Digital Signatures and Digital Certificates perform different functions and therefore cannot replace each other. At some point in your life, you might need both products for very different purposes. So it will be useful to know what they are, how they differ and how they can make a difference to your online security requirements.

Digital Signature: A 'Virtual' Signature

A popular misconception is that a Digital Signature is simply a scanned, digital copy of your handwritten signature. This is not true.

A Digital Signature is actually a digital attachment, i.e. a 'virtual' signature, that establishes the signer's identity. This identity cannot be altered, neither can the contents of the document to which the signature is attached. If any attempt is made to do either, the Digital Signature will be invalidated which will make the entire document redundant.

A digital signature provides 3 critical advantages:

- **Authenticity**: It ensures that the contents of the document are not tampered with.
- **Data integrity**: It ensures that the receiver receives the same document sent by the sender with all its data intact.
- **Non-repudiation**: It prevents the signer/sender from denying signing the document at a later stage. In other words, it makes the document 'binding'.

Digital Certificate: Affirmation of Legitimacy

A Digital Certificate is a small server file that establishes the credibility and legitimacy of the information being sent. In the case of a website, this information could establish site/domain ownership, location, etc.

It is always issued by a Certificate Authority (CA) like an online security agency, tech company, government organisation or department, etc. The CA runs a background check of the applicant before actually issuing the certificate. This then acts as a seal of approval with regards to the applicant's genuineness and authenticity. Furthermore, the recipient can confirm the legitimacy of received information by verifying the sender's ownership.

A Digital Certificate scrambles the data being sent so that only the recipient with the correct 'key' can decrypt and access the real data. Thus, it prevents unauthorised personnel from eavesdropping into the data exchange, and ensures tamper-proof data flow between the sender and receiver.

So how exactly are they different?

Despite common advantages like authenticity and legitimacy that both Digital Signatures and Digital Certificates provide – which gives the impression that they are both the same product – there are plenty of differences between the two.

1. **Purpose**

A Digital Signature verifies and establishes the source of a document and the sender's identity. The document could be a contract, an employment offer, a tender or bid, a quotation, tax returns or anything else.

A Digital Certificate on the other hand, establishes the credentials, legitimacy and ownership of an online asset such as a website.

2. **How secure is it?**

A Digital Signature protects the rights of both the document's sender and receiver. It ensures that the sender cannot be held accountable or liable for documents not signed by him. At the receiver's end, it ensures that the sender cannot non-repudiate signing the document at some later time.

A Digital Certificate protects information-exchanging parties from cyber attacks, eavesdropping, cross-site scripting, and other such security challenges. It also provides assurance that users are dealing with a reliable and genuine digital asset (e.g. a website).

3. **How to get it?**

A Digital Signature can be obtained from an online security agency or issuing authority. Individuals applying for a Digital Signature must provide valid personal identification documents. The Digital Signature is then issued in their name and for a specific purpose (different signatures for different purposes).

A Digital Certificate is issued by a Certificate Authority (CA) after conducting a background check on the applicant.

4. **Encryption method**

A Digital Signature is created based on Digital Signature Standard (DSS) and uses a SHA-1 or SHA-2 algorithm for message encryption and decryption.

A Digital Certificate works on the principles of Public Key Cryptography Standards (PKCS). It is created in the X.509 format.

Both Digital Signatures and Digital Certificates serve different purposes, both of which are essential to security in today's digital world.