# ELECTRONIC AUTHORISATION OF DOCUMENTS AND EXPENDITURE

**PARTNER**
**AUDIT & ASSURANCE**
**KEVIN FRANEY**

## Authorising Documents & Expenditure in an Electronic World

In an increasingly digitised world and with the impacts of COVID-19, the next natural step is for organisations to implement electronic approval processes (e-signing). We are beginning to see organisations commence the use of electronic signatures to sign documents and to authorise transactions.

## What are e-Signatures?

Electronic signatures, or e-Signatures, are the electronic version of manually handwritten, physical signatures (known as 'wet signatures'). Like a wet signature, an e-Signature is a legal concept; its purpose is to bind a signatory to a document, in a way that proves the person signing is who they say they are.

There are several ways of achieving this, some of which are more reliable than others. Examples include a:

- digitised version of a physical signature, for example a scanned image of the signature saved in an electronic format and pasted into a document
- typed name at the end of an email message
- digital signature, which uses encryption and decryption technology alongside public key infrastructure (PKI).

The latter technology (digital signatures) requires the signatory to prove their identity through an authentication process. This prevents tampering, making it the most secure and reliable option. It is the foundation on which almost all enterprise e-signature software is built.

## Digital versus electronic signatures

Although the terms are similar, e-signatures and digital signatures are quite different.

An e-signature is a legal concept and a catch-all term for a variety of methods (see those listed above) for authenticating signers.

Digital signatures are a very specific security technology for authenticating and securing objects using public/private key cryptography. The signature is authenticated with a certificate-based digital ID, typically issued by a trusted, third party certificate authority.

A good, enterprise e-Signature platform will use digital signatures.

## What weight do electronic approvals have and what controls do I need to support using them?

Those charged with the governance of your organisation are required to design the control environment to suit their business needs and reduce the risk of fraud and error to an acceptable level.

As auditors, we examine whether organisations have suitably designed and implemented effective approval controls. This means that if your organisation intends to use electronic means to approve documents or expenditure, we will review how you have designed your controls to reduce the risk of fraudulent approvals being accepted.

The Electronic Transactions Act (NSW) 2000 and the Electronic Transactions (Queensland) Act 2001 outlines that if a person's signature is required then three tests must be met for the signature to be valid:

1. Identification—a method must be used to identify the person/people and capture their intentions. For example, the signing officer is bound by their declaration even if they did not send the communication but rather consented to someone sending it on their behalf.
2. Reliability—the process must maintain the integrity of the information. For example, the information must remain complete and unaltered throughout the course of a transaction.
3. Consent—the recipient must agree to receive digitally signed documents.

A scanned image of a signature on an unsecured document fails these tests, because the document:

- fails to identify who attached a picture of the signature—anyone can scan your signature from a public document and attach it to an approval form without your knowledge
- can be manipulated to add the signature, varying what was intended to be approved.

Enterprise e-signature platforms require a signatory to prove their identity in order to sign the document. This provides evidence of their identity, and then 'seals' the document to prevent it being easily edited. These controls increase its reliability and add an extra layer of security.

## Policies on their own are not enough

Most organisations have reviewed their control environment and developed policies that aim to address these three tests. But they are not always adjusting their control activities to implement their policies. This means that processing staff are inappropriately accepting documents with just pictures of signatures or email approvals.

## Does an email from me count?

Generally, no, because a basic email also fails these tests.

Over the last couple of years, we have seen an increased number of fraud attempts whereby fraudsters impersonate an email account holder to change bank account details for employees or vendors.

This shows that emails lack the security to evidence the identity of the account holder and the account holder's intentions. Emails are not reliable because they can be manipulated before being sent or once received.

Organisations need to consider the risks of accepting email approvals and requests when designing their control environment and implementing control activities. This includes implementing complimentary controls to verify information, such as calling the sender from independently sourced contact details from the entity's website rather than the footer of the email.

The information provided in this document has been provided with thanks from the Queensland Audit Office