



BULLETIN 60: SIGNATURE, SEAL AND DELIVERY OF ELECTRONIC DOCUMENTS

FIRST EDITION: OCTOBER 2009

This bulletin has been approved and formally adopted by resolution of the AIBC Council. It contains guidance and council rulings on the use of electronic certificate technology to sign/seal and deliver documents.

1.0 Introduction

1.1 Previously the AIBC had not sanctioned the application of an electronic image of a member's professional seal to documents requiring her/his signature and stamp or seal.¹ The reasons for this relate to public protection, regulatory requirements of the *Architects Act*, security of the seal, and document integrity concerns described in more detail in this bulletin. As a result, any document requiring a member's seal had to be physically printed out and then dated, signed and hand-sealed.

1.2 The world has changed substantially since the 1920s when the *Architects Act* was first proclaimed. Modern legislation, that makes electronic documents as enforceable as hard copy, and allows for electronic production and delivery, is now in place in British Columbia. This legislation can be applied to the *Architects Act*, allowing "electronic signature, seal and delivery" so long as adequate measures are in place to ensure:

- security and verification of electronic documents; and
- regulation of use and revocation of a member's seal.

1.3 The AIBC has secured electronic document certification technology for use by its members. Along with the Association of Professional Engineers and Geoscientists of British Columbia, the AIBC has contracted certification services through Notarius, a not-for-profit certification provider founded by the Quebec Society of Notaries Public. Notarius provides

¹ The Act and bylaws require certain documents to be dated, signed and sealed or stamped by the architect. Until now, this meant the application of a physical imprint of the seal or ink stamp. For ease of reference, the term "seal" will be used to refer to either the embossed seal or the inked stamp.

the technology and security services through which professionals can sign, seal and deliver electronic documents safely and in a manner that meets AIBC regulatory requirements.

2.0 Terminology

2.1 The terminology can be confusing when equating the physical act of signing and sealing a document in the “real world” to doing so electronically. In the electronic world, a document is signed or sealed by the application of an electronic “certificate” (also called a digital certificate) unique to the user. The electronic/digital certificate is a security tag which identifies the sender and locks down the document. When you apply your digital certificate to a document, it prevents you or anyone else from making any unauthorized or undetected changes to that document. Because the certificate is unique to the user who controls its use by secure password, the certificate is used to verify that the user (and only that user) actually signed and sent the document.

2.2 Applying an image (picture) of a person’s professional seal and signature is not the same as digitally (electronically) signing or sealing that document. The picture of the signature and seal can be applied in many places on a document. The document is not officially electronically/digitally signed or sealed until such time as the electronic/digital **certificate** is applied. The electronic/digital certificate is applied just once, when the document is complete and ready for electronic archiving and/or transmittal to an intended recipient.²

3.0 Regulatory Considerations

3.1 The following is a brief explanation of the four driving considerations that must be addressed when contemplating electronic signature, seal, and delivery of documents.

Revocability of the Certificate/Seal

3.2 The architect’s seal is a signal to the world that at the time the document is signed and sealed, the architect was a member entitled to practise. Because the profession of architecture is recognized as both a right-to-practice and right-to-title regime, regulated by the AIBC, the public interest (and the legislation) demands that the professional seal always remain the property and under regulatory control of the AIBC. An AIBC member’s seal must be returned when that member ceases to be a member and/or loses his or her right to practise.

3.3 To meet these regulatory requirements, an AIBC member can only get a professional seal with the express written permission of the AIBC. The seal has to be obtained from a

² It does not matter where the certificate is placed in the document so long as it is placed on the final version. The technology allows a user to customize how the certificate will appear on the document. It also gives the user the option of including a picture of his/her professional seal and physical signature in the certificate image. This can lead to some confusion. Applying an image of the professional seal and/or physical signature is NOT the equivalent of “digitally signing/sealing” the document. Signing and sealing in the electronic world requires applying the **digital certificate**.

supplier authorized by the AIBC, and must be returned to the AIBC on demand. These rules must apply equally in the physical and electronic worlds.

3.4 In the electronic world this can be done through an arrangement between the AIBC and a third-party provider that allows the AIBC to retain control of issuance and revocation of digital certificates.

Security of the Certificate/Seal

3.5 There must be a way of ensuring that only an authorized person (in this case an MAIBC who meets the requirements for signature/seal under the Act, bylaws and bulletins) is able to apply his/her certificate to an electronic document. This is fundamental to the public protection mandate of the AIBC, as well as to protecting architects. To ensure this regulatory imperative, the AIBC must be able to grant permission for issuance and use of the certificate, and must also be able to revoke permission if and when circumstances warrant.

Verification/Authentication of the Document Now and Into the Future

3.6 Both the **identity** and **authority** of the person sending an electronic document must be verifiable. This is done through certificates issued by Notarius in two ways. First, only members with current access rights to the technology and a secure password can apply their certificate to a document. Second, once a certificate is applied, the document contains technology that enables any recipient to determine whether or not the certificate was valid when applied. If the certificate expires or is revoked (loss of membership/practice rights), the technology will flag the document and let the recipient know the certificate is invalid.

3.7 Once verified, the document must also be able to be authenticated. Authentication is the process through which a person can prove that the electronic document sent or received is the original and has not been altered in any way. Applying a certificate does this by effectively “locking down” the document. Any changes made to the document after the certificate has been applied is flagged and tracked.

Document Storage

3.8 The average lifespan of an electronic document has variously been reported at between three to five years - not a long time given the potential for professional accountability and legal liability issues to arise many years later. While the AIBC has taken steps to address considerations of security, revocation, and authentication/verification, it cannot directly address storage issues. This is something that must be addressed by the member. This said, the AIBC recommends, as a matter of prudent practice that members have in place document storage, backup, and recovery systems that meet legal and regulatory requirements. Members are strongly encouraged to consult with legal and information technology professionals to determine if they are adequately protected.

4.0 Obtaining an Electronic Certificate

4.1 Members can purchase a licence to use a unique certificate that they control through the use of secure passwords. A member wishing to apply for an electronic certificate may do so by visiting the AIBC section on the Notarius website and following the directions set out on that page. The website address is:

(http://www.notarius.com/en/clientele_AIBC.html).

5.0 Ten Requirements for use of a Digital Certificate:

5.1 Electronic signature, seal and delivery is permissible **if and only if** an MAIBC member with current authority to sign and seal documents under the *Architects Act*, bylaws and AIBC rules, acquires an electronic certificate issued by Notarius under the authority of the AIBC.

5.2 No document bearing one or more images of a member's professional seal and/or signature in electronic form is valid unless that member applies her/his Notarius/AIBC digital certificate to that document.

5.3 Members must use their digital certificate issued by Notarius under authority of the AIBC for all documents requiring their signature and seal which they intend to sign/seal and or deliver electronically.

5.4 Members must not disclose any personal codes or marks enabling any other persons to use their digital certificate, including passwords, activation codes or verification codes used for identification purposes. **Failure to comply with this obligation may result in the immediate revocation of the certificate by either or both the AIBC and Notarius.**

5.5 Members must inform Notarius and the AIBC as soon as possible of any changes to their contact information including e-mail address.

5.6 Members must use their computer equipment securely, remembering to close their certificate software or log out of the application before leaving their workstation unattended.

5.7 Members must inform Notarius and the AIBC immediately if they believe the confidentiality/security/integrity of their certificate has been compromised.

5.8 Certificate and software licences for the certificate technology cannot be sold, transferred, distributed or otherwise assigned without the express written permission of Notarius and the AIBC.

5.9 Members shall not attempt to apply a certificate if it has been cancelled, suspended or revoked.

5.10 Members shall follow the destruction method specified by Notarius if their certificate is cancelled, suspended, revoked or otherwise is no longer valid or in use.

6.0 How digital certificates work in the “real world”

6.1 This bulletin deals primarily with the rules and rationale for digital certificates. It is not intended as a fulsome instruction manual on how to use and apply the technology. Notarius has technical support personnel who can assist via telephone as well as instructions and manuals on their website. This said, a few words on how the technology actually works is included in this bulletin as some additional rules and considerations need to be highlighted.

6.2 The Notarius technology is, essentially, applied is as follows:

- A person will create a document in any one of a number of different software applications. Reports, memos, letters, and other such documents are typically created in any one of a number of commercially available word-processing programs. These programs will typically also allow a person to create a signature block in which an image of a signature and professional seal can be applied.
- Once the document is created and the images are applied, it must then be converted to .pdf format. It is not necessary to have a Adobe Acrobat (in any of its versions) to use the technology. The software package provided by Notarius contains an application which allows users to convert their documents into .pdf format.

If the user does have Adobe Acrobat Pro, it can be configured to use the Notarius digital certificate to certify the document. Notarius technical support can assist in configuration if the user is unfamiliar with digital certificate set-up in Adobe. The advantage of applying the certificate within Adobe itself is that the certificate block is more customizable than if the user were to use the Consigno application provided through Notarius. For “one-off” documents, this may be the preferable option. If, however, the user needs to certify a large batch of documents (like individual files for each sheet in a package of drawings as discussed later in this note), the Consigno application is likely the better option as it allows for batch “signing” capabilities.

- Once the .pdf file is created, it is then opened in the Notarius-provided software application (called Consigno) and the digital certificate is applied.

At this point the document becomes a valid electronically “signed and sealed” document.

6.3 The same principles apply to drawings created by CAD and related software applications. Images of a member’s professional seal and signature can be placed in each of the title blocks after which the document is then converted to .pdf format and the digital certificate is applied.

6.4 What is the best way to proceed when issuing a set of drawings, often running into tens if not hundreds of pages? Creating a single document with one electronic certificate, or creating multiple documents each with its own certificate? Either approach is acceptable

(and will be explained in more detail in paragraphs 6.7 and following below), so long as the following rule is respected.

Every person receiving a document bearing a member's signature and/or seal must be able to tell from that document that: (1) it is the current document; (2) it can be relied upon; and (3) if it is a revision of one or more previous documents, what those antecedent documents were and what changes have been made.

6.5 This rule applies in both the physical and electronic worlds. In the electronic world, any document to which a member's digital certificate is applied must contain information (either in the title block or in a tracking schedule) which indicates whether the document is the first issue or a revision. If the document is a revision, information on how that revision relates to its predecessor documents is also included.

6.6 If the document is one which will be printed out and provided in hard copy form to the recipient or others, wording in the form prescribed below must be added to each page (either in the title block or some other prominent location) signifying it is a paper copy of the electronic original as well as the conditions on which it can be relied.

This document has been electronically certified with digital certificate and encryption technology authorized by the AIBC and APEGBC. The authoritative original is in electronic form transmitted to you. Any printed version can be relied upon as a true copy of the original when supplied by the original author, bearing images of the professional seal and digital certificate or when printed from the digitally certified electronic file sent to you.

The document is then converted to .pdf format and the digital certificate is applied.

6.7 The recommended (best practice) when dealing with a multi-page set of drawings is to create a separate .pdf file for each drawing page. The Notarius technology allows for bulk/batch conversion of such files as well as bulk/batch certificate application. This method is similar to what happens in the physical world where a person has to physically apply the seal and physically sign each page. The advantage here is that the process is a lot quicker and easier in the electronic world. The individual digitally signed .pdf files for each drawing can then be "bundled" together in a single "zip" or other archive file for transmission or archiving as a single file containing many individual .pdf drawing files.

6.8 The main advantage to this method is that if a single sheet needs to be changed, that change can be made in the CAD/Design software, the revision tracking information can be typed into the template, and that page can then be converted into a single .pdf file and digitally certified. That page can then stand alone without having to convert and print the entire set again.

6.9 An alternative method, suitable for smaller sets of documents where changes are not anticipated, is to convert all of them into a single .pdf format file to which the digital certificate is applied. The advantage of this method is that the certificate only needs to be applied once. The disadvantages are that:

- a control sheet must be included detailing whether the set is original, whether it is a revised set, as well as each and every revision made to the set;
- each page of the bundle must include wording indicating that it is part of a complete set and can only be trusted if the set remains together; and
- the extra image that appears when the digital certificate is applied will only appear once in the set.

7.0 Feedback and future development of this bulletin

7.1 Members are encouraged to provide feedback on their experience with electronic signature, seal and delivery of documents both within the context of their own practices and in collaboration with engineering consultants and authorities having jurisdiction. Feedback may be directed to Jerome Marburg (jmarburg@aibc.ca).

The AIBC does not provide legal, accounting or insurance advice and expressly disclaims any responsibility for any errors or omissions with respect to legal, accounting or insurance matters that may be contained herein. Readers of AIBC documents are advised to consult their own legal, accounting or insurance representatives to obtain suitable professional advice in those regards.