ARIZONA

August, September, October 2006 Volume 9 No. 3

Using Digital ID's to Sign Professional Documents

BTR Policy and Rules Authorize Secure Electronic Signatures

by P. Douglas Folk, Esq. Folk & Associates, P.C.

Digital ID Rules Adopted. Arizona's Board of Technical Registration ("Board" or "BTR") has updated its rules and substantive policies to free registered design professionals – including architects, engineers, registered land surveyors, and landscape architects – from the need to use hand-written signatures to authenticate their professional documents when they are transmitted over the Internet or via electronic storage media. In June 2002, the BTR adopted a substantive policy statement recognizing two new laws that permit anyone to use secure electronic signatures-also known as digital signatures or digital I D's – wherever a handwritten signature is required as proof of the author's identity or to make an agreement legally binding and effective. These new laws make a handwritten signature unnecessary to "seal" professional documents stored on electronic media or transmitted via the Internet.

The BTR subsequently formalized its policy statement in an amendment to the rules concerning the use of professional seals. Its new rule – A.A.C. R4-30-304.G – explicitly states that registrants may use secure electronic signatures to "sign" their professional documents so long as certain conditions are met.

This new BTR policy allows design professionals to create and transmit professional documents electronically, and use them as record documents with the same legal protections afforded a traditional wet seal and hand-written signature. Digitally signed documents also have one other very important advantage over a traditional wet seal and manual signature; they are inherently tamper and copy proof. Any alteration of a digitally signed electronic file immediately destroys the seal and leaves a record of the alteration. Likewise, the digital ID cannot be removed from the file if it is copied or transmitted to someone other than the original recipient because this alteration will also make an indelible mark on the file. This unique security feature provides enhanced protection to the public and the design professional because the unauthorized duplication of a registrant's seal and handwritten signature is child's play with the high-resolution scanners and color photocopiers that are also available in the marketplace.

E-SIGN Validates Electronic Signatures. To better understand this new BTR policy, we must first understand the legal precedent for secure electronic signatures. In 2001, Arizona joined the rest of the nation by implementing the federal Electronic Signatures in Global and National Commerce ("E-SIGN") Act of 2000, to give legal effect to agreements and other records that exist only in electronic media. Two new state laws were enacted as part of Arizona's Electronic Transactions Act to secure E-SIGN's protections for electronic documents and transactions. A.R.S. § 44-7007, part of the state's commercial laws, states that a record, contract, or signature cannot be denied legal effect solely because it exists only in electronic form. Sub-section D of this same statute also states that an electronic signature satisfies any law that requires a signature. This law is revolutionary in its impact on electronic commerce because it essentially gives legal effect to any indication of a user's intent to have some electronic symbol serve as a signature-whether that is a facsimile of a handwritten signature, a digitized thumbprint, a typewritten name, or a check-box on a website marked "I Agree". Were it not for the second law authorizing secure electronic signatures, there might be room for some uncertainty about what really constitutes a registered professional's digital signature.

The second new law, A.R.S. § 44-7031, prescribes the legal criteria for a secure electronic signature, also known as a digital signature or digital ID. Anyone who uses digital authentication technology meeting the requirements of this law will obtain all the legal presumptions, rights and remedies afforded to electronic records, signatures and transactions.

BTR Recognizes Electronic Signatures. After evaluating Arizona's Electronic Transactions Act, the BTR decided that it did not need additional legislation to authorize the use of digital ID's to authenticate professional documents stored or transmitted via electronic media and the Internet. Another Board rule already allows reproduction of a registrant's professional seal within a computer-generated document or electronic file. The Electronic Transactions Act simply makes a digital ID or digital signature the legal equivalent of a registrant's hand-written signature when applied to the electronic version of a professional document.

Determined to make its electronic signature policy technology-neutral, so that registrants are not forced to purchase one particular vendor's hardware or software to comply with this law, the BTR turned to Arizona's public key infrastructure ("PKI") statute – A.R.S. § 41-132 – to establish the technical requirements of a digital ID. The PKI law authorizes the use of electronic signatures on official records and documents filed with state agencies. A digital ID certificate or software that meets the technical requirements of this statute will be recognized by the state of Arizona as a secure electronic signature.

Readers should note, however, that state and local policy as to what constitutes a digital signature and which vendor's digital ID's will be accepted for official documents is still evolving. The Arizona Secretary of State's office has, to date, recognized only digital ID's

Using Digital ID's/*to page 17*

from page 1/Using Digital ID's

issued by the Digital Signature Trust Company for secure electronic signatures. Some other state and local agencies, such as the Arizona Department of Transportation, are accepting digital ID's issued by other certificate authorities such as Verisign. Readers are encouraged to confirm current policies and procedures before submitting professional documents signed with secure electronic signatures to public agencies

Pending completion of its formal rule-making process, the BTR adopted the following Substantive Policy Statement entitled "Use of Electronic Seals and Signatures", which took effect on 17 June 2002:

> Electronic seals and signatures that meet the criteria of Arizona Revised Statutes (A.R.S.) Title 41 and Title 44 are acceptable for all professional documents. Security, verification and control of the signature are the responsibility of the registrant.
>
> This policy statement does not change or limit any existing rule or method of sealing professional documents.

The second paragraph of this policy statement was included to assure that the traditional wet seal and manual signature could still be used by those registrants who did not need or want to use digital ID's, and to assure that a traditional seal would still have full legal effect in authenticating professional documents.

To formalize this substantive policy statement, Arizona's BTR later adopted

this same standard in its new rule A.A.C. R4-30-304.G, which reads as follows:

> An electronic signature, as an option to a permanently legible signature, in accordance with A.R.S. Title 41 and Title 44, is acceptable for all professional documents. The registrant shall provide adequate security regarding the use of the seal and signature.

The combination of this new administrative rule and substantive policy statement confirms that the Board will recognize electronic media signed with a secure electronic signature (a digital ID) as properly sealed professional documents.

Obtaining and Installing Digital ID's. The technology behind digital ID's or electronic signatures is exceedingly complex because it employs the same computer algorithms used to encrypt government secrets and protect financial transactions, but that complexity is hidden from the computer user. Anyone who has access to a computer with up-to-date software and Internet access can obtain a digital ID. Several companies, such as Verisign (http://www.verisign.com) or the Digital Signature Trust Company (http://www.diqsiqtrust.com) , have developed and sell digital ID's that can be installed on an enterprise-wide basis or for individual users within a firm. Once installed on a user's computer, these digital ID's perform three essential functions: (1) they authenticate the creator of an electronic document; (2) they secure the document against alteration; and (3) they prevent the author from later repudiating the document as his or her work.

Any unauthorized change to the contents of the electronic media or remove the digital ID after it has been digitally "signed", generates a warning that the document has been altered. Anyone accessing the digital ID attached to this electronic document will see this warning, and the digital ID and any warning of alteration cannot be removed from the file.

The major software tools used by design professionals to create or transmit electronic documents, such as AutoCAD®, Bentley's MicroStation® (formerly Intergraph), Microsoft Outlook®, and Netscape Navigator® can all be configured to create secure electronic signatures using digital ID certificates or public-private key pairs (another type of digital ID). Vendors of digital ID's also serve as Certificate Authorities to authenticate their ID's on request from any computer user who receives a digitally signed document. The accessibility of these public Certificate Authorities on the Internet makes it possible for any recipient of a digitally signed document to authenticate that document even if that user did not communicate with or receive the digitally signed electronic media directly from the registrant who created it.

Furthermore, if the computer holding the registrant's digital ID were stolen or the security of that ID were compromised by an unauthorized user, the owner can also revoke the digital ID by notifying the Certificate Authority. Once a digital ID is revoked, the Certificate Authority also warns anyone receiving a document bearing that ID that the ID was no longer valid. This added layer of protection further guarantees that a digital ID could not be misused by someone who was not authorized to use it.

Design professionals who use electronic media to facilitate coordination with reviewing agencies, consultants and contractors, and anyone who uses the Internet to transmit professional documents, may now employ secure electronic signatures as the legal and functional equivalent of a wet seal and signature in Arizona. Since the federal ESIGN law has been implemented in most other states 10, this digital signature will also be legally effective outside Arizona. In time, this digital ID will prove to be even more secure and tamper-proof than the traditional wet seal and signature.