordance with the requirements of this appendix by the EWD System Manager.

Note: The audit of the record keeping system is independent to the assessment of a Driver or Drivers compliance with relevant fatigue regulations.