COMMONLY ASKED QUESTIONS ABOUT DIGITAL ENGINEERING DOCUMENTS

By José Vera, P.Eng., MEPP

In recent years, digital engineering documents have become ubiquitous. For example, some municipalities now accept only digital documents for building permit submissions, including engineering drawings, plans, reports and specifications. Although the use of digital documents comes with several advantages over paper documents—they are easy to access and take up less physical storage space than paper—their use also presents some challenges, such as the risk of unauthorized alteration and potential for digital seal misuse. Consequently, PEO's practice guideline *Use of the Professional Engineer's Seal* requires practitioners who use digital engineering documents to adopt a form of security appropriate for the circumstances.

Below are four commonly asked questions answered through real-life scenarios from practitioners using digital engineering documents. The solutions described here were developed by practitioners who were kind enough to share their methods with PEO's practice advisory team.

1. How can I verify that the digital engineering document I issued was not altered?

With additional precautions in place, you can ensure that your digital documents are not altered after they have been issued to clients. Consider this scenario: Engineering firm XYZ issues sealed building permit drawings in a digital format to client ABC. Months pass before a building department contacts XYZ to ensure that the digital drawings they received from client ABC are, in fact, the ones that were issued by XYZ and that the digital drawings were not altered in any way.

XYZ has a digital document verification process in place that relies on Secure Hash Algorithms that generate hash values. The hash value is analogous to a digital fingerprint. Even a minor change, such as adding a comma to a digital drawing, will result in a different hash value. Specifically, just before the digital drawings were issued to client ABC, the information technology (IT) department of XYZ generated hash values for each drawing.

XYZ's IT team finds that the hash values of the digital drawings received by the municipality are identical to the hash values of the digital drawings that were issued to client ABC. Hence, XYZ was able to validate that the drawings were not altered in any way. XYZ has reassured the building department and addressed its concerns. Consequently, the building department can now proceed with approving the building permit. Thanks to XYZ's preparation, any concerns regarding the authenticity of the digital drawings were promptly and effectively addressed.

2. How can I better protect my digital seal from misuse?

One approach is to implement a watermark on digital seals to deter unauthorized copying. Consider this scenario: The Ministry of the Environment, Conservation and Parks (MOECP) contacts engineering firm DEF to confirm that an environmental site assessment (ESA) report, which they received from client JKL in a digital format and that contains the DEF logo, was, in fact, issued by DEF. Furthermore, the MOECP notes that the ESA report contains a digital seal of an engineer named Jane Q.

The engineering manager at DEF is assigned to reply to the MOECP and recalls that there was an engineer by the name of Jane Q working at DEF, but she recently retired and is travelling around the world and is therefore unavailable to confirm that she issued the report. However, the manager checks the transmittal record and confirms that at no time was an ESA report issued from DEF to client JKL. This development leads the manager to inform the MOECP that DEF did not issue this report.

The MOECP accepts the manager's conclusion that the report was not issued by DEF; nevertheless, the MOECP still wants to confirm if the seal is authentic. DEF has a process in place where all the digital seals of their engineers contain a watermark to deter unauthorized copying of sealed digital engineering documents and their information. Upon review of the ESA report, the IT team at DEF verifies that the seal within the report received by the MOECP does not have such watermark, and therefore could not have been sealed by employee engineer Jane Q.

continued on p. 22

continued from p. 21

The MOECP contacts JKL to inform them that the ESA report in question was not issued by DEF, and after discussions with DEF, the MOECP now has reason to believe JKL used a fabricated seal. Consequently, the MOECP reports this issue to PEO. Finally, JKL is convicted of breaching the *Professional Engineers Act* by the Ontario Court of Justice and fined for use of a fabricated professional engineer's seal.

3. My firm uses Notarius in Quebec and DocuSign in the United States; can we use either of them in Ontario?

In short: PEO does not endorse any specific digital signature software. Consider this scenario: Engineering firm GHI is a large transnational firm. The engineering manager at their Ontario office, Michel S., recently read PEO's *Use of the Professional Engineer's Seal* guideline and notes that the guideline requires practitioners to use a form of security for digital engineering documents that, in the judgment of the practitioner, is appropriate for the circumstances. Therefore, Michel S. determines that GHI's Ontario location should select a digital signature software to comply with this requirement.

Michel S. is familiar with Notarius, which provides digital signatures and is used by GHI's Quebec office. Furthermore, Michel S. finds out that the US offices of GHI use another product for digital signatures known as DocuSign. Michel S. contacts PEO to determine if GHI can use either of these two products in Ontario.

While speaking with practice advisory staff at PEO, Michel S. learns that PEO does not endorse any specific digital signature software solution. Furthermore, PEO's position is that practitioners can use any digital signature software that meets the requirements outlined in the *Use of the Professional Engineer's Seal* guideline. After reviewing the product specifications, Michel S. concludes that either Notarius or DocuSign will provide an appropriate security method for GHI's Ontario location.

4. Is there a secure method for digital documents that is completely foolproof?

Often, practitioners will try to find a secure method that prevents inappropriate tampering of digital documents in every possible scenario. However, IT security experts will tell us that no security method is completely foolproof, including the solutions presented in this article. Therefore, practitioners should place reasonable reliance on the recommendations of IT security experts to minimize the risks associated with using digital engineering documents. Furthermore, there may be better solutions than those presented in this article, or at least solutions more appropriate to the specific circumstances faced by practitioners, meaning there is even more reason to rely on an IT expert.

PEO's practice advisory team is available by email at practice-standards@peo.on.ca and welcomes questions from practitioners looking for general information on their professional obligations, such as best practices involving the use of digital engineering documents. However, practitioners looking for assistance on specific IT security-related issues should always contact their IT department or their IT consultant, who can best address technical issues involving security of digital engineering documents. e

FURTHER READING "A method for verifying integrity & authenticating digital media," by Martin Harran, William Farrelly and Kevin Curran, *Applied Computing and Informatics*, Volume 14, Issue 2, July 2018, p. 145–158, sciencedirect.com/science/article/pii/S2210832717300753

José Vera, P.Eng., MEPP, is PEO's manager of standards and practice.