

**Disclaimer:** Whilst every effort is made to ensure accuracy, SEA-GP (Brisbane) does not accept any liability for any injury, loss or damage incurred by or reliance on the information contained within this information sheet.

## What is Public Key Infrastructure (PKI)?

Public Key Infrastructure (PKI) is a combination of policies, procedures and technology allowing you to transfer information and images between computers safely and securely.

The main benefit of PKI is it allows you to send and receive health information securely and privately. With PKI, you know for sure:

- Who sent the message (authentication);
- That the content hasn't changed between sender and receiver (integrity);
- That the sender stands behind the message (non-repudiation);
- And that only you, as the intended receiver, can open the message.

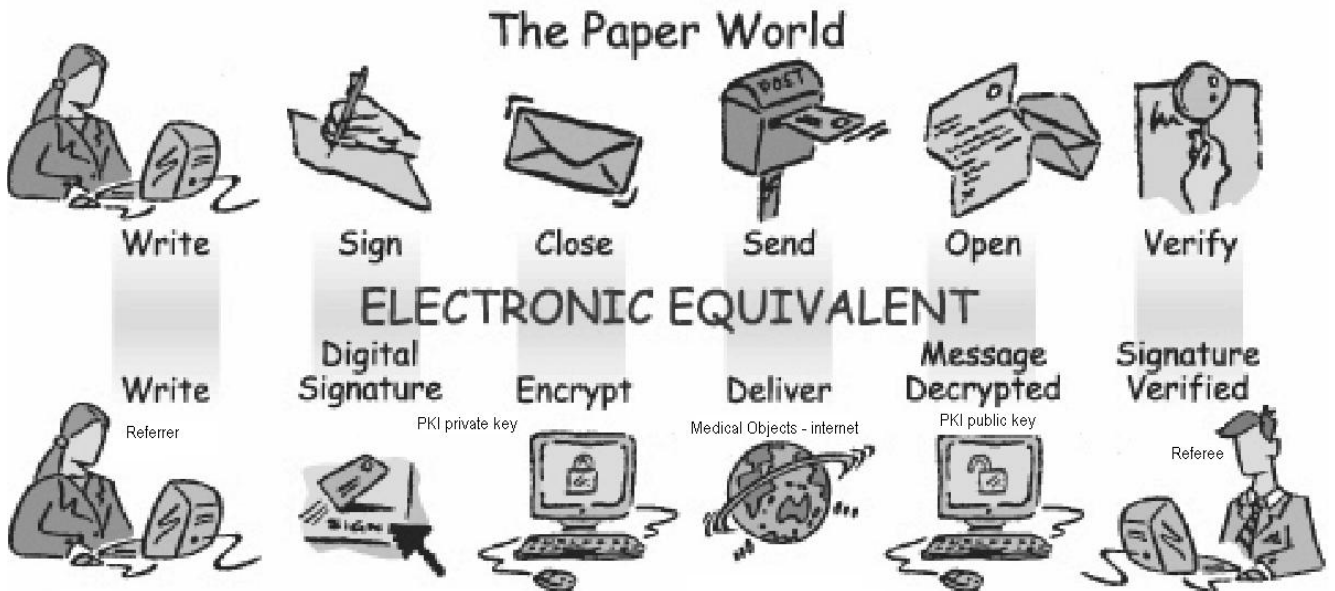
With PKI, you can securely send a file to someone, and know he or she is the only one who can open it. You can also receive a file, confident it has been sent to you securely.

## What is the role of Medicare (previously of HeSA)?

Medicare is a Gatekeeper accredited Registration Authority which means they are authorised to:

- Conduct Evidence of Identity (EOI) Checks;
- Generate Digital Keys and Certificates;
- Issue Digital Keys and Certificates;
- Suspend Digital Keys and Certificates;
- Revoke Digital Keys and Certificates; and
- Re-key Digital Keys and Certificates.

The processes and procedures utilised by Medicare to issue and manage PKI Digital Keys and Certificates means that these electronic signatures carry the same legal value as a written signature and therefore allow some transactions to be paperless, which means quicker and more accurate flow of important health information. *Figure 1* provides an example of the paper and electronic equivalent signatures.



**Figure 1 - Paper versus Electronic Communications World**

## What is a Digital Certificate?

A digital certificate is an electronic document used to identify an entity and bind that identity to a public key. In the case of the Healthcare PKI, the digital certificate identifies either an individual or a 'health sector entity'.

What is a Healthcare **Individual** Certificate? The Healthcare Individual Certificate is used to identify a **person** from whom a message has been received and allows the sender to attach a digital signature. To obtain one, a person needs to supply their email address.

What is a Healthcare **Location** Certificate? The Healthcare Location Certificate is used to identify the **location** from which a message has been received and allows a number of people at the same location to sign and encrypt messages. Practices use this for one Medicare claiming.

## Why Use a Digital Certificate?

Digital Certificates are utilised to send and receive information over the public internet in a secure manner and ensures the authenticity, integrity and non-repudiation of the information being sent.

## Why is an Individual Certificate Required?

The Trinity - Medical Objects Referral Client applications utilise the Medicare **Individual** Digital Certificate **only**. Being a tool that provides functionality to do electronic referrals and it being a legislative requirement that referrals are signed by an individual practitioner or health care professional this application will only support Medicare Individual Digital Certificates.