In the CA I Trust
A Look at Certification Authorities

James E. Shearer
for CSEP 590, Practical Aspects of Modern Cryptography
March 7 2006

1 Introduction

The American Bar Association has long advocated the need for a legally valid means of electronic signature while recognizing that the technology and legal ramifications are in their infancy. In 1997 the ABA stated "Laws and policies for digital signatures should balance the need for consistency across state and national boundaries, the need to allow for experimentation and innovation, and need to respect traditional state jurisdictions, e.g., commerce, contracts, and state rules of evidence."[1]

The philosophy of deferring to the states for the details was codified when the United States Congress passed the Electronic Signatures In Global And National Commerce Act (E-Sign) in June of 2000[2]. This act states that contracts involving interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because it and/or the signatures on it are in electronic form. However, it is noteworthy that this act specifically does not restrict how electronic signatures are applied or validated, leaving this detail to the individual states (a-priori) and the courts (post-priori).

2 Signatures and Law

The American Bar Association Information Security Subcommittee (ABA-ISC) offers the following (slightly paraphrased) tutorial on the meaning of "signature".[3]:

> A signature is not part of the substance of a transaction, but rather of its representation or form (it's "writing"). Signing writings serve the following general purposes:
>
> - **Evidence**: A signature authenticates a writing by identifying the signer with the signed document.
> - **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 intention that the writing have legal effect.
> - **Efficiency and logistics**: A signature on a writing often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a writing if, for example, it is examined at a later date by a third party.
>
> 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 writing, 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.

The effect of E-Sign and the definitions above is that the individual states have a mandate to provide a legal framework for facilitating electronic signatures that satisfy the ABA attributes. Various states have taken one of two paths, "electronic signature" laws and "secure signature laws."

Electronic signature laws (such as those in Florida, Virginia, and Texas) merely recognize the common law of signatures to clarify how current law should apply to electronic authentication. These laws would explicitly recognize the commonly held view that many different technologies are capable of creating valid signatures, including digital images of signatures, PIN numbers, and biometric devices.

Secure signature laws typically give special statutory benefits (such as evidentiary presumptions and liability limits or other special recognition) for electronic signatures that have an established degree of reliability. For example, Utah, Washington and Minnesota recognize digital signature technology as being sufficiently reliable to warrant special statutory treatment. The state of California, rather than recognizing digital signature technology in the statute itself, provides certain security criteria that must be met and provides for the promulgation of regulations to specify what technologies shall qualify. The current draft proposed California regulations specifically recognize digital signatures as a approved technology.

Texas' law[4], for example, states in section 43.001;

> "If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record."

In contrast, Washington's law[5] states in RCW 19.34.300:

> "Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature, if:
>
> (a) The digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;
>
> (b) The digital signature was affixed by the signer with the intention of signing the message; and
>
> (c) The recipient has no knowledge or notice that the signer either breached a duty as a subscriber; or does not rightfully hold the private key used to affix the digital signature."

Note that Washington's law is technology-specific. It is also much longer than Texas' (6 page) law and includes several sections on the licensing and obligations of the CA mentioned in bullet (a).

California's law[6] splits the difference. It defines the attributes of a legal digital signature like Texas and then lists acceptable technologies like Washington. However, California lists two acceptable technologies; Public Key Cryptography and Signature Dynamics. and it also includes provisions for adding new technologies to the list of acceptable technologies when they become available.

3 CA Certification

States that have secure signature laws generally have a requirement that the Certification Authorities themselves must be certified to operate within the state. This certification process is either conducted by the state itself, as in Washington, or by a non-government Registration Authority designated by the state, as in Kansas[7]. In all cases, the State's interest is to provide a voluntary licensing mechanism for digital signature certification authorities by which businesses, consumers, courts, government agencies, and other entities can reasonably be assured as to the integrity, authenticity, and non-repudiation of a digitally signed electronic communication. This means that the CAs need to prove their own identity and show that they use computing resources and documented processes (a "Certification Practice Statement") that (1) verify the authenticity of subscribers to an acceptable level of confidence and (2) protect the CA's keys adequately to establish non-repudiation. Further, Washington State requires as part of its licensing that CAs maintain an office or have established a registered agent for service of process in Washington. This allows the state to claim jurisdiction and seek damages if the CA violates the terms of the license.

The result is that, while there are well over a hundred CAs world-wide (See reference [9] for a list of 125 of them), Washington State licenses only 2 CAs (Digital Signature Trust Co., and VeriSign Inc.) and California has approved 4 CAs (Digital Signature Trust Co., VeriSign Inc., Entrust Inc., and GeoTrust Inc.).

4 Certificates

Certificates come in four flavors, distinguished by the level of confidence represented by the certificate. These are:

High Assurance Certificates, which require the applicant to appear in person for positive identification and to prove possession and use of adequate private key hardware token and processes.

Medium Assurance Certificates, which require the applicant to appear in person for positive identification (as per the Kansas law) or to provide an identification chain back to an approved registration authority (as per VeriSign's CPS) and to prove possession and use of adequate private key protection processes, which may be in software.

Basic Assurance Certificates, which can be applied for on-line. Positive identification is established by look-up in a database or by being vouched for by someone who already is recognized by the system. For example, VeriSign just verifies that the subscriber can answer E-mail at the subscriber-provided e-mail address, which is functionally equivalent to the ISP vouching for the subscriber.

Rudimentary Assurance Certificates, which do not require proof of identity and are intended only for ensuring data integrity. For example, the United States Postal Service offers an Electronic Postmark service (USPS-EPM)[8] that provides integrity signing and storage of Microsoft Word documents.

The first three require a way to represent the subscriber's identity in the certificate. This usually means the subscriber must have a X.500 distinguished name, and many CAs require that this name be associated with a web address.

5 Liability

People are accustomed to using credit cards and are often at least slightly familiar with its liability model. In the credit card model, the "subscriber" (card holder) is only liable for $50.00 if the card is stolen. The credit company assumes the rest of the liability. However, Certification Authorities do not follow this model. Liability is shared between the Certification Authority, the Subscriber, and the Relying Party, but the shares are not at all equal as we shall see.

5.1 CA's Liability

Certification Authorities are considered to be in the same category as Public Notaries and as such, enjoy limited liability for misuse of the certificates they issue (But only if they are licensed or approved within the State carrying jurisdiction!). This puts the burden of liability on the subscriber and the relying party. In fact, Washington State lets the CA determine its own liability limit!

> "By clearly specifying a recommended reliance limit in a certificate and in the certification practice statement, the issuing certification authority recommends that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit."
>
> - Washington State RCW 19.34.280

VeriSign has set its own liability at $100.00 for a class 1 (basic assurance) certificate, $5,000.00 for a class 2 (medium assurance) certificate, and $100,000.00 for a class 3 (high assurance) certificate[10]. But they will gladly sell you their NetSure Protection Plan extended warranty.[11]

Digital Signature Trust seems to have set its own liability even lower. It's CPS[12] states:

> "Except as otherwise specified herein, DST disclaims any and all representations and warranties of any type with respect to any certificate on which you may rely, whether express or implied, including but not limited to any implied warranty of merchantability, fitness for a particular purpose, title, and non-infringement."

But there is no "otherwise specified herein" that this author can find, suggesting that they are disclaiming all liability.

By Washington law, even the small amount of liability that VeriSign signed up for applies only to a loss caused by reliance on a misrepresentation in the certificate of a fact that the licensed certification authority is required to confirm, or failure to comply with the licensing provisions in issuing the certificate. Washington State exempts the CA entirely from:

- A loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with the requirements of its license.

- Punitive or exemplary damages.
- Damages for pain or suffering.

There is also a small piece of weasel wording in RCW 19.34.280 that this author is not quite sure what to make of:

> "Consequential or incidental damages may be liquidated, or may otherwise be limited, altered, or excluded unless the limitation, alteration, or exclusion is unconscionable. A licensed certification authority may liquidate, limit, alter, or exclude consequential or incidental damages as provided in this subsection by agreement or by notifying any person who will rely on a certificate of the liquidation, limitation, alteration, or exclusion before the person relies on the certificate."

5.2 Subscriber's Liability

Liability has been shifted to the subscriber for the bulk of cases involving loss or failure of the certification or its underlying keys. If the subscriber is the level of user that requires high or medium level certificates, the subscriber can be expected to obtain the necessary technical expertise to understand the issues. This in turn makes the risk look a lot like any other transactional risk under standard contract law. Subscribers for Basic Assurance certificates may not be as technically savvy and as such may be open to more liability than they realize. A relatively brief search did not expose any litigation regarding failure of a Basic Assurance certificate so it's not clear what the scope of the problem (if any) is.

5.3 Relying Party's Liability

This is an interesting problem. When a relying party goes to a web site that has a certificate, Internet Explorer handles validating the certificate under the covers. But going to that web page and invoking a transaction inherently incurs a liability. VeriSign states it this way in their CPS:

> Before any act of reliance, Relying Parties shall independently assess:
>
> 1. The appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. VeriSign is not responsible for assessing the appropriateness of the use of a Certificate.
> 2. That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled, then the certificate may not be relied upon for validating a Subscriber's signature).
> 3. The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

The relying party is totally at the mercy of the automated certificate validation system for points 1 and 2, and gets a pop-up if the system detects an expired or revoked certificate in the chain as described in point 3. This is very much a buyer-beware system.

6 A Case History

One can hardly discuss the legal infrastructure of Certification Authorities without dredging up the now-infamous case of the fraudulent Microsoft certificates issued by VeriSign in 2001. The initial advisory from VeriSign begins as follows[13]:

> VeriSign, Inc, discovered through its routine fraud screening procedures that on 29 and 30 January 2001, it issued two digital certificates to an individual who fraudulently claimed to be a representative of Microsoft Corporation. VeriSign immediately revoked the certificates. The updated certificate revocation list (CRL) is available at http://crl.verisign.com/Class3SoftwarePublishers.crl or through VeriSign real-time Online Certificate Status Protocol (OCSP) Services.
>
> The certificates were VeriSign Class 3 Software Publisher certificates and could be used to sign executable content under the name "Microsoft Corporation". The risk associated with these certificates is that the fraudulent party could produce digitally signed code and appear to be Microsoft Corporation. In this scenario, it is possible that the fraudulent party could create a destructive program or ActiveX control, then sign it using either certificate and host it on a Web site or distribute it to other Web sites.
>
> What you should do:
>
> VeriSign is working closely with Microsoft, which has developed an update that will protect customer desktops in the following ways: a) by downloading a VeriSign certificate revocation list (CRL) and enabling CRL checking for software publisher certificates, and b) by scanning the user's system for any sign that the user has previously accepted content signed using either certificate. The update will be available shortly, at which time Microsoft will provide specific details. VeriSign is encouraging all users to download this security update when it becomes available. For more information, see the Microsoft bulletin at: http://www.microsoft.com/technet/security/bulletin/MS01-017.mspx.

This problem was exacerbated by a conflict in the way VeriSign and Microsoft handled revocation lists at the time. Microsoft's defense was built around certificates conforming to section 4.2.1.14 of the RFC 2459 standard[14], which recommends, but does not require that certificates include an extension that points back to a CRL distribution point. Unfortunately, VeriSign at that time did not support that section of the standard.

The technical problem of revocation was resolved by both Microsoft and VeriSign. Microsoft issued a Windows patch that included its own revocation list, and VeriSign changed their policy to include the CRL Distribution Points extension on "most" of their high and medium assurance certificates (see section 7.1.2.6 of VeriSign's CPS).

Apparently the certificates were not used in a malicious way before the fixes were distributed, so we didn't get the pleasure of watching a liability court case unfold between Microsoft and VeriSign. Some of the questions that might have appeared in such a trial are:

- Did VeriSign violate their license when they miss-identified the fraudster as Microsoft (in which case Microsoft should be entitled to that $100,000.00 class 3 liability), or was the fraudster's strategy "unforeseeable"?
- Did Microsoft know (or should they have known) that VeriSign did not include the CRL extension in their certificates before this event occurred? If so, did their failure to proactively protect themselves (as in the later patch) violate their agreement with VeriSign as per their acceptance of VeriSign's CPS?

- Would any Relying Parties who got burnt by fake Microsoft downloads between the time VeriSign updated their CRL and Microsoft issued their patch be in violation of VeriSign's CPS clause that "the Relying party is solely responsible" for validating certificates? If so, would this exonerate BOTH VeriSign and Microsoft?

It looks like we'll have to wait for the next major PKI catastrophe to get legal rulings on these issues.

7 References

[1] (1997) ABA-ISC Statement: States' Role in Developing Digital Signatures Policies and Standards, http://www.abanet.org/scitech/ec/isc/stateds.html

[2] (2000), Electronic Signatures In Global And National Commerce Act (E-Sign), United States Federal Public Law 106-229.

[3] (Undated), ABA-ISC Digital Signature Guidelines Tutorial, http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html

[4] (2002) Texas Business and Commercial Code, Chapter 43; Uniform Electronic Transaction Act, http://www.capitol.state.tx.us/statutes/docs/BC/content/pdf/bc.004.00.000043.00.pdf

[5] (1996) RCW 19.34, Washington Electronic Authentication Act, http://apps.leg.wa.gov/RCW/default.aspx?cite=19.34

[6] (1998) California Digital Signature Regulations, http://www.ss.ca.gov/digsig/regulations.htm

[7] (2001), Kansas Information Technology Executive Council Policy #5200, http://www.da.ks.gov/itec/documents/ITECITPolicy5200_A1.pdf

[8] (2001) United States Postal Service Electronic Postmark Service (USPS EPM), https://www.uspsepm.com/info/main.adate

[9] Kelm, Stefan (2005), The PKI Page, http://www.pki-page.org

[10] (2005) VeriSign Certification Practice Statement, Version 3.1, http://www.verisign.com/repository/CPS/VeriSignCPSv3.1.pdf

[11] (2001) VeriSign NetSure Protection Plan, Version 5.0, http://www.verisign.com/repository/netsure/netsure2.html

[12] (2000) Digital Signature Trust Certification Practice Statement, Version 2.0, http://www.digsigtrust.com/certificates/policy/ts/dst-cps-v20000926.html

[13] (2001) Advisory from VeriSign, http://www.verisign.com/support/advisories/authenticodefraud.html

[14] (1999) IETF Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://www.ietf.org/rfc/rfc2459.txt