No PEXA digital certificate policy? You're at risk.

Does your firm have effective policies for maintaining the security of digital certificates? Are digital certificates being shared within your firm? Below are some of the risks and consequences and what you should do about it.

PEXA digital certificates are a necessary part of the electronic conveyancing process in Australia. Digital certificates are an encrypted digital signing technology that allows users to electronically sign documents on PEXA. They are issued to an individual within a subscriber's business and can only be accessed by using a dedicated PIN.

Once used within the PEXA Workspace, the signature represents confirmation of the transaction request and the client's instructions. It is binding and traceable back to the individual who is responsible for its proper use.

The digital certificate and the PIN should not be shared with anyone else and only used by the owner. Sharing the digital certificate is a breach of the Model Participation Rules issued by ARNECC and sections 4.2 and 4.5 of PEXA's Security Policy. It is important that subscribers and users take the security policy and the participation rules requirements seriously as the Registrar in each jurisdiction has the power to audit compliance with them including how digital certificates are used. Further information about the compliance examinations can be found in ARNECC's guidance note no. 6.

Sharing your digital certificate is the equivalent to letting someone else sign your signature on documents. While you may think that you can trust the staff member to use the digital certificate appropriately we don't always know what staff are going through or dealing with. In past fraud cases staff were often suffering from gambling additions or other financial or personal problems that no one in the firm knew about.

If something does go wrong the damage to the firm's reputation could be significant as not only something fraudulent happened, but the firm and the digital certificate owner actively allowed it to happen by arming the fraudster with the means to do it.

The dishonest or fraudulent use of a digital certificate by a practitioner in a conveyancing transaction to misappropriate trust money or trust property held by the practitioner may well be a trust default and excluded from cover under LPLC's professional indemnity policy. Alternatively, if the conduct does not constitute a trust default but gives rise to a claim which LPLC is obliged to pay under the policy, any person who committed or permitted the dishonest or fraudulent use of the digital certificate is required to indemnify us for the loss paid out and for all defence costs incurred. See clause 14(b)(v) of the current defence costs exclusive policy.

Firms that develop their own robust policy for the effective management and security of digital certificates create compliance checkpoints. To help you develop an office policy to manage the security of digital signatures we have created a Key Risk Checklist: Electronic property transactions – office management. We encourage all firms using PEXA to develop a written policy on the use of all digital certificates.