Digital vs. "Wet" Signatures

Elizabeth Cortez
Lawrence Green
Office of the
Los Angeles County Counsel

Overview

Terms, Definitions and Mis-named Phrases

- What is a *Digital* Signature?
- What is an *Electronic* Signature?
- What is a *Digitally Recorded* or *Digitized* Signature?
- Does Digital = Electronic?
- Can't I just use a pen?

2

WHY do you Sign Something?

- When you place your signature on something, why are you doing it?
- You may be demonstrating that you are:
  - Agreeing to something;
  - Certifying the contents of something;
  - Identifying yourself;
  - All of the above.

3

The American Bar Association identifies four key elements that a signature serves:

- ***Evidence***: authenticating a writing by identifying the signer;
- ***Ceremony***: signing the document calls to attention the legal significance of the act of signing;
- ***Approval***: signing expresses the signer's approval or authorization of the writing; and
- ***Efficiency/logistics***: signing imparts a sense of clarity and finality to the transaction.

4

Why Move from Wet Signatures to Electronic Signatures

- With so many activities being conducted over the Internet and via on-line communication, the business and legal communities need someway to record a "signature" where no paper copy may exist.
- New Laws may mandate or authorize the use of electronic signatures in daily activities.
- Different methods have evolved, each trying to meet the criteria of a traditional signature, but with unique features.

5

- According to the American Bar Association outline on Online Transaction Management:

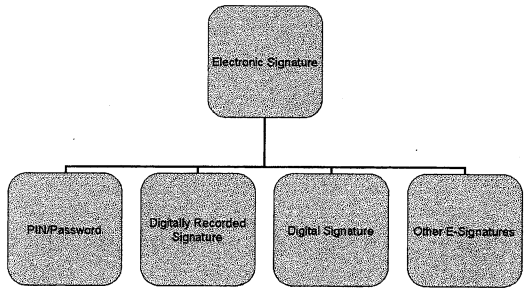
  The primary points of US Federal and State statutes enacted regarding digital signatures have been to "prevent conflicting and overly burdensome local regulation and to establish that electronic writings satisfy the traditional requirements associated with paper documents."

6

Electronic Signature

- "*Electronic* Signature" generally refers to ANY type of signature method involving a computer and the electronic act of signing:
  - Password/PIN
  - Using a faxed signature
  - Digital Signature
  - Other "electronic" signing methods (e.g., Click-Wrap, Biometrics, SmartCards, etc.)
- Each approach provides different levels of security, authentication, record integrity and protection against repudiation.

7



8

Password/PIN/Digitized Signatures

Password/PIN

- A type of electronic "signature" in which the party involved agrees to something by entering their Password or PIN number into a program.
- The act of transmitting the Password/PIN "signs" the action, indicating a volitional act to accept what is presented.

Digitized Signatures

- A digitized signature is an electronic representation of a handwritten signature. (California Vehicle Code Section 12950.5(a))
- Also, someone may sign a document, then fax or scan it, providing that as proof they've signed.

⟹ Easy to set-up or quickly rely upon, but not particularly secure.

9

Other E-Signatures

- Click-Wrap transactions are on-line agreements, one "clicks" to "sign." Examples include software licenses, or when you hit "purchase" on an on-line website.
- Biometrics include using fingerprints or iris scans.

⟹ While usable, not entirely reliable and they do not insure the reliability of the document.

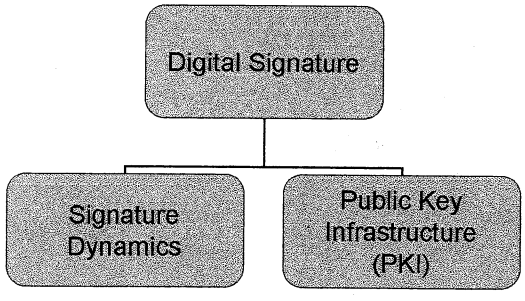
10

Digital Signature

- Digital Signatures are a very specific kind of Electronic Signature, and may be considered the most secure.
- Digital Signatures reliably "lock" a document by ensuring that if the signature is removed, or the document is modified, the change will be revealed.

11

Two Types of Digital Signature Are Recognized in California



12

Signature Dynamics
Digital Signature

- Variation on a *Digitized Signature* in which each pen stroke is measured.
- The resulting "metric" can be compared to an earlier recorded value, which authenticates that the person signing is who they appear to be.

13

PKI Digital Signature

- Uses two mathematically linked keys: one is private, held by the signer; the other is "Public," and part of a "Digital Certificate" maintained by a "Certificate Authority."
- The "Digital Certificate" is a digitally signed electronic document that binds the individual's identity to a private key in an unalterable fashion.
- A "Certificate Authority" is a trusted third-party which issues and manages key pairs and certificates. The Authority provides secure access to public keys that allow for validation and verification of signatures. Examples include Verisign, GlobalSign, and Entrust.

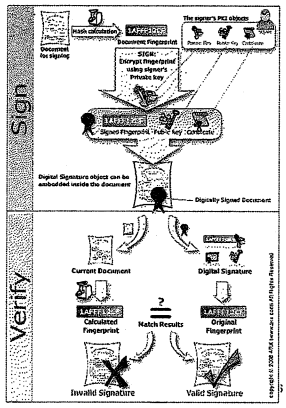
14

PKIs Continued

- A PKI is governed by a certificate policy that governs all aspects of a digital certificate's generation, management use, and storage.
- PKI is considered the most reliable because it is not possible to deduce the private key from the public key, and any alteration of the document or signature is revealed when compared.
- A PKI-based system may also be known as an "**Asymmetric Cryptosystem**" describing a system using a computer algorithm or series of algorithms that has two different keys, where: one key signs a message, the other key verifies a given message, and where even if someone has one key it is still computationally infeasible to discover the other key.
  (see California Code of Regulations Title 2, Chapter 10, Sections 22000-22005).

15

PKI in Action



Compare

- **Traditional**:

- **Digital**:

256933ECA960A6B4 F46F1546B6D5F74B C3570CD7DD981EA1
0B506B345FB159BE 6F7BAB26F6A8A143 000B4DOA944AE4D7
96C17A4587267B05 A991D76EDE989583 9E47C19054CDB818
5BD21EE36BAC9803 CD994483A1083AB5 896777AB26BE28631
1BF17D029332B6D5 2EE83CEB2FC554A8 BDE5874D82B20B9F

17

California SecState Points of Consideration

- On the decision between using PKI-based systems and Signature Dynamics-based systems, the SecState page identifies:
  - If a public entity needs immediate absolute verification of a signature, then this technology may not be the best option for [Signature Dynamics] transactions. However, the secretary of state can foresee instances where the level of security and verifiability of signature dynamics signatures could suffice for communications with public entities.
- See California SecState's web page on Digital Signature Regulations at http://www.sos.ca.gov/digsig/digital-signature-regulations.htm

18

Another Take...

- The State of New York's Office for Technology identifies some considerations in choosing an appropriate e-signature method:

  "The business analysis and risk assessment should be viewed as integrated... It is up to the governmental entity to identify its overriding concerns in the selection of an e-signature solution."

19

NYS Trust Model Factors-Identification

Identification Methods	Level of Risk
No registration, only self-identification as part of the signing process	Negligible or very low
Comparison of user supplied information with a trusted data source before authorization	Low
Acceptance of a previously conducted and trusted identification and registration process where the individuals personally presented themselves and proof of their identities	Medium
A separate identification process to authorize the use of an e-signature where the individuals personally present themselves and proof of their identities	High

20

Additional Factors-Authentication

Authentication Methods	Level of Risk
No method of authentication beyond user identification as part of the signing process	Negligible or very low
User selected PIN or password	Negligible to low
PIN or password assigned by the governmental entity	Low
PIN or password assigned by the governmental entity along with user supplied verifiable personal information	Low to medium
Cryptographic key or biometric (often includes two factor authentication through the use of a password or PIN)	Medium to high
Two factor authentication including the use of hardware device such as a smart card	High

21

When Can You Use Electronic Signatures?

- Is there authority to rely?
- Is it general?
- Is it in question? Why?
- If the matter is one with higher risk issues, is "general authority" sufficient?
- Should a specific methodology be used?
- Is there specific Legislation that you can rely upon?

22

Authority to Use E-Signatures

- The federal government and virtually every state now provide that the use of E-Signatures is valid for use with the equivalent force and value of a traditional or "wet" signature.
  - E.g., Uniform Electronic Transactions Act (UETA), Electronic Signature in Global and National Commerce Act (E-SIGN), New York's Electronic Signatures and Records Act (ESRA), State of Washington's Electronic Authentication Act (EAA).
- Use of E-Signatures is not permitted typically under specific circumstances:
  - where there either is no authorizing legislation, or
  - an exception exists.

23

- General Rule of Validity of electronic signatures in federal law:

  15 U.S.C. § 7001 *et seq.*

  (a) In general *Notwithstanding any statute, regulation, or other rule of law (other than this subchapter and subchapter II of this chapter), with respect to any transaction in or affecting interstate or foreign commerce—*

  (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

  (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

24

E-Signatures in California

- Principal authority for use E-signatures lies in two sections: Government Code 16.5 and Civil Code 1633.11
  - The Government Code provides that a digital signature will have the same force and effect as a manual signature provided it meets specific attributes.
  - The Civil Code provides that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
  - Key: there must be a prior agreement to use electronic signatures.
- Coordinate sections have been enacted in California Code of Regulations Sections 22010 *et seq.*

25

Consider Also...

- Government Code Section 12168.5(a) authorizes the Secretary of State to adopt rules/regulations to authorize electronically filed and signed documents.

  "...A signature on a document electronically filed or filed by facsimile in accordance with those rules and regulations [regarding electronic filing] is prima facie evidence for all purposes that the document actually was signed by the person whose signature appears on the electronically filed document or facsimile."

26

Attributes for Use of Digital Signatures Under Gov. Code Section 16.5

- It is unique to the person using it.
- It is capable of verification.
- It is under the sole control of the person using it.
- It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.
- It conforms to regulations adopted by the Secretary of State.

27

Exceptions to the Rule of General Authority?

- Government Code Section 12168.5(c), for example, exempts filings and recordings under the Political Reform Act of 1974, thereby identifying a carve-out to the general authority to use electronic signatures.
- In such an instance, reliance on electronic signatures does not appear to be authorized.

➢ IMPORTANT TO REMEMBER: Laws and regulations authorizing the use of electronic signatures always provide that use is permitted *unless* otherwise excepted. And, generally, there must be an agreement to use; it cannot be forced on someone.

28

Where Once Not Allowed...

- Prior to specific authorization, there was no provision to use electronic signatures for many Department of Motor Vehicle business transactions.
- Assembly Bill 461 (Horton) in 2005 sought authority for the DMV to accept electronically signed documents.
- Vehicle Code was specifically amended in Section 1801.1 to permit the use of electronic signatures.

29

Electronically Submitted Documents

1801.1.

(a) Notwithstanding any other provision of law, the department may allow a person to submit ***any*** document required to be submitted to the department by using electronic media deemed feasible by the department ***instead of requiring the actual submittal of the original document***.

(b) If a signature on a document is required by law in order to complete a transaction, and the document is submitted electronically, that ***signature requirement may be met by an electronically submitted signature***, if the department retains information verifying the identity of the person submitting the electronic signature.

(c) The department may establish minimum transaction volume levels, audit and security standards, and technological requirements, or terms and conditions, including methods of authentication for electronically submitted signatures, it deems necessary for the approval of this process.

(d) ***An electronically submitted document, once accepted by the department, shall be deemed the same as an original document, and shall be admissible in all administrative, quasi-judicial, and judicial proceedings.***

30

Board of Equalization Goes E-Signature Friendly

- Prior to enactment of Assembly Bill 1042 (Spitzer) in 2007, it was not entirely clear to the Orange County Assessment Appeals Board that electronic signatures were permitted, even in light of Government Code Section 16.5.
- Revenue and Taxation Code Section 1603(g) now specifically authorizes the use electronic signatures where the signature is accompanied by the required certification, and the manner of signature is approved by the Board.

➢ NB: this provision was sponsored by the Orange County Board of Supervisors after confusion arose from the requirement in R&T Code Section 1603(a) that a filing with the assessment appeals board must be a "verified, written application..."

31

Additional Examples

- Public Resources Code Sections 71060-71068, added in 1994, regarding environmental data reporting:
  - The Secretary for Environmental Protection is authorized to establish the use of electronic communication to report and receive filings.
  - The use of electronic signatures is specifically authorized in Section 71066.
- Government Code Section 14608, added in 1994, regarding the Department of General Services:
  - Whenever any statute requires by the use of the word or words "approve," "approval," "authorize," or "authorization," the director of the department to approve or authorize any act or transaction, the approval or authorization shall be deemed to have been given only if given in writing... The term "in writing" includes a secured **electronic signature**, whereby an electronically produced document may be signed electronically by the authorized signatory who possesses a secured **electronic** password available **only** to the signatory or his or her designee

32

Important Elements to Remember

- Once Electronic Signatures are authorized, if used they have the SAME force and effect of a pen-based signature.
- Different methodologies offer different strengths and weaknesses; the "best" method depends on the use in question.
- Generally, in California, the use of Electronic Signatures is allowed unless an exception exists.

33

Going Back to the Pen...

- Consider the legislative analysis in the bill to authorize the Secretary of Environmental Protection to use electronic reporting: "The blizzard of incoming paper reports often exceeds the capacity of a public agency to digest the information."
- In its Digital Signature Guidelines Tutorial, the ABA report notes that as to document authentication, "A paper signature identifies the signed matter less than perfectly. Ordinarily, the signature appears below what is signed, and the physical dimensions of the paper and the regular layout of the text are relied upon to indicate alteration. However, those mechanisms are not enough to prevent difficult factual questions from arising."
- ➢ In an environment where a digital signature is used, these liabilities may be controlled and reduced.

34

Further Information

- California Secretary of State Electronic Signature Information:
  http://www.sos.ca.gov/digsig/digital-signature-faq.htm
- PKI and Electronic Signature Basics:
  http://electronicdigitalsignature.com
- American Bar Association
  - Digital Signature Guidelines Tutorial
    http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html
- New York State Office for Technology
  - Electronic Signatures and Records Act (ESRA) Guidelines:
    http://www.oft.state.ny.us/Policy/G04-001/index.htm#table_of_contents
- South Carolina Department of Archives and History
  - Electronic Records Management Guidelines: electronic and digital signatures
    http://www.state.sc.us/scdah/erg/ermEDS.pdf
- Digital Ink Signatures
  - Concepts and Technology:
    http://msdn.microsoft.com/en-us/library/ms812501.aspx#tbconinksig_topic1

35