acloserlook

Issue 3 - June 2017

Securing electronic records for the Evidence Act

What you need to know about digital signatures.

An ongoing series

For 20 years, PwC has been a Certifying Authority authorised to certify document imaging systems as an "approved process" for the purposes of Section 116A(6) of the Evidence Act. This is a series of articles to share its experience in this very niche sector of document digitisation.

To view our other A Closer Look pieces on Evidence Act, please visit www.pwc.com/sg/evidence-act

Highlights

- Why is it necessary to distinguish between a scanned hardcopy and an "electronically born" document?
- Is the use of digital signature a compliance criteria under EA?

Many organisations in Singapore have embarked on the journey of converting existing paper documents into electronic forms. This is done through scanning (commonly referred to as digitisation) of paper documents.

However, digitising documents is only the first step to the life cycle of an electronic document. The digitised documents are usually uploaded to an electronic document repository and organised into subject or object folders.

An issue that quickly surfaced is how one would know whether a document in the repository originated from a scanned hardcopy or was an "electronically born" document; the latter referring to documents that started their existence in electronic forms, for example a Word document converted to PDF or an email attachment.

This differentiation is necessary because the scanned images would have been through the Evidence Act (EA) certified process while "electronically born" documents have not. Another reason is that most repositories would deploy a convention of storing documents in a standard format (e.g. PDF, which is very common nowadays); it is not possible to infer from this standard format the origin of the document (e.g. how to tell that a PDF was produced from a scan or was an email attachment).

Because of this, we need a way to be able to positively identify documents in a repository that originated from an EA certified process. Over the years, organisations have explored various methods of doing this, but eventually, it was agreed that digital signature is the answer.

> A digital signature is a string of numbers that is derived using mathematical formula, based on the contents of the document and a secret key. The property of the digital signature is such that even if one bit of the document is changed, the entire digital signature is "broken" – this means, it will fail authentication.

In the EA, specifically section 116A on presumption in relation to electronic records, nothing is said about digital signature. There is also no mentioning of digital signature in the Evidence (Computer Output) Regulations, which is the subsidiary legislation of the EA. Therefore, the use of digital signature is an industry practice, not a compliance criteria.

pwc

So where did the use of digital signature come from?

Back in 1997, when PwC started performing EA certification, we realised that we need a means to positively identify electronic images that are produced through an approved process. This allows the scanning operators and ourselves to know the documents that are covered by the certification. A study of various methods was undertaken to narrow down to digital signature.

Since then, PwC has advocated the use of digital signature in all certified process, and over time, this has become the industry practice.

Today, most sites with EA certified process apply digital signature to scanned documents. This has helped to testify that the documents have been produced from a certified process and also prove that the documents have not been manipulated or changed while they are in the repository.

For organisations that are selecting document repository systems, it would be useful if the system has built-in features to facilitate the generation, capturing and storing of digital signatures. Some repository systems may allow third-party add-ons. However, we have come across systems that could not support digital signatures and alternative methods to work around the limitation have to be devised.

If you are interested in exploring this topic further, feel free to engage us in a discussion on the following:

- How to secure digital signatures?
- What about Evidence Act for the electronically born documents?

Contact information

For a deeper discussion please contact

Chia Peiru
peiru.chia@sg.pwc.com