

Interim Guidelines for Electronic Road User Charges Management Systems

November 2010



Ministry of **Transport**
TE MANATŪ WAKA



NZ **TRANSPORT AGENCY**
WAKA KOTAHI

Contents

Introduction	3
Roles and responsibilities	4
PART ONE:	6
APPLYING FOR AN APPROVAL.....	6
Electronic distance recorder approval process.....	7
PART TWO:.....	13
OUTCOME-BASED PERFORMANCE REQUIREMENTS	13
Introduction	14
Electronic distance recorder	16
Communications	23
Back-end system.....	24
Data to information layer	30
PART THREE:	36
TERMS AND CONDITIONS THAT THE SECRETARY MAY APPLY	36
Terms and conditions of approval	37
Appendix one: glossary.....	41

Introduction

On 1 January 2010 the Road User Charges Regulations (No 2) 2009 came into force. These regulations enable approved electronic distance recorders to be used for measuring distance travelled (for road user charges (RUC) purposes) and the electronic display of RUC licences.

The purpose of these guidelines is to provide information on the process of becoming an electronic RUC service provider, and to provide an alternative voluntary option to paper licenses and hubodometers.

These guidelines are interim and in the longer term the performance requirements contained here may be replaced with the introduction of more detailed standards.

The Ministry of Transport (the Ministry) and the NZ Transport Agency (the NZTA) welcome comment on the guidelines. Feedback should be directed to rucguidelines@transport.govt.nz.

The document follows the following format:

- Part one sets out the process for applying for an approval from the Secretary for Transport (the Secretary)
- Part two sets out the (largely) outcome-based performance requirements on which the testing process is based
- Part three provides an indication of the terms and conditions that may accompany the Secretary's approval.

Legal authority

The RUC system is operated under the [Road User Charges Act 1977](#) (the Act) and the [Road User Charges Regulations 1978](#) (the Regulations) including the 2009 amendments to those regulations. You should familiarise yourself with this legislation before contacting the NZTA, and seek legal advice if necessary.

Waiver

These guidelines are not prescriptive. They are intended to provide an overview of the process for becoming an electronic RUC service provider and the obligations of applicants and other participants in the system.

As this is a new procedure which involves the introduction of new technology, the technical information required from applicants and the content of this document will be subject to change.

It is your responsibility to ensure that your methodology does not infringe any existing intellectual property rights. The approval process administered by the NZTA and MOT does not involve the consideration of such matters and the MOT and the NZTA bear no responsibility for patent infringement arising from an approval of an electronic distance recorder.

Roles and responsibilities

This section describes the roles of the various participants in an electronic RUC system.

The Ministry of Transport

The Ministry administers the RUC legislation and is responsible for:

- providing policy advice to the government on changes to RUC legislation
- providing advice to the Secretary on applications for approval of electronic distance recorders
- monitoring improvements in technology.

The Secretary has overall statutory responsibility for the RUC system and is responsible for:

- granting approvals for electronic distance recorders under regulation 6A of the Regulations
- setting the terms and conditions of an approval
- varying or revoking existing approvals.

The NZ Transport Agency

The NZTA administers the RUC system under delegated authority from the Secretary and is responsible for:

- the collection of RUC, including the appointment of agents to act on its behalf
- auditing and investigating transport operators in order to assess RUC compliance and, when necessary, recover outstanding RUC
- managing the process of testing electronic distance recorders
- providing a recommendation to the Secretary on applications for approval of electronic distance recorders
- auditing electronic service providers to ensure compliance with agency agreements and the terms and conditions of the Secretary's approval
- monitoring improvements in technology.

The New Zealand Police

The New Zealand Police (the Police) enforce the RUC regime through the criminal justice system.

The Police are responsible for:

- inspecting each proposed electronic distance recorder as part of the NZTA testing process and providing an endorsement that it meets their needs for roadside enforcement of RUC

- roadside enforcement, usually through roadside inspections and the issuing of offence notices.

Electronic service providers

Electronic service providers are private sector companies that:

- have been authorised as agents by the NZTA
- have an electronic distance recorder approved by the Secretary.

These companies may also provide commercial services (e.g., fleet-tracking) to transport operators in addition to RUC functions.

As an electronic service provider you are responsible for:

- development or provision of the electronic distance recorder
- issuing electronic RUC licences and forwarding revenue to the NZTA
- ensuring that electronic RUC services are performed in accordance with the terms of your agency agreement with the NZTA and the Secretary's approval of your electronic distance recorder
- ongoing management of the installation, repair and exception resolution process (including monitoring attempts to tamper with the device) for your electronic distance recorders
- ensuring that transport operators have 100% access to records you hold on their behalf
- complying with RUC legislation
- obtaining legal advice to ensure avoiding the infringement of other's intellectual property rights.

Transport operators

A transport operator is an operator of one or more heavy vehicles.

In the context of electronic RUC, transport operators are responsible for:

- engaging the services of an electronic service provider
- purchasing appropriate RUC licences
- ensuring that each of their vehicles are fitted with a functioning, approved distance recorder
- notifying the NZTA of a change of distance recorder (although in some instances this process may be undertaken by an electronic service provider on their behalf)
- ensuring compliance with RUC legislation.

**PART ONE:
APPLYING FOR AN APPROVAL**

Electronic distance recorder approval process

Application requirements

All applications for approval of an electronic distance recorder must be made to the Secretary. The Secretary's approval is granted under regulation 6A of the Regulations which provides that:

- the Secretary must be satisfied that the electronic distance recorder is fit for the purpose
- an approval may be subject to terms and conditions imposed at the discretion of the Secretary (refer to Part three of these guidelines)
- an approval may be varied or revoked by the Secretary by notice in writing to the electronic service provider to whom the approval was granted.

To commence the approvals process, please complete the application form found in this section and forward it to the NZTA (details provided below under NZTA contacts). If you are applying for approval of an electronic distance recorder for a prime mover and a trailer you will need to complete a separate application form for each device.

Guidance on how to meet the application requirements is set out below. A diagrammatic overview of the process is provided at the end of this section.

Becoming an agent of the NZTA

As an electronic distance recorder is required to electronically display RUC licences (issued by an electronic service provider) the first step to gaining an approval is to become an agent of the NZTA, authorised to issue RUC licences electronically.

To register your interest in becoming an agent of the NZTA, please send a confidential business proposal to the NZTA Agencies Relationship Manager (details on page 10 under NZTA contacts). The business proposal must include:

- a description of the corporate entity - background picture, strategic direction, financial overview (size, stability), customer base (numbers, size and types of organisations) and current services offered
- a description of the proposed service for administering RUC, including the business model and licensing process
- an outline of the expected customer base and a qualified estimate of the number of RUC licences expected to be issued per annum
- a description of how the provision of this service will benefit the performance of the RUC system
- a nominated contact for any further discussions.

An authorisation to issue RUC licences electronically will be contingent on the security of your systems, integration with the NZTA network and your ability to perform the services of selling and issuing licences to the NZTA's satisfaction.

Self-testing

To demonstrate the accuracy and reliability of your device, you will need to demonstrate that you have completed your own comprehensive testing¹ and make the results available to the NZTA.

Fit-for-purpose

In general terms, fit for purpose means that the electronic distance recorder and its back-end application should be of acceptable accuracy, reliability and security.

Further guidance on what is considered to be fit-for-purpose is provided in Part two of this document.

Factory acceptance testing plan

To assist with independent testing of the electronic distance recorder, you will need to design and supply a factory acceptance testing plan. This plan will be used as a starting point by the NZTA's engineering specialist; however any tests that they deem appropriate to assess the suitability of the electronic distance recorder may be undertaken.

Independent security review

To ensure your device and associated back-end have an appropriate level of security, you will need to develop a security plan covering electronic and physical security and undergo an independent security review by an industry-recognised, information-systems security specialist. The NZTA must be satisfied with the contents of the report following this review.

Aspects of this process may overlap with the requirements for becoming an agent of the NZTA, but you will not be expected to duplicate the review requirements in such instances.

To prevent any loss of revenue that could result from adjustments to electronic distance recorders, you will need to explain to the NZTA what protocols and restrictions are in place to prevent any alteration of the distance recorder reading, including the effect of any exceptions resolution undertaken by you or your authorised installers and repairers and, when necessary, how you will notify the NZTA authorised representative.

¹ This should include a trial where your electronic distance recorder is fitted as a secondary device to heavy vehicles in a working environment.

NZTA testing process

You will need to provide at least three devices of the type and model for which approval is being sought. In supplying these, you accept that these devices may be damaged during the testing process. The devices will become the property of the NZTA, though the NZTA may return them to you, by mutual agreement.

As part of the testing process you will need to provide the NZTA's authorised representative with appropriate online access to monitor the performance of the device. You will also need to provide access to all relevant data captured during the independent testing phase.

Police demonstration

In order to ensure that an electronic distance recorder is accessible for the purpose of a roadside inspection, you must provide the Police with a demonstration of a working model when requested, along with a simple user guide that explains how your device functions.

No recommendation for approval can be made until the Police have confirmed with the NZTA that they are satisfied with the device. The NZTA will facilitate this process and will need to be contacted first to arrange a demonstration with the Police.

Installation and repair

You will need to develop fitting, testing and repair specifications that can be provided to your authorised installers and repairers. You will need to supply the NZTA with a list of your authorised installers and repairers and advise what access these parties will have to the electronic distance recorder and associated back-end applications.

Costs

You will be responsible for all costs associated with testing. These include the costs incurred in the testing undertaken by a third party on behalf of the NZTA. As an indication, the testing of an electronic distance recorder is expected to be less than \$10,000 but this could vary depending on the complexity of the device. You will be advised of the cost before testing takes place, and you will need to make payment before testing begins.

The decision

On completion of the NZTA testing process and a police demonstration, the NZTA will forward your application to the Secretary, along with a recommendation as to whether the NZTA believes the device is fit-for-purpose as an electronic distance recorder.

The Secretary will make a decision on the approval, taking into account the information provided by the NZTA and any other information he/she considers relevant to the request.

You will be informed in writing of the Secretary's decision. Any approval from the Secretary will be subject to terms and conditions (see Part three of this document for terms and conditions that the Secretary may apply).

NZTA contacts

To apply to become an NZTA agent authorised to issue RUC licences please contact:

Chris Taylor
Manager Agencies

DD 06 953 6016
Email: chris.taylor@nzta.govt.nz

Level 3, 43 Ashley Street
PO Box 1947
Palmerston North 4440

To apply for approval of an electronic distance recorder or for information about the approvals process for electronic distance recorders please contact:

Bryan Talbot
Senior Technical Advisor

DD 04 894 5062
Email: bryan.talbot@nzta.govt.nz

Level 9, PSIS House
20 Balance Street
P O Box 5084
Lambton Quay
Wellington 6145

The NZTA authorised representative for electronic RUC management systems is:

Delaney Myers
Commercial Operators Policy Manager

DD 06 953 6026
Email: delaney.myers@nzta.govt.nz

Level 3, 43 Ashley Street
PO Box 1947
Palmerston North 4440

APPLICATION FOR APPROVAL OF ELECTRONIC DISTANCE RECORDER

Under Regulation 6A(1) of the Road User Charges Regulations 1978, the applicant requests that the Secretary for Transport approve the..... (device brand name/make/model) as an electronic distance recorder.

(Application to be sent to the NZ Transport Agency on behalf of the Secretary for Transport)

Applicant name (company):	
Contact name and position:	
Phone number:	
Email:	
Postal address:	
Physical address:	

The applicant is an NZTA agent authorised to issue RUC licences Yes/No

The applicant has completed and made available to the NZTA:

- documented self-testing for reliability and accuracy Yes/No
- a factory acceptance testing plan Yes/No
- an independent security review Yes/No

The applicant has made provision for:

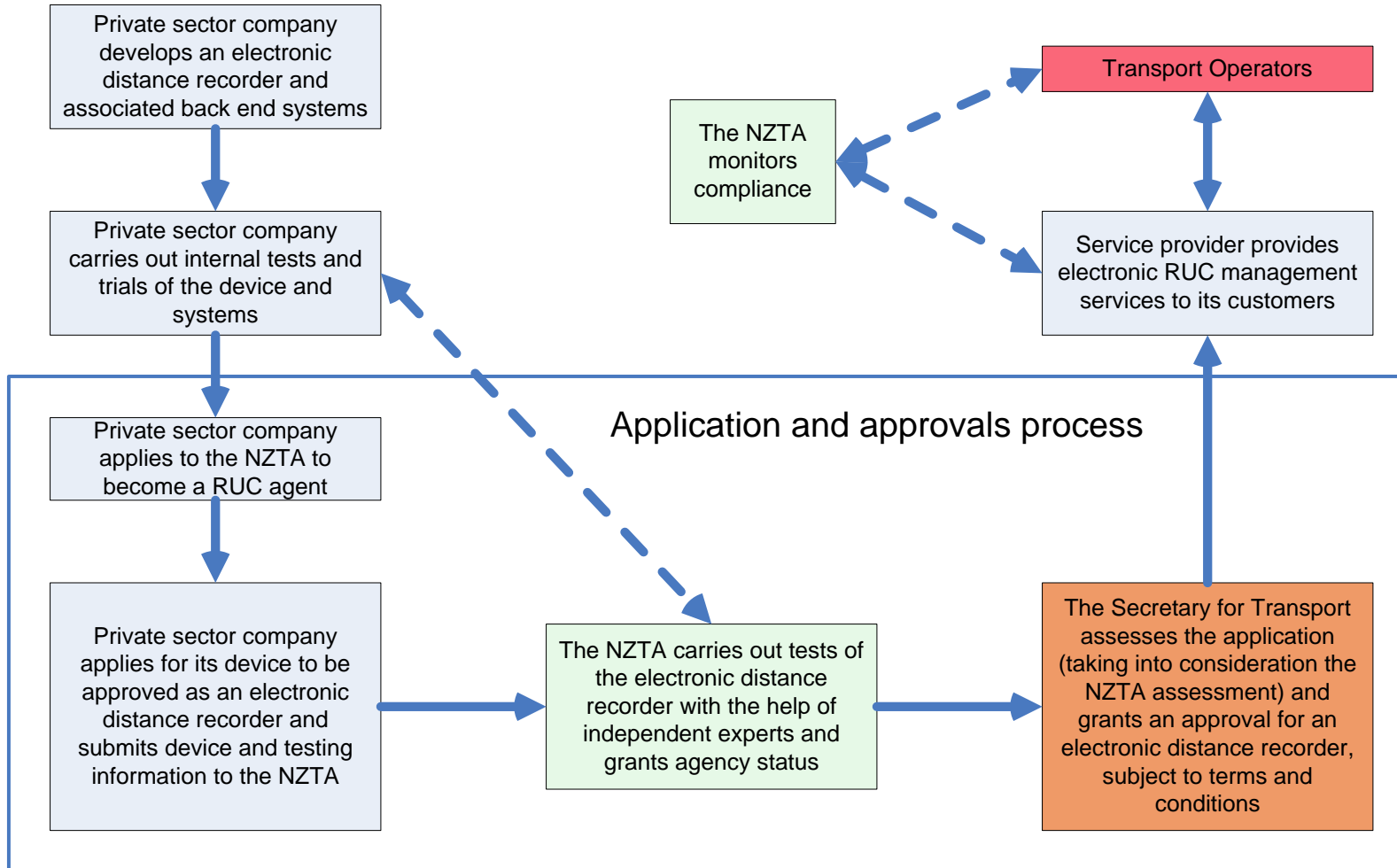
- supplying at least three prototypes to the NZTA for testing Yes/No
- back-end access for the NZTA authorised representative during testing

Yes/No

Signed :
Name:
Position:

Date:

Overview: electronic RUC service provision



**PART TWO:
OUTCOME-BASED PERFORMANCE
REQUIREMENTS**

Introduction

Part two describes an information-systems approach and is intended to act as a guide to the system requirements for an electronic RUC system². The requirements are expressed as outcomes or outputs; however, in some instances suggestions on how this outcome might be achieved are provided in footnotes.

Alternative methods to achieve the outcomes will be considered by the NZTA. This is especially the case if sound technical reasons are provided, subject to demonstration that all legal requirements are met, and that NZTA business requirements and improved technical function can be achieved.

You will be required to prepare or obtain a number of documents detailing how your information-system is designed and how it operates. The intention of these guidelines is to encourage innovation and technological progress while setting out legal requirements (fit-for-purpose) and other requirements relating to business process and security.

System components

There are four conceptual layers in the information systems approach, as drawn in Figure 1, with a fifth section (blue shaded area) indicating the major user groups.

The first layer in Figure 1 concerns the data capture and display functions. This refers to the electronic distance recorder which is the primary in-vehicle part of your information-system (replacing the mechanical hubodometer and the paper RUC licence).

The second layer in the information-system is communications. This generally refers to mobile data communications between the electronic distance recorder and your back-end. Secure monitored communications will also be required between other parts of the information system.

The back-end (layer three) refers to a range of identified functions to be performed by the software applications that support your information-system.

The data-to-information layer refers to the process of defining and collating all required data, adding context to provide meaningful information, and developing information by comparison with and analysis against other information.

² The data, functions and interfaces referred to in this section are not fully described and are likely to be the subject of longer-term development of the guidelines or replacement standards.

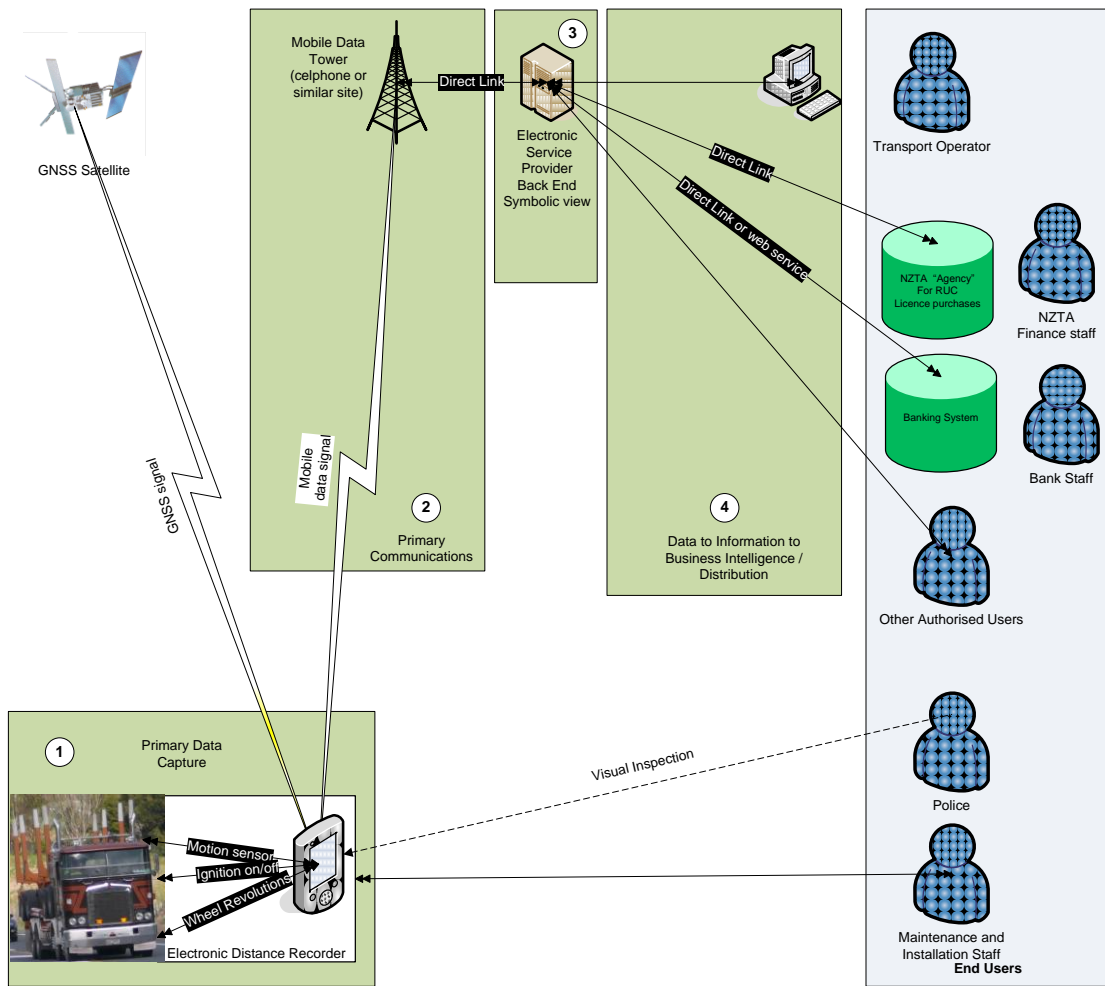


Figure 1: Conceptual layers applied to generic tracking system in current legal environment

Electronic distance recorder

The electronic distance recorder is the in-vehicle unit that acts as the primary data capture device and electronic distance licence display. The full definition of an electronic distance recorder is provided in Appendix one.

Before applying to the Secretary for an approval, your electronic distance recorder will be tested by an independent engineering expert, to the satisfaction of the NZTA.

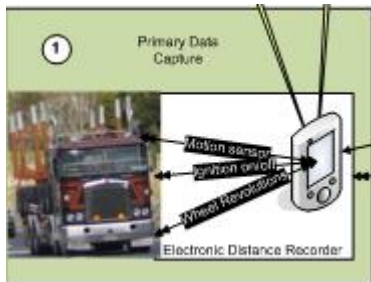


Figure 1: Primary Data Capture

Required function

An electronic distance recorder must:

- record wheel revolutions or derivation of wheel revolutions as the primary method of accurately recording distance travelled
- gather positioning data from a global navigation satellite system (GNSS) receiver to accurately determine distance travelled.
- include an accelerometer housed within the electronic distance recorder to validate, and ideally estimate the distance travelled
- have an ignition sensor (or other engine running input) to validate movement in heavy motor vehicles (trailers should have a similar validation methodology indicating when they are being towed)
- cross-reference data from the above sensors and, when significant variation is apparent, report an exception
- display the electronic distance licence and distance travelled in accordance with section 19 of the Act and in the form prescribed in Schedule 2 of the Regulations (either as an integrated part of the electronic distance recorder or on one or more separate electronic display panels)
- continue to accurately display the distance run, irrespective of communications network coverage
- clearly indicate visually whether or not there has been a reported exception that is unresolved
- transmit data to your back-end at intervals of not more than two minutes while the vehicle is moving and at least once a day when the ignition is switched off (subject to mobile data communication network coverage) and store all data that has not been received by your back-end

- continue to transmit all data in the event of any exception or tampering unless the device is tampered with to the extent that it is no longer capable of communication
- in the event of an exception, continue to record distance travelled, time, date, and the location and description of the exception. This includes any event of:
 - o the wheel-revolution recorder or any other sensor failing to provide a reading
 - o the wheel-revolution recorder or any other sensor being damaged
 - o the wheel-revolution recorder being disconnected from the electronic distance recorder
 - o the case, distance calculator or any external sensors, feeds or related equipment (e.g., distance, ignition, primary power supply) being tampered with
 - o any other occasion on which any part of the electronic distance recorder (internal or external) does not operate as designed and approved, or any attempt is made to penetrate, open or otherwise access or remove the case
 - o the data-validation process indicates an exception.

All required data must be captured by the electronic distance recorder. Basic data requirements are listed on pages 30-33.

Required form

An electronic distance recorder (including separate electronic licence display, if any) must:

- be housed in a secure, rigid and durable case³ or cases (enclosure) designed to:
 - o minimise the risk of unauthorised entry
 - o make any unauthorised entry (or attempt) visually tamper evident
 - o report each entry (or attempt) electronically as an exception.
- be permanently fitted to the vehicle in such a way that the electronic distance recorder may not be detached or removed without opening the case and creating an exception
- be permanently powered on
- include a continuous power supply, which cannot be deactivated when ignition or electrical circuits are switched, and contain an independent internal battery backup (housed within the case) with a minimum battery life of three

³ It may be possible to use more than one case provided that all cases meet the requirements.

months⁴ of normal device operation without connection to any external power source

- indicate all tampering and exceptions including power disconnection and low battery power by readily apparent means on the electronic distance recorder case (and the display case if this is separate) and transmit a corresponding exception to your back-end, sufficiently detailed for you to correctly analyse the issue
- record the distance travelled and update distance travelled portion the display at not more than two second intervals from GNSS positioning and accelerometer inputs at any time when the primary distance recorder is not providing a valid distance input
- be permanently connected to any external inputs (wheel revolution, power, ignition, etc), monitor those inputs and create exceptions in the event of any alteration or tampering with the sensors, the connection between those sensors and the electronic distance recorder, or the communications medium
- include sufficient on-board memory⁵ to store six⁶ months of data (before transmission), in the event that communications and /or your back-end are unavailable
- ensure that all data captured from the vehicle is recorded to the memory of the electronic distance recorder and is erased only after your back-end confirms receipt of that data, or, in the case of a RUC licence, when a more recent licence is current and displayed.

It is desirable (but not essential) that an electronic distance recorder is able to store distance licences that have been purchased in advance but are not yet current.

The electronic licence display must (in addition to other electronic distance recorder requirements):

- at all times while a vehicle is on a road, display the current RUC licence in accordance with the provisions of the Act and the Regulations. If a current licence has not been purchased, the most recently purchased licence must be displayed. If there is no mobile data coverage and a current licence is not stored in the electronic distance recorder, the licence that was displayed during the last period of coverage must continue to be displayed. You are advised to obtain legal advice on the display requirements of the legislation.

⁴ Ultra performance batteries are available with a life cycle of 5-7 years of operation under extreme conditions.

⁵ Independent advice received by the NZTA suggests that the memory should be solid state, non-volatile memory. Solid state memory overcomes issues experienced with other types of memory exposed to vibrations and shock while non-volatile memory does not require a power source to retain data (whereas volatile memory requires constant power).

⁶ This timeframe corresponds with the legal requirement to have a vehicle inspected for certificate of fitness and therefore logically moving into an area where communications are available.

The transport operator remains liable for ensuring that a new licence has been purchased when a vehicle is outside coverage⁷.

- meet the Act's requirement to produce the distance licence on demand
- be easily read from outside the vehicle in conditions of sunlight and darkness, as far as technically possible
- not be of such an intensity or size that it will dazzle, confuse or distract other road users or display any forward-facing red lights or flashing amber lights.

Clearly display the brand name of the electronic distance recorder, the model and version number and the unique serial number in a permanent format visible on a part of the electronic distance recorder which can be seen from outside the vehicle. Permanent format means not as part of the electronic display, e.g. on a metal plate securely fastened to the unit. Please also refer to the terms and conditions under 'devices to have a brand name'.

If the electronic licence display is contained in a separate case from the distance recording function, the two cases must be both physically or electrically connected, and reliably and securely electronically linked (irrespective of connection to a vehicle's electrical system) in such a manner that the display cannot be moved more than 25 metres from the vehicle without creating an automated exception.

A technical solution is required to reliably and securely deal with coupling and decoupling trailers if the option of displaying the trailer's electronic distance licence in the towing vehicle is to be considered.

Minimum performance requirement

Electronic distance recorders must be able to operate normally in the face of drops, shocks, vibration, humidity, altitude, rain, dust, sand, temperature extremes (-30°C - +80°C) and thermal shock⁸.

Assurance is required that the electronic distance recorder will not interfere with other electronic devices or systems on or around the vehicle and, similarly, that those devices or systems will not affect the operation of the electronic distance recorder⁹.

Externally mounted electronic distance recorders must be able to withstand high-pressure hosing and immersion in water up to 1metre¹⁰.

Accuracy specifications

The wheel-revolution distance displayed must be within the range +/- 2%¹¹ of the distance measured by a properly calibrated instrument at all times.

⁷ This legal requirement dictates the back-end requirement for an operator to be able to request purchase of a licence apart from those requests that may be automatically generated.

⁸ Compliance with MIL-STD-810G tests is suggested. .

⁹ Compliance with MIL-STD-461F tests (or other equivalent standards) to provide assurance on electromagnetic interference (EMI) and electromagnetic compatibility (EMC) is suggested.

¹⁰ Compliance with IP 67 rating is suggested.

Raw GNSS positioning must normally be within 10 metres of actual physical position.¹²

The distance estimated by dead reckoning (ie, the accelerometer) must be within +/- 3%¹³ of the distance measured by a properly calibrated instrument at all times.

Reliability specifications

The electronic distance recorder (including all components and display/s) must be designed to perform normally while withstanding all New Zealand environmental extremes, including temperature, dust, ultraviolet radiation and moisture without significant deterioration over the design life cycle of the electronic distance recorder.

Data capture must be as reliable and up-to-date as technically possible ie, 100% reliability and near real time subject to physical connections, satellite constellation coverage and mobile communications network coverage.

Electronic security

The electronic distance recorder must:

- have sufficient security mechanisms to mitigate the risk of physical and electronic tampering, and must detect and electronically report physical, and electronic tampering or inaccurate source data
- monitor external cables to ensure that data and power sources are direct and free from unauthorised adjustment, corruption or interference, detecting any alteration or tampering and reporting these as an exception
- adopt a methodology that ensures that data cannot be altered, and the source is authenticated during otherwise insecure two-way communications¹⁴ with your back-end
- secure all data to a high standard¹⁵ before transmission to your back-end and reject all incoming data that is not secure and authenticated as originating from your back-end
- report an exception if the case housing the electronic distance recorder, processor, memory, communications or display is opened
- report any exception to your back-end and display an exception warning on the device and display, until such time as you clear that warning

¹¹ The NZTA test standard for mechanical hubodometers.

¹² The word “normally” allows for factors such as canyoning, loss of constellation and outliers.

¹³ 50% more lenient than primary distance standard and corresponds with international indications of GNSS accuracy.

¹⁴ The NZTA will approve a VPN (virtual private network) between the device and your back office with a standard of encryption that has not been broken or alternately will approve properly configured digital signing.

¹⁵ Independent advice received by the NZTA suggests that 128-bit advanced encryption standard (AES) encryption is a desirable minimum standard and is widely used globally in banking and other secure systems.

- enable authenticated electronic identification of the data source (electronic distance recorder and sensors).

The display function of the electronic distance recorder must be limited to reading and displaying RUC licence data, identifying and indicating any exception on the device itself and then transmitting that exception securely to your back-end.

The electronic distance recorder must enable exception reporting. It is highly desirable that distance reporting and data transmission from the electronic distance recorder to your back-end (while disabling the electronic distance recorder's ability to receive any new distance licence data) continues in the event that the case is open or another exception has been reported¹⁶. It is intended in future guidelines to make this mandatory; however there will be a transition period in the mean time while consultation with industry occurs around this.

Physical security

The electronic distance recorder must:

- be designed in such a way as to be physically secure from any attempt to tamper with internal and external data capture points, components, wiring, electrical currents or electronic signals, and to recognise any such tampering as an exception
- be permanently fixed to the vehicle in such a way that removing the electronic distance recorder (including the display) is not possible without reporting an exception
- be enclosed in such a way that accessing, adjusting or tampering with internal components is not possible without penetrating or opening the case, and in either event the EDR must report an exception
- report any exceptions by all of the following methods: automatically indicate exception on each electronic distance recorder (and associated display/s), transmit full details of each exception to any associated display and back-end system and make any physical tampering evident

Methodology requirements

The primary distance recorded must be derived from wheel revolutions.

The electronic distance recorder must validate the primary distance measured and onboard time against GNSS location /time, accelerometer and ignition circuit data.

A sample method for distance calculation is as follows:

1. Recording the primary distance and time from wheel revolutions or derived from wheel revolutions.
2. Deriving a secondary distance calculated from a series of GNSS receiver locations at corresponding times

¹⁶ This alerts the information system that any data received may not be reliable while continuing to report exceptions and unconfirmed distance.

3. Validating movement using a three axis accelerometer
4. Validating movement using the ignition (or similar) circuit
5. Authentication of measured distances from steps 1 and 2 and validation using steps 3 and 4 using a parameter and exception model
6. Transmitting the distance determined to the back end (e.g. a part of the system that monitors RUC).

The Ministry and the NZTA bear no responsibility for patent infringement arising from an approval of an electronic distance recorder; please refer to the waiver provision on page 3.

The electronic distance recorder must communicate all data to your back-end at intervals not greater than two minutes whenever the vehicle is moving and at least once a day when the ignition is switched off, unless the vehicle is operating outside mobile communication coverage range of the selected communication provider.

If the vehicle has been operating outside mobile coverage range it must update your back-end immediately when it regains network coverage.

The priority for updates at any time when coverage has been lost and is regained should be:

1. exception reports
2. distance travelled
3. distance licences
4. supplementary licences and other data.

The electronic distance recorder must recognise any exceptions to any requirement in this section of the guidelines and return an exception notification to your back-end recording all exceptions in your exception register.

Communications

Communications will occur between the electronic distance recorder and your back-end, and between your back-end and authorised parties.

Communications may also occur between devices on a vehicle (electronic distance recorders, input sensors, electronic display (where separate), trailer sensors); between electronic distance recorders and device maintenance tools.

In the current environment the most common method of data communications between vehicles and your back-end is the commercial mobile data network. This does not preclude other options: e.g., satellite, ViFi etc.

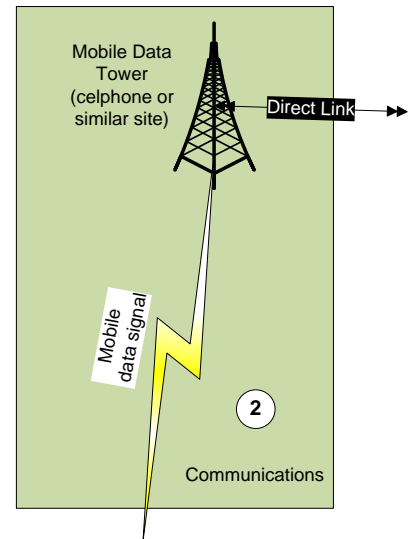


Figure 2: Communications layer

Required function

Communications are required to transmit data effectively between different system components.

Required form

Two-way wireless communications must be available to and from moving vehicles at all times while within range (coverage)

Communications between devices on a vehicle or between a towing vehicle and trailers attached to it must be secure and automatic. Connections between devices on a vehicle or combination must not rely on any connections that are plugged in each time a trailer is connected.

All internet communications must meet applicable security standards (ie, HTTPS).

Minimum performance requirement

All communications networks and mobile data transmission must be continuously available, network (round trip) latency must ensure delivery of all data to the destination within one minute of transmission and confirmation of delivery to be received by the in-vehicle unit. Network coverage must be greater than 40%¹⁷ of the geographic area of New Zealand (calculated by land mass not population).

Physical security

All on-board communications equipment must be fully enclosed within the secure electronic distance recorder casing(s).

¹⁷ Your telecommunications provider will need to certify that these requirements can be met.

Back-end system

The back-end of your information-system will typically consist of a number of functional services. For example, GNSS processing and correction, data validation (comparing recorded distance with GNSS calculation, accelerometer and any other data), administration and fee calculation, exception management, payments and licence-issue service, reporting to authorised users, storage, etc. It will also consist of a range of interfaces between services, users and the electronic distance recorder, each requiring differing levels of security, data formats and specifications.

While the diagram below illustrates the major components and functions, it is recognised that considerable further detail will be required and the final architecture may not resemble the illustration.

It is also recognised that the back-end is a highly vulnerable part of any information-system. This is addressed in part by the requirement for you to prepare, maintain and update formal information-system specifications and an information-system management plan. Up-to-date versions must be provided to the NZTA’s authorised representative, checked as part of any internal review and produced for reference at the time of any audit of your information-system.

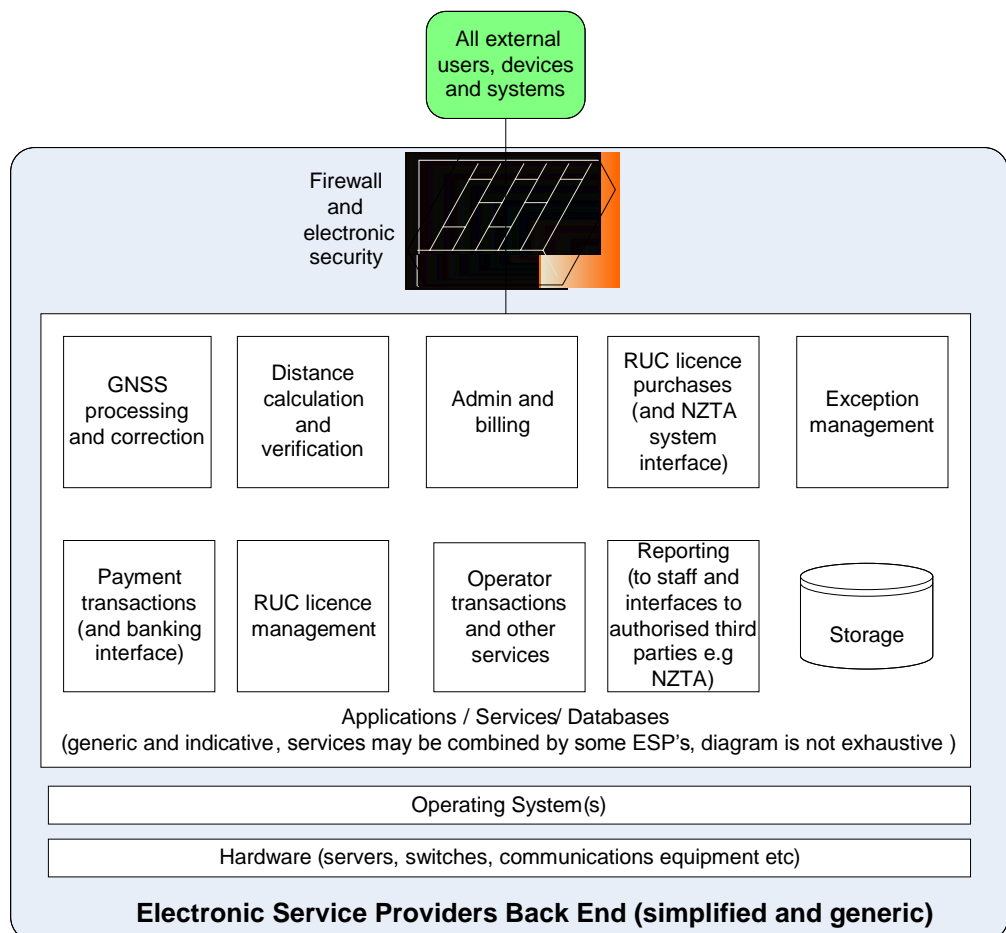


Figure 3: Simplified illustration of major information system components in a generic back-end

Required function

Input: secure data.

Output: information tailored to various uses for each user group or user.

Required form

Your back-end must be remote from participating vehicles, although some back-end functions may be performed partially or entirely in electronic distance recorders or virtualised across other secure environments that meet information-system requirements.

Your back-end must provide storage of data for each vehicle for a minimum of seven years. Historical data (that which is not required for current operations) can be stored in an archive retrieval system provided it can be accessed with reasonable notice.

Minimum performance requirement

Your back-end must operate in real time (updated within three minutes¹⁸ of any mobile data being logged by an electronic distance recorder – subject to mobile data coverage) and continuously available (greater than 99.75%). Your back-end must enable up-to-date checks at any time to verify RUC licence status, distance travelled and the status of the electronic distance recorder.

Your information-system management plan should detail the system architecture, storage and archive measures and any backup and disaster-recovery procedures.

Accuracy specifications

Your back-end must operate in such a way that it processes all data received with 100% accuracy in relation to reported distance travelled for each vehicle.

It must not be possible for any recorded vehicle location, distance, weight, time or other relevant data to be deleted or altered by a person or system (it is accepted that location outliers may be repositioned. It is accepted that system administrators are technically able to alter data but required that they will not).

Reliability specifications

Your back-end must be continuously available (as defined above) to receive and process information from electronic distance recorders. You are responsible for ensuring sufficient information-system redundancy levels and power sources to ensure this outcome.

Please note that RUC licence purchases are not continuously available because of constraints in the current NZTA RUC system. An application for a RUC licence is lodged only when entered into the NZTA RUC system.

¹⁸ Allows for up to two minutes before transmission and a further minute for communications

Electronic security

You must:

- ensure that your back-end is built using an industry standard methodology that restricts the level of user that is capable of changing data, ensures that a secure log records all alterations to data, the reason for those changes and the user id of the person making those changes. Each data source must be authenticated
- mitigate the risk of unlawful electronic access to any part of the system as far as is reasonably possible, using security levels, firewalls and other applications to prevent, limit, contain and report any intrusion attempts
- include adequate security protocols to ensure that the RUC licence details returned to you from the NZTA RUC system cannot be altered before or during transmission to the vehicle
- include exception reporting from within your back-end, electronic distance recorders, and all other data feeds such that the type of exception can be determined precisely without physical inspection
- include an exception-handling process ensuring that every exception and resolution is notified, permanently recorded, and actioned appropriately within a time frame approved by the NZTA authorised representative
- ensure that your back-end records the most recent time and location of any transaction with an electronic distance recorder
- generate and maintain a map of locations where communications network coverage is normally expected and where no transmission has been received and generate an exception notification where expected transmissions have not been received from the electronic distance recorder

Physical security

You must develop a physical and electronic security plan to provide assurance that your security exceeds, or is readily comparable to, bank grade security¹⁹. The security plan must undergo a review by an independent security expert who is approved by the NZTA authorised representative.

Your back-end environment and information-system must comply at all times with the approved security plan. It is recommended the security plan should include as a minimum:

- a physically secure environment for your back-end, strict access control policy and monitoring (including an access control system with appropriate identification factors e.g., biometric factors), alarm activations and exception notification and reporting

¹⁹ Bank grade security indicates the requirement to adequately protect around \$1 billion revenue per annum. The applicant will be required to demonstrate that their system meets rigorous standards and that serious consideration has been given to ensure no exploits are available.

- vetting of personnel, including a Police vetting at yearly intervals of personnel that are permitted direct access to server administration. Any personnel who have convictions for dishonesty and/or any RUC offending should not be permitted to have access to the server administration.

Methodology requirements

Your back-end must continuously receive data from a variety of sources and process that data to accurately, reliably and continuously ensure correct payment for RUC licences for all distances travelled by any vehicles fitted with your electronic distance recorder.

GNSS processing and correction

GNSS positioning is a relatively imprecise science and corrections are part of normal business process when reported positions do not correspond with previous and subsequent positions. The rules which you develop and /or apply to correct GNSS derived data, whether applied to the electronic distance recorder or at the back-end, must be documented and available for audit at any time.

In addition, GNSS position data (in association with a mapping database) is likely to be used to determine whether a vehicle is on or off-road for the purposes of submitting a claim against a RUC licence for off-road travel. Any additional rules developed for correcting position inputs and /or reconciling position data against known road classifications and locations must also be documented and available for audit at any time.

Your system must comply at all times with the documented rules covered in the previous two paragraphs.

Administration and billing

Administration and billing are internal functions which depend on other parts of the information-system. These functions must not expose you to any additional security issues.

Payment transactions

Payment transactions involve an interface with the banking system, and compliance with banking system requirements is likely to be considered sufficient for this function.

Exception management

You must maintain an exception register in electronic form, investigate every exception report and record authenticated responses from transport operators. The exception register shall include:

- every identified exception and non-compliance
- detail of the exception or non-compliance
- the corresponding time, date, location, vehicle and transport operator
- the time and date the transport operator was notified

- authenticated electronic response and /or voice-recording of the transport operator's response and /or written response signed by the transport operator
- your resolution
- whether or not the NZTA authorised representative was notified.

RUC licence purchases

Your system is required to include an NZTA interface to permit purchase of RUC licences via the NZTA RUC system.

Operator transactions and other services

You may provide additional services to your customers using the electronic distance recorder and information system as long as provision of these services does not expose you to any additional security issues.

The transport operator remains liable for ensuring that a new licence has been purchased even when a vehicle is outside coverage. Therefore, the transport operator must be able to access your information-system to purchase new distance licences in the event that the vehicle is outside coverage for an extended period.

The transport operator must be able to carry out all other current licence-purchase functions.

Your back-end must record any successful and unsuccessful attempts to purchase or electronically deliver a RUC licence to the electronic distance recorder. In the event of a failed purchase attempt, the customer must immediately be made aware of the failure so that they know that the transaction has not occurred.

Reporting

Reporting functions must be able to be performed without any interference with information-system transaction processing speed. A dedicated reporting server may necessary to fulfil this requirement.

Storage

Storage must be configured to minimise data loss in the event of catastrophic system failure or total power failure.

Interfaces

The following interfaces are identified, but not all of these have yet been specified:

- Back-end to electronic distance recorder (may remain part of information system or may be specified)
- Back-end to banking system, subject to existing banking requirements
- Back-end to NZTA RUC system, subject to NZTA contract for agents
- Back-end to transport operators (may remain part of information-system or may be specified)

- Back-end to other authorised remote users (likely to be specified in the future).

It is noted that more information may be required to satisfactorily enable RUC information-system design. These guidelines are designed to assist with the initial process.

Data to information layer

The key considerations in system and data architecture are that all data must be highly accurate, reliable, validated and authenticated wherever possible, and traceable to source.

Data is the raw ingredient collected from each source. Data is gathered and placed in context to develop meaningful information.

Reference to the data listed below shows that the RUC system does not require or contain any personal information.

Required function

Input: data.

Output: data and information.

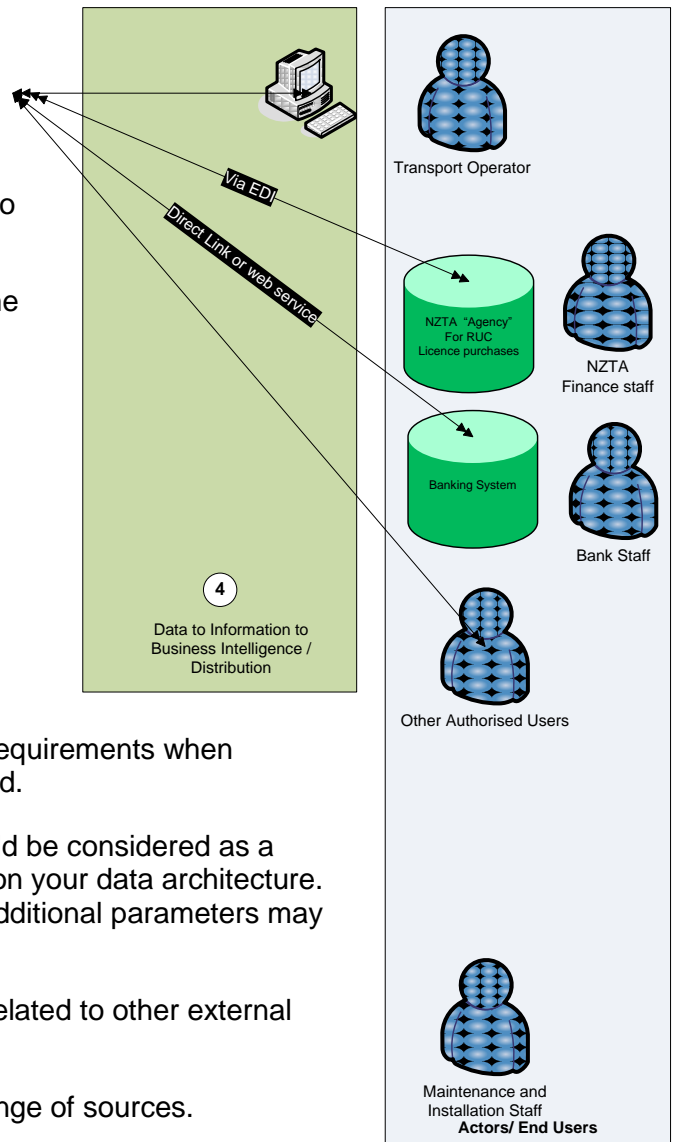
Required form

The suggested minimum data requirements are listed below. The NZTA may have further data requirements when interfaces are defined or subsequently re-defined.

It is important to note that the following list should be considered as a minimum starting point rather than a constraint on your data architecture. A flexible system with the capacity to manage additional parameters may be an advantage.

This list currently excludes metadata and data related to other external systems such as the banking system.

Please note that data will be collected from a range of sources.



Data	Format	Source	Comment	Capture interval and accuracy
Distance run	Km	Electronic distance recorder derived from wheel revolutions and validated by other sensors	Primary distance data	Continuous minimum display interval 100m must be accurate to within +/-2% at all times
Electronic distance recorder date and time	Hh:mm dd/mm/yy	Electronic distance recorder system time	Required to be automatically calibrated against GNSS time to maintain system consistency	Must continuously update and must always be calibrated within +/- 1 second of NZ standard time (GMT +12) or adjusted for daylight saving when relevant
GNSS location and time	X,Y,Z, GMT	Electronic distance recorder derived from GNSS satellites Time GPS only	Used for validation of electronic distance recorder distance run / time in conjunction with accelerometer	X,Y raw position within 5 meters when constellation coverage available. Z used for validation
Accelerometer or gyroscope	X,Y,Z	Electronic distance recorder derived from internal sensor	Used for dead reckoning, tamper detection and validation of distance run and GNSS	Must enable no more than 10% error
Ignition on/off (or other engine running sensor)		Electronic distance recorder	Used for validation of movement and minimum reporting intervals	
Electronic distance recorder ID and make	Unique device ID	Electronic distance recorder	Must be unique ID, independent of number plate but associated with the vehicle (device make and serial number)	Once only, but must be physically verified following any tamper exception

Data	Format	Source	Comment	Capture interval and accuracy
Tamper or normal	Alarm	Electronic distance recorder	Indicates any tamper or exception on the device and identifies the issue in the back-end until resolved by you	Only on exception but must be completely accurate
Low power	Alarm	Electronic distance recorder	Identifies if the primary power source has been disconnected or the internal battery is low	Only on exception but must be completely accurate
Vehicle registration number	Up to 6 alpha numeric characters	Electronic distance recorder installer must confirm association between the electronic distance recorder ID and registration number	Must be permanently associated with the electronic distance recorder ID	
On or off-road	On/off	Base map	May be obtained from road centre line and width data, geo fencing, cadastral or other such combination as currently approved or specified by NZTA	
Back end time and date	Hh:mm dd/mm/yy	Back end system time	Required to be automatically calibrated against GNSS time to maintain consistency	Must continuously update and must always be calibrated within +/- 1 second of NZ standard time or the daylight saving adjustment

Data	Format	Source	Comment	Capture interval and accuracy
RUC licence vehicle type	3 numeric	NZTA RUC system	As per the Regulations	Permanently associated with the vehicle
RUC licence weight	Up to 3 numeric	NZTA RUC system	Nominated by the transport operator	Currently nominated per 1000kms for distance licences
RUC licence serial number	Up to 10 alpha-numeric characters	NZTA RUC system	Currently only numeric	
RUC licence type	Distance or time or supplementary	NZTA RUC system		
RUC licence electronic distance recorder serial number	Up to 10 alpha-numeric characters	NZTA RUC system	Must correspond precisely with electronic distance recorder ID	
RUC licence minimum and maximum distances	6 numeric characters	NZTA RUC system		

Accuracy specifications

All distance data obtained from wheel revolutions must be validated against GNSS and accelerometer data to ensure the 2% accuracy requirement is continuously met throughout service life.

All information generated from the data must be 100% accurate in relation to the available data (to the extent possible within system constraints).

Reliability specifications

All data and information must be continuously updated and available subject only to availability of communications and NZTA RUC services. Your system must ensure that all data reaches the back-end within three minutes of capture by the electronic distance recorder unless there is no communications coverage at that time. This accounts for transmission at intervals not exceeding two minutes and up to one minute for communications.

Electronic security

You must take all reasonable steps to ensure the security of electronic access to, integrity and accuracy of, data and information provided.

Physical security

You must take all reasonable steps to ensure the physical security of access to data and information.

Mapping

The Ministry is considering adopting a base map regime in future guidelines which may include the NZ standard map series. This is currently the LINZ topo map series (tiled) – this meets the NZGD 2000 projection which complies with the international WGS84 projection (these projections correspond with a satellite’s view of the world).

On-road versus off-road travel

Further definition is required of what constitutes on-road and off-road (physically and electronically). Possibilities include cadastral, distance from centre line, geo fencing, road width at each location or a combination of these. A single standard of map layer information is likely to be required in the future in order to achieve equity in charging. It is likely that a commercial map layer provider will be selected for this purpose and you may be required to include that layer in your system particularly for the purpose of on-road versus off-road calculations.

It is noted that various private sector companies provide New Zealand map layer information and it is accepted that each company is likely to have differences in the data recorded.

PART THREE:
TERMS AND CONDITIONS THAT
THE SECRETARY MAY APPLY

Terms and conditions of approval

The following provisions are indicative of the terms and conditions that are likely to accompany the Secretary's approval for an electronic distance recorder. The wording of the actual terms and conditions may differ slightly and the Secretary reserves the right to impose provisions in addition to those outlined below.

Company requirements

The approval will be given only to a registered New Zealand company with at least one company director residing in New Zealand.

Term of approval

The approval is granted for a term of three years.

No later than three months before the expiry of this term you may apply to the Secretary in writing for a re-approval. The Secretary will review your performance under the approval and, if satisfied, he /she may agree to grant a re-approval for a term of three years. The term of a re-approval will begin immediately following the Secretary's consent.

Further re-approvals may be possible and will follow the same process.

Cost of compliance

You are responsible for, and must bear all costs of, complying with your obligations under the approval.

Approval given for specific device

You must specify the make and model of the electronic distance recorder which is the subject of the approval.

The approval is granted for a specific make and model only. Should you change the parameters of the electronic distance recorder (or any associated software) in a way that adversely or materially affects its functionality it is deemed to be a new model and the existing approval will no longer apply.

Change management

In the event of any changes to your information-system that may affect the back-end interface with either the transport operator, the electronic distance recorder or other authorised remote users, you agree to:

- maintain a change management register that records the reason for the change, relevant application/s, testing conducted, date and time implemented, version number, NZTA notification and impact of every change. The change register must be in a format approved by the NZTA authorised representative and made available to the NZTA authorised representative on request
- advise the NZTA authorised representative at least seven days in advance of any firmware or software upgrade unless the nominated NZTA representative

specifically authorises an urgent upgrade. The advice must include the reason, date, time, version number and impact of every upgrade

- advise the NZTA authorised representative within in one working day if any implemented change impacts on your information-system in any way that was not anticipated
- accept liability for the cost (if any) of any changes to your information-system necessary to conform to revised interface specifications required by the NZTA or other providers of services interfacing with your information-system.

The NZTA reserves the right to require system testing at your expense if, in the opinion of the NZTA authorised representative, any upgrade to any part of your information-system could affect the security or accuracy of data, data transmission, or the security or accuracy of the data capture device or any associated display or payment. It is noted that communications firmware upgrades are highly unlikely to have such an effect.

Business process audits

You agree to permit the NZTA authorised representative at any time to audit, observe, test or inspect:

- the equipment, any part of your information-system, and the location or any site at which any activity or work is carried out for you or on your behalf
- your records, including business process documentation, exception logs and any other information relating to the functions carried out under this approval and the applicable law.

Conditions relating to the fitting of electronic distance recorders to vehicles

Only you, or an installer authorised by you, shall fit an electronic distance recorder to a vehicle. This must be carried out in accordance with your fitting and testing specifications and records must be kept to confirm compliance for each vehicle installation. These records must be available to the NZTA authorised representative on request.

Conditions relating to the repair or modification of electronic distance recorders fitted to vehicles

Only you, or a repairer authorised by you, shall repair or modify or attempt to repair or modify in any way, any part of an electronic distance recorder. This must be carried out in accordance with your repair specifications, and relevant records (including exception records) must be completed.

Customer relations

You must provide support to your customers in respect of faulty or damaged distance recorders.

In the event that you discontinue the provision of RUC services to a customer, you must notify the NZTA authorised representative (under protocols agreed with the

NZTA authorised representative), that the customer is no longer using your RUC services.

You must have a discontinuation protocol, approved by the NZTA authorised representative, which ensures:

- that the customer is not prevented from complying with their obligations under the Act by any action which you take
- that the electronic distance recorder continues to record distance and location and display the distance recorded, as well as transmitting that data to your back-end, until such time as it is removed from the vehicle/s, or until you are advised by the NZTA authorised representative that you may discontinue this function
- you must deliver to the customer copies of all information you hold on their behalf specific to the provision of RUC services, including distance recording.

Devices to have a brand name

Your electronic distance recorder must carry a brand name and model number. This must be visible from outside the vehicle.

Systematic exception reporting

You must maintain an exception reporting system that includes a log of every exception report, the investigation and authenticated responses from transport operators.

You must report to the NZTA authorised representative any exception that carries the risk of loss of revenue to the Crown (such as suspicious or systematic exceptions) along with any associated authenticated responses from transport operators.

In the event that you report a suspicious or systematic exception you will grant the NZTA access to all records you hold relating to the event.

Management of data and records

Your back-end systems must provide storage of all data relating to the provision of RUC services for a minimum of seven years. If your approval lapses you must deliver to the customer copies of all information you hold on their behalf specific to the provision of RUC services, including distance recording.

Access to aggregate information

You agree, upon request, to provide the Ministry or the NZTA, at reasonable cost, in a format specified by the Ministry or the NZTA anonymous aggregate traffic or transport information from your clients for the Ministry and /or the NZTA to use, copy, modify, store and disclose as they see fit.

Termination of approval

If your authorisation under section 10(3)(b) of the Act to issue RUC licences (contained in the service delivery agreement) is terminated, the Secretary's approval

of an electronic distance recorder under regulation 6A of the Regulations will also be terminated with immediate effect.

Variation or revocation of approval

The approval (including these terms and conditions) may be varied by the Secretary by notice in writing, in the event that:

- there is a change in applicable law
- you alter the parameters of the electronic distance recorder (or any associated software) in a way that provides minor enhancements to its functionality
- in any other circumstances that the Secretary considers appropriate.

The approval may be revoked by the Secretary, by notice in writing, in the event that:

- you alter the parameters of the electronic distance recorder (or any associated software) in a way that adversely or materially affects its functionality
- there is a serious breach of, or non-compliance with, the terms and conditions of an approval
- the Secretary becomes aware of a defect with the electronic distance recorder or supporting systems which he/she reasonably believes presents a risk to Crown revenue.

You remain responsible for advising your customers of any material variation or revocation of your approval.

Appendix one: glossary

Accelerometer: a device that measures acceleration forces.

Act: means the Road User Charges Act 1977.

Agency agreement: see service delivery agreement.

Approval: means an approval granted by the Secretary of Transport of an electronic distance recorder.

Audit: includes any visual, physical, mechanical, electrical and electronic inspection as determined by the auditor, to determine a party's capacity to meet, or continue to meet, initial and on-going certification requirements, as set by the Ministry or the NZTA.

Authorisation: means authorisation from the NZTA for an electronic service provider to issue RUC licences electronically.

Authenticated: confirmation that something is what it claims to be and cannot be something else.

Back-end: includes all hardware, operating system/s software application, data and other parts of the information-system used to collect and process data from one or more electronic distance recorders, their associated transport operators, the NZTA and other parties.

Base map: a standard map on which standardised primary data is recorded for reference within the system.

Cadastral: publicly recorded data about legal ownership of land.

Data validation process: see validation.

Dead reckoning: allows a system to estimate present position by projecting past courses and speeds over the ground from a last known position.

Electronic distance recorder: means a distance recorder approved by the Secretary under regulation 6A, fitted to a motor vehicle, that—

“(a) uses internal and external sensors to—

(i) accurately measure and record in kilometres the distance travelled by the motor vehicle; and

(ii) identify and record the location of the distance travelled by the motor vehicle; and

(b) uses 1 or more electronic display panels that show—

(i) the distance travelled by the motor vehicle; and

(ii) the distance licence for the motor vehicle; and

(c) electronically transfers to the server of an electronic service provider information relating to the distance travelled by the motor vehicle and the location of the distance travelled by the motor vehicle.”

An electronic distance recorder operates in a vehicle, performing primarily distance measuring and licence display functions, validated against GNSS positioning, ignition and accelerometer, incorporating secure mobile data communication with a remote back-end operated by the electronic service provider.

Electronic service provider: means a company authorised under section 10(3)(b) of the Act to issue a licence displayed electronically (an agent of the NZTA) and has an approval from the Secretary for Transport under regulation 6A.

Exception: means any time that any part of the information-system is not operating normally or within agreed parameters (as designed or expected).

Factory acceptance testing: testing of electronic distance recorders to demonstrate that all avenues of system tampering have been satisfactorily addressed and the system is capable of operating to specification.

Firmware: the programs and data structures that internally control an electronic device.

Geo fencing: the establishment of a virtual perimeter on a geographic area so that when a specific device enters or exits the area a notification is generated.

Global navigation satellite systems (GNSS): including (and often referred to as) the well-known US NAVSTAR Global Positioning System (GPS), the Russian Glonass system, the European Galileo system, the Chinese Beidou/ Compass system and India’s IRNSS system. Of these, the only current fully operational system is GPS.

Hypertext transfer protocol secure (HTTPS): is a combination of the Hypertext Transfer Protocol with the Secure Socket Layer or Transport Layer Security protocol to provide encryption and secure identification of the server. HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in web based information systems.

Information-system: means an electronic system for producing, sending, receiving, storing, displaying, or otherwise processing, electronic communications. For the purpose of an electronic service provider an information-system includes all electronic distance recorders, all other hardware, software applications and related systems, services, data and communications.

Information-system management plan: details the operational management procedures to follow policy defined by an electronic service provider to effectively meet all the NZTA requirements, the Secretary’s terms and conditions and other system objectives. This should include consideration of system architecture, exception handling, backup, continuity of service, disaster recovery and other considerations.

Information-system specifications: details the core requirements for ensuring adequate data-management capability. The NZTA requires assurance that an information-system considers, includes and correctly processes data for all required business functions.

Ignition sensor: means a sensor that can determine whether or not the ignition circuit of a vehicle is in the power-on or power-off state.

Interface: means a set of defined operations that can be invoked by clients of the electronic service provider's information-system.

Internal review: a review arranged by an electronic service provider to ensure that their information system continues to comply with the guidelines. Internal reviews should be conducted at least annually, and documented and corrective action taken if necessary.

Metadata: is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about data or information about information.

Ministry: the Ministry of Transport.

Non-compliance: a deficiency in the content, documentation or implementation process of an electronic service provider's information-system which means it does not fulfil a term or condition of their approval.

NZTA: the NZ Transport Agency.

NZTA authorised representative: the NZTA Commercial Operators Policy Manager, or any person specified in writing by, or on behalf of, the NZTA Commercial Operations Policy Manager to the electronic service provider as being an authorised representative for the purposes of the voluntary electronic RUC system.

NZTA RUC system: means the NZTA's computer equipment, telecommunications equipment, the software and the Landata database management system.

Regulations: means the Road User Charges Regulations 1978.

Road user charges (RUC): charges payable by individual road users as specified by the third schedule to the Road User Charges Act 1977. Charges are applicable to all vehicles over 3.5 tonnes manufacturer's gross laden weight and all vehicles of 3.5 tonnes or less powered by a fuel not taxed at source (eg, diesel vehicles). All RUC licences are based on a vehicle's motive power, distance travelled, axle configuration and weight²⁰. Charges are paid in advance and each vehicle must be continuously licensed so that when a distance or time is complete a new licence is required.

Secretary for Transport: means the Chief Executive of the Ministry of Transport.

Security plan: means the document prepared by an electronic service provider detailing all physical and electronic measures to ensure the information system and information system environment are fit for purpose.

Service delivery agreement: the agreement between the NZTA and an agent for the provision of RUC licensing services.

²⁰ This weight refers to the maximum weight that will be carried by the vehicle over a particular licence period not a declaration of the weights that will be carried on particular parts of a trip or on particular roads.

Tamper: conduct which is intended to prevent an approved system from functioning properly.

Terms and conditions: provisions set by the Secretary for Transport which must be complied with in return for an approval being granted and maintained under Regulation 6A.

Validation: a check to confirm whether data corresponds with defined criteria. This provides a level of certainty that the data is correct and eliminates data that is clearly not correct.

Virtual private network (VPN): a computer network that is implemented in an additional software layer (overlay) on top of an existing larger network for the purpose of creating a private scope of computer communications or providing a secure extension of a private network into an insecure network such as the internet.