OREGON DEPARTMENT OF TRANSPORTATION

Technical Services
Traffic-Roadway Section

Geometronics Unit
200 Hawthorne Avenue S.E.
Suite B250
Salem, OR 97310
(503) 986-3103

Ron Singh, PLS
Geometronics Manager
Chief of Surveys
(503) 986-3033

Digital Signatures

For

Engineering Documents

30 September, 2008

Revision History

Authored by
Ron Singh, Geometronics Manager /Chief of Surveys

First Draft – 6 November, 2005

First Release - 7 December, 2005
Presented to Oregon DOT

Updated for the International Highway Engineering Exchange Program Conference
Albany, New York
14 September, 2007

Updated for the National Association of County Surveyors Meeting
American Congress on Surveying and Mapping Conference
Spokane, Washington
7 March, 2008

Updated for the American Council of Engineering Companies of Oregon Meeting
Beaverton, Oregon
18 March, 2008

Updated for the Professional Engineers of Oregon – Joint Engineering Conference
Bend, Oregon
23 April, 2008

Final Release
30 September, 2008

Introduction

The intent of this document is to outline issues relating to the utilization of digital signatures on engineering related documents with the Oregon Department of Transportation.

> For the purpose of this document, the term engineering will include all branches of engineering performed within the agency, including surveying, geology, and any other branch that requires the placement of a seal and signature on a final product.

Traditional hand written signatures on physical engineering documents worked well during the era of hand written/drawn documents. In the early days of utilizing computers to simply speed up the document development process with the intent of producing final documents on paper, hand written signatures also worked reasonably well. However, the use of computers has progressed into an era where electronic documents are transmitted; reviewed and approved; utilized during the bidding process; utilized for stake-less construction; and archived for future retrieval. To apply a hand written signature to these electronic files requires printing, signing the paper document, and then scanning it back into an electronic file. This process loses the electronic file's native format and any imbedded intelligence, is time consuming, and unnecessary. There is a better way: digital signatures.

This document does not intend to provide a complete solution for the use of digital signatures, but rather to serve as a starting point for discussions within the agency and its engineering partners; for development of internal policies; and possible legislative initiatives to modify and/or create new laws related to this issue.

It is expected that several related documents will follow detailing specific areas of interest such as: How digital signatures enable the development of an engineering data management system and streamline the engineering process; and the hardware, software, and procedures required to digitally sign engineering documents.

Although the focus of this document is the digital signing of engineering documents, the concepts are almost identical to digital signatures on any digital file; therefore general concepts will be described here.

Wet Signatures

A "wet" signature is usually a hand written stylized version of the signer's name on a physical document. Its purpose is not to prove identity, but rather to show deliberation, agreement, and/or informed consent to the content or intent of the document. The historical legal concept recognizes any mark made with the intention of authenticating the marked document as a signature.

For engineering documents in Oregon, Oregon Revised Statutes 672.020 and 672.025 require that the mark be a specific seal affixed to the document with the signature of the registered professional. This law does not address digital signatures on digital documents and the general understanding is that this requires physical documents with wet signatures. This specific section of the law may need to be modified to enable the utilization of digital signatures on engineering documents.

672.025 Practice of land surveying without registration prohibited; seal required. (1) No person shall practice land surveying in this state unless the person is registered and has a valid certificate to practice land surveying issued under ORS 672.002 to 672.325.

(2) Every registered professional land surveyor shall, upon registration, obtain a seal of the design authorized by the State Board of Examiners for Engineering and Land Surveying. Every final document including drawings, specifications, designs, reports, narratives, maps and plans issued by a registrant shall be stamped with the seal of and signed by the registrant. The signature and stamp of a registrant constitute a certification that the document was prepared by the registrant or under the registrant's supervision and control.

The Problems with Wet Signatures

The signature itself may not bind the signer to the document, unless the signer's identity was authenticated during the placement of a signature. In the United States this authentication may be performed by a Notary Public. Even though the signature may be notarized, the signer may later disown it by claiming the signature was forged.

The signature itself does not certify the integrity of the document. The document may be either intentionally or accidentally altered without effect on the existing seal and signature. Multiple page documents may require a wet signature on each page. Without access to the document with the original signature, a copy of the document could be easily repudiated.

Today, most seals are simply Computer Aided Drafting (CAD) cells stored in a cell library open to anyone to copy, alter, and affix to any drawing. The signatures are not notarized and could be challenged as to their authenticity.

The requirement for wet signatures significantly hinders the agency's abilities to fully integrate the development, transmittal, execution, archival, and retrieval of digital engineering documents.

The implementation of a robust digital signature process will resolve these problems and provide other benefits described throughout this document.

Electronic Vs Digital Signatures

Often the terms *electronic signature* and *digital signature* are used interchangeably to mean the same thing. In the information security world, the two terms are distinctly different. The term *electronic signature* may include scanned images of hand written signatures; typed notations such as /s/ Jane Doe; or signature blocks on email messages, etc. without any authentication and/or encryption system included. The term *digital signature* is more properly used to describe a signature system applied to an electronic document that utilizes specific technical processes to provide significant added security, authentication, and/or encryption as described below.

What is a Digital Signature?

A digital signature is to an electronic document as a handwritten signature is to a paper one and much more. A digital signature provides signer authentication, document authentication, possible document encryption, and efficiency.

Instead of using pen (wet signature) and paper, a digital signature uses digital keys to attach the identity of the signer to the document and record a binding commitment to the content of the document. Digital signatures enable "authentication" of digital documents, assuring the recipient of a digital document of both the identity of the sender and the integrity of the document. A digital signature provides “who” signed the digital file. A time stamp of that digital signature provides “when” the digital file was signed.

A robust digital signature system must be capable of creating a signature that is unique to the person using it; is capable of verification; is under the sole control of the person using it; and is linked to the document in such a way that if any part of the document is altered, the digital signature is rendered invalid.

Why use Digital Signatures?

A digital signature actually provides a greater degree of security than a handwritten signature. The recipient of a digitally signed document can verify both that the document originated from the person whose signature is attached and that the document has not been altered either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated.

A significant benefit to the agency is in the reduction of paper handling and maintaining the data in a digital format. Signing documents digitally will enable and greatly facilitate the development of an Engineering Data Management System resulting in greater project delivery efficiency.

Digital signature technology has undergone thorough research and development for over a decade. It is not an emerging technology. Digital signatures have been accepted in several national and international standards developed and accepted by many corporations, banks, and government agencies.

The likelihood of malfunction or a security problem in a digital signature system designed and implemented as prescribed in the industry standards is extremely remote. Less robust digital signature systems should be avoided.

What is needed to create a Digital Signature?

Creating a digital signature requires software, a signing certificate, and optionally a piece of hardware to provide further security with a signer’s private key. Creating the signing certificate involves creating a public-private digital key pair and optionally obtaining the services of a Certificate Authority.

The *public key* certificate creates proof of the identity of the signer and made available to anyone who needs to verify the signature. The combination of the public key and proof of identity result in a public key certificate - also called a signer's certificate.

The *private key* is something kept only by the signer. The document is signed with the private key. The public and private keys are related mathematically. Knowing the public key allows a signature to be verified but does not allow new signatures to be created. If the private key is not kept "private," then someone could maliciously create the original signer's signature on a document without consent. It is critical to keep the private key secret.

To verify a digital signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key. The solution to this is to use a trusted third party to associate an identified signer with a specific public key. That trusted third party is referred to as a "Certification Authority".

A self-signed certificate is one that is created by the individual signer without the services of a certification authority and should be avoided. Digital IDs provided by 3rd parties are generally considered more secure, because an independent certification authority has ratified them. A signature applied using a self-signed certificate signature tells a document recipient that "This document is valid, and I am authorized to sign it," while a signature applied using a 3rd party digital ID tells them that "This document valid, I am authorized to sign it, and [CERTIFICATION AUTHORITY X] verifies my identity." This additional assurance can make a big difference when it comes to legal documents or those sent out to a wide audience.

To associate a key pair with a prospective signer, a Certification Authority issues a certificate, an electronic record which lists a public key as the "subject" of the certificate, and confirms that the prospective signer identified in the certificate holds the corresponding private key. The Certification Authority performs a background check on each individual that is assigned a signing certificate.

The Oregon Department of Consumer and Business Services, Division of Finance and Corporate Securities has the responsibility to administer the registration procedure for Authentication Authorities who issue digital signatures. At this time there is only one Authentication Authority registered in Oregon:

VeriSign, Inc.
487 E Middlefield Rd.
Mountain View, CA 94043
(650) 426-3425
Web site address: http://www.verisign.com

Types of documents that may utilize Digital Signatures

- CAD Drawings (Microstation Design Files)
  - Coordinate correct engineering drawing
  - Contract Plans
  - Record of Surveys
  - Standard Drawings
  - Others
- Spreadsheets
  - Engineering Calculations
  - Material Lists
  - Others
- Word processor Documents
  - Inter-Governmental Agreements
  - Contracts
  - Engineer/Surveyor Narratives
  - Design Exceptions
  - Others
- Email
  - Correspondence
  - Others

Items Needed

Items needed to implement an agency wide digital signature system would consist of:

- Digital Signature software.
- Services of a Certification Authority to issue certificates. ODOT may be able to obtain a site license.
- Verification software and access to certificates and certificate revocation lists in a repository.
- If further security is required a USB key (hardware) may be purchased for each signer.

Signatures and the Law

The following excerpts are from "Digital Signature Guidelines" American Bar Association – Section of Science and Technology Information Security Committee:

In a digital setting, today's broad legal concept of "signature" may well include markings as diverse as digitized images of paper signatures, typed notations such as "/s/ John Smith," or even addressing notations, such as electronic mail origination headers.

The legal and business communities must develop rules and practices which use new technology to achieve and surpass the effects historically expected from paper forms.

Signing writings serve the following general purposes:

- **Evidence:** A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.
- **Ceremony:** The act of signing a document calls to the signer's attention the legal significance of the signer's act, and thereby helps prevent "inconsiderate engagements.
- **Approval:** In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it have legal effect.
- **Efficiency and logistics:** A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document. Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.

To achieve the basic purposes of signatures outlined above, a signature must have the following attributes:

- Signer authentication: A signature should indicate who signed a document, message or record, and should be difficult for another person to produce without authorization.
- Document authentication: A signature should identify what is signed, making it impracticable to falsify or alter either the signed matter or the signature without detection.

In June, 2000, President Clinton signed the electronic signature act.

Although this law pertains primarily to electronic commerce and financial transactions, it also promotes the acceptance and use of digital signatures in contracts, etc.

Oregon State Law

In 1997, the Oregon legislature passed the Digital Signature Act, ORS Chapter 192.825 to 192.855

The Act states that the intent of the legislature was:

1. To facilitate economic development and efficient delivery of government services by means of reliable electronic messages.
2. Enhance public confidence in the use of digital signatures.
3. Minimize the incidence of forged digital signatures and fraud in electronic commerce.
4. Foster the development of electronic commerce through the use of digital signatures to lend authenticity and integrity to writings in any electronic medium
5. Ensure that proper management oversight and accountability are maintained for agency conducted electronic commerce.

Although the above may pertain mainly to electronic commerce with the focus of financial transactions, the spirit of this act may support the concept of digital signatures on other documents that enable “efficient delivery of government services”.

In 2001, Oregon adopted the Uniform Electronic Transactions Act, ORS 84.001 to 84.061. Under that Act, if a law requires a signature, an electronic signature satisfies the law.

New Oregon Administrative Rules

The Oregon State Board of Examiners for Engineering and Land Surveying (OSBEELS) adopted the new Oregon Administrative Rules on July 8th, 2008 and filed it with the Oregon Secretary of State’s Archives Division making it effective on July 9th, 2008.

The new language follows:

(820-010-0010 Definitions)

(16) "Digital signature" means a type of electronic signature, as allowed by the ORS 84.001 to 84.061, that transforms a message through the use of an algorithm or series of algorithms that provide a key pair, private and public, for signer verification, document security and authentication.

(820-010-0620 Official Seal)

(5) A digital signature, as an option to a handwritten signature in permanent ink is acceptable for final documents.
(a) The digital signature must be:
(A) Unique to the registrant using it; and
(B) Capable of verification; and
(C) Under the sole control of the registrant using it; and
(D) Linked to a document in such a manner that the digital signature is invalidated if any data in the document is changed.
(b) Documents signed using a digital signature will bear the phrase “digital signature” in place of the handwritten signature.

(820-015-0010 Processing Complaints)

(5) Upon request of the Board, digitally signed documents must be provided to the Board in a form that can be processed by the Board's information processing systems.

Next Steps

- Continued public outreach and demonstration of system to various entities
- Continue work of Digital Signatures for Engineering Products Committee to investigate hardware, software, and infrastructure solutions, including studying the option of ODOT being its own Certification Authority.
- Development of cost estimate for agency-wide implementation.
- Development of procedures for agency staff and consultants.
- Internal agency training.
- Implementation.