

# Device Lifecycle – All You Need To Know

## Who Is Payments NZ?

Payments NZ Limited (PNZ) is responsible for setting and overseeing the rules and standards that are central to the way payment instructions are exchanged and settled.

We ensure that everyone involved in payments in New Zealand has complete confidence in the integrity of the payments system.

We are the central body dedicated to establishing the best possible guidelines and rules of engagement for all.

## What is the Consumer Electronic Clearing System?

The Consumer Electronic Clearing System (CECS) includes all consumer electronic payments. Today this covers EFTPOS. It also includes emerging technology like mobile payments and road toll payments.

To make an electronic payment happen, different entities have to “talk” to exchange information about the payment. CECS creates the rules and standards that govern how this should happen.

The table below lists some examples:

The rules and standards for...	Include...
<b>Issuer</b>	<ul style="list-style-type: none"> <li>• What a card must have and do, and</li> <li>• What they must ensure the customer has; e.g. PIN.</li> </ul>
<b>Acquirer</b>	<ul style="list-style-type: none"> <li>• What a merchant must do; e.g. make available a receipt, and</li> <li>• Stringent encryption requirements to keep cardholder information secure.</li> </ul>
<b>Merchant</b>	<ul style="list-style-type: none"> <li>• The minimum requirements of what they must be capable.</li> </ul>
<b>Devices</b>	<ul style="list-style-type: none"> <li>• The minimum requirements of the actual hardware that cardholders use to initiate their transactions.</li> </ul>
<b>Switches</b>	<ul style="list-style-type: none"> <li>• What information gets exchanged,</li> <li>• How, when, and how quickly it is exchanged, and</li> <li>• Formats for the data.</li> </ul>

## What device types require approval within CECS ?

Two device types require approval within CECS:

- Pin Entry Device (PED)
- Unattended payment terminal (UPT)

## Why is there a NZ specific registration process?

In NZ we adhere to standards as prescribed by PCI Security Standards Council (SSC). While the CECS device security standards are closely aligned with current New Zealand and/or international standards, from time to time there will be differences within the local market.

The NZ CECS device standards will recognise those differences, clarify the interpretation of the international standards and, where required, define how they apply in New Zealand.

In aligning our requirements in this way we make sure that we are applying both national and international best practice in a fair and transparent manner.

## What is the device registration process?

The device registration process includes an assessment of the following:

- the PCI letter of approval has been granted,
- all relevant supporting documentation has been provided,
- the device is at an appropriate lifecycle stage for use in NZ, and
- there are no known security threats on the device at the time of the application.

PNZ participants must ensure that only registered device models are being used in NZ.

## When is a device registration required?

If you have a device model that does appear on the PNZ list of approved devices it must be registered by PNZ before it can be used in NZ.

## What are the registration criteria?

The criteria for registering a device model are:

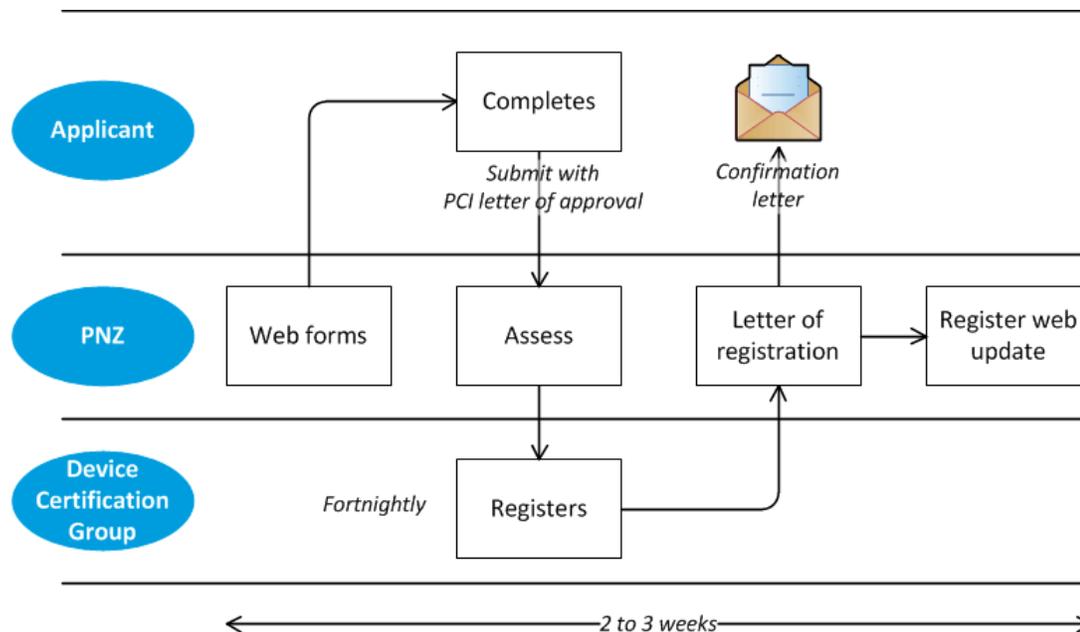
- a letter from the PCI SSC confirming that the model conforms with a version of a PTS standard,

- the version of the PTS standard to which the application relates is specified on the table of device lifecycle dates, and
- the date of registration of the device model will be before PNZ stops registering models of device that comply with the version of the PTS standard.

## How does the authorisation process work?

When a device comes to PNZ for authorisation, PNZ will check that each device has the relevant paperwork required for an approval, and then enter the application into the queue for assessment. Assessments will be made within a 10-day period. When approval has been received the device may proceed to the switch for testing.

The diagram below illustrates the authorisation process:



## What information is required to adequately identify a device?

A device submitted for approval must be identified appropriately. Each device will require the device's:

- manufacturer,
- model number,
- hardware and firmware
- version,
- PTS approval number,
- approval version and class, and
- approval expiry date.

The device identifiers will be included in the approval letter and on the CECS list of approved devices.

If an identical PED is used across a family of devices, vendors are cautioned against using a hardware version number that may restrict approval only to that device model.

## Where can I find a list of currently approved devices?

This can be found on the PNZ website under [CECS device register](http://www.paymentsnz.co.nz/clearing-systems/consumer-electronic-clearing-system/device-register) (http://www.paymentsnz.co.nz/clearing-systems/consumer-electronic-clearing-system/device-register)

## Why a device lifecycle?

We need to make sure that each model of device is secure enough to protect every pin from unauthorised use. The device lifecycle describes the framework in which we do this.

It also allows greater control over the distribution of devices in market and ultimately better protects the consumer electronic payments system.

## What is the device lifecycle?

The device lifecycle describes the process a device goes through from market entry to market removal. The table below lists the defined lifecycle stages.

Stage	Lifecycle	Description
1	Device registration	Initial approval of a device model for use in NZ that complies with a PCI PTS standard.
2	No new registration	The date PNZ will stop registering models of devices that comply with a PCI PTS standard; i.e. PNZ will decline any application for registration received after the published date.
3	No new connections	The date from which any new devices of the model can no longer be connected to EFTPOS network.
4	Sunset	The date that devices of the registered models of the device must be disconnected from the EFTPOS network.
5	Disconnect due to compromise	Process for disconnection registered models from the EFTPOS network if the model experiences a security breach.

## What are the device lifecycle dates?

The device lifecycle dates are the dates associated with each of the device lifecycle stages. They are published here <http://www.paymentsnz.co.nz/clearing-systems/consumer-electronic-clearing-system/device-dates>

## Why are the PNZ dates different in some instance to the PCI dates?

PCI provide date guidelines and do not mandate the removal of devices from a market. It is the role of Payments New Zealand to set dates that make sense for New Zealand. The underlying device lifecycle framework ensures that the dates are achievable and that we have clear, robust processes to support the transition through each device lifecycle stage.

## What are the details of each stage of the device lifecycle?

### 1. Device registration

PCI develops the standards for PIN security in terminals and manages the technical and operational requirements for protecting cardholder data.

Each version of the standard has a 36 month lifecycle to keep pace with technological innovation and changes in security threats. If a device is approved under these standards, PCI gives the vendor a letter that includes when the approval expires.

PNZ maintains a register of EFTPOS devices that records the following information for each model of device registered:

- date of registration,
- manufacturer,
- model number,
- hardware/firmware,
- version,
- PTS approval number,
- approval version and class,
- date the approval expires,
- any date determined by PNZ from which devices of the registered model must not be connected for the first time to the switching network,
- any date determined by PNZ from which all EFTPOS devices of the registered model must be disconnected from the switching network, and

- any date which models of EFTPOS device that comply with an old version of a PTS standard will no longer be registered.

Acquirers ensure the devices that are used by their merchants are listed on the EFTPOS device register.

## **2. No new registrations**

PCI phases out the old PTS standards, then sets a date from which PNZ will stop registering models of devices that conform to the old standard.

PNZ discloses the date by:

- recording the “no new registrations” date on the EFTPOS device register,
- notifying (in writing) participants, switch companies, and terminal vendors,
- ensuring from that date PNZ stops registering models of that device.

## **3. No new connections**

PNZ sets a date from which new devices that conform to the old standard must not be connected to the EFTPOS network.

PNZ discloses the date by:

- recording the “no new connections” date for that model on the EFTPOS device register, and
- notifying (in writing) participants, switch companies, and terminal vendors

Acquirers ensure from that date its switch does not connect new devices that conform to the old standard.

## **4. Sunset**

PNZ sets a date from which devices of a registered model conforming to the old standard must be disconnected from the EFTPOS network.

PNZ discloses the date by:

- recording the “disconnect” date for that model on the EFTPOS device register,
- notifying (in writing) participants, switch companies, and terminal vendors,
- (prior to the sunset date) publishing on the PNZ website monthly information about the devices subject to the sunset date, and
- (on the sunset date) removing the model from the EFTPOS device register.

Acquirers ensure from that date its switch disconnects the devices that conform to the old standard.

## 5. Disconnection due to compromise

Under the rules, an EFTPOS device is compromised if it fails to protect a cardholder's PIN from unauthorised disclosure or use.

PNZ is responsible for leading the high-level EFTPOS industry response to the compromise event.

PNZ responds to the compromise event by:

- making the decision as to whether or not to require disconnection of a model of device that failed to prevent unauthorised disclosure or use of a PIN,
- providing written notification to all participants, switches, the Reserve Bank, and terminal vendors of the compromised model,
- providing public notification on PNZ's website about the compromised model,
- requiring acquirers to ensure switch companies disconnect the devices from the disconnection date, and
- (on the disconnection date) removing the model from the EFTPOS device register.

The switches are responsible for disconnecting the devices of the compromised model from the EFTPOS network. Switches also manage the operational response to the compromise.

## Where can I find a list of device lifecycle dates?

These can be found on the PNZ website under [CECS device dates](http://www.paymentsnz.co.nz/clearing-systems/consumer-electronic-clearing-system/device-dates) (http://www.paymentsnz.co.nz/clearing-systems/consumer-electronic-clearing-system/device-dates)