RISK AND TRUST MANAGEMENT TECHNIQUES FOR AN "OPEN BUT BOUNDED" PUBLIC KEY INFRASTRUCTURE

Daniel J. Greenwood*

CITATION: Daniel J. Greenwood, Risk and Trust Management Techniques for an "Open But Bounded" Public Key Infrastructure, 38 Jurimetrics J. 277-294 (1998).

I. INTRODUCTION

Establishing trustworthiness requires an analysis of the business, technical and legal requirements for each party to a Public Key Infrastructure (PKI) based transaction.[1] Much of the current discussion about PKI requirements revolves around the license, accreditation, or other sets of ratings as applied to certification authorities (CA). It is becoming apparent that an exclusive focus on CA quality control is too narrow to provide adequate measures for risk and trust. Trust management derives from a more complete evaluation of each party's relationship

* Daniel Greenwood is the Deputy General Counsel for the Information Technology Division of the Commonwealth of Massachusetts and holds an academic appointment as Lecturer at Massachusetts Institute of Technology, where he teaches at the graduate level on topics of electronic commerce and online government. Mr. Greenwood has testified before the U.S. Congress and state legislatures on electronic authentication legislation. He co-chairs the Certificate Authority Ratings and Trust Task Force of the National Automated Clearinghouse Association's Internet Council, as well as co-chairing work groups of the American Bar Association's Information Security Committee and the Committee on the Law of Commerce in Cyberspace. The author thanks Pam Price, a second-year law student at Suffolk University Law School, for her helpful assistance with this article.

The grant of permission that appears at page ii to make copies of articles in this issue for educational use does not apply to this article.

[1] This discussion assumes a rudimentary knowledge of public key cryptography and the applications that support it. For a quick primer of this topic, consult *Basics of Public Key Cryptography and Digital Signatures* (Dec. 19, 1996) <http://www.magnet.state.ma.us/itd/legal/ crypto-3.htm>. For a more in-depth explanation, see *RSA Laboratories' FAQ 3.0 on Cryptography* (visited May 15, 1998) <http://www.rsa.com/rsalabs/newfaq/>.

to the transaction and to the other parties. Ultimately, this must include not only the directly transacting parties, but also the technology providers, the connectivity providers, and the authentication providers. However, this paper is limited to an exploration of the agreement that would be entered into only by parties that are directly involved in the issuance, usage, or reliance upon a digital certificate.

For purposes of this paper, these issues are discussed in the context of the Internet Engineering Task Force PKIX Part IV Certificate Policy Framework[2] (PKIX Framework). The PKIX Framework permits an "apples to apples" comparison between PKI-based systems. Among the PKI certificate policy initiatives currently underway are: the Government of Canada PKI,[3] the American Bar Association's developing Certificate Policy and Accreditation Guidelines,[4] the United States Federal PKI Task Force Model Certificate Policy,[5] and the Department of Defense Certificate Policy Draft, the General Services Administration Draft Certificate Policy for the ACES System, the Commonwealth of Massachusetts Draft Certificate Policy for Server Certificates, and the certificate policies being developed by the National Automated Clearinghouse Association.[6] This paper explores the concept of "open but bounded" (OBB) PKI as a possible basis for conducting public and private sector transaction via multi-use, trustworthy certificates.

II. BACKGROUND: OPEN AND CLOSED PUBLIC KEY INFRASTRUCTURES

The term certificate policy (CP) comes from the X.509 specification,[7] which uses the following definition:

> A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular [CP] might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.[8]

[2] Santosh Chokhani & Warwick Ford, *Internet Public Key Infrastructure Part IV: Certificate Policy and Certification Practices Framework*, PKIX Working Group (Sept. 30, 1997) <http://www.pca.dfn.de/eng/team/ske/drafts/draft-ietf-pkix-ipki-part4-02.txt>.

[3] CERTIFICATE POLICIES FOR THE GOVERNMENT OF CANADA PUBLIC KEY INFRASTRUCTURE (draft 1997) *Home Page for Daniel Greenwood* (visited May 15, 1998) <http://www.tiac.net/biz/danielg/goc_int.htm> [hereinafter CANADA CERTIFICATE POLICIES]. The authors have requested that it be noted that these are still "working documents and are not the policies of the Canadian Government."

[4] INFORMATION SECURITY COMMITTEE, SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOCIATION, ABA GUIDELINES FOR CERTIFICATE POLICIES AND ACCREDITATION (Jan. 1998).

[5] UNITED STATES FEDERAL PKI TASK FORCE, MODEL CERTIFICATE POLICY, (Preliminary Discussion Draft, Nov. 25, 1997) [hereinafter MODEL CERTIFICATE POLICY].

[6] National Automated Clearinghouse Association Internet Council is conducting a Certificate Authority Interoperability Pilot under the Authentication and Network of Trust Work Group and is also exploring certificate policy usage under the Certificate Authority Ratings and Trust Task Force. For work group and task force public information, see *The Internet Council* (last modified Mar. 29, 1998) <http://www.nacha.org/tic/workgrps.htm>. The other referenced certificate policies can be accessed through *Home Page for Daniel Greenwood* (visited May 15, 1998) <http://www.tiac.net/ biz/ danielg?#Certificate Policy>.

[7] International Telecommunications Union, X.509 Version 3.

[8] *Id.* at § 3.3.

One of the major unanswered questions about the use of public key cryptography for digital signatures, and a major point of contention between advocates of different types of electronic signature laws, relates to the business model for CA services that will ultimately prevail in the marketplace. A larger infrastructure will need to evolve to support use of this technology. While advances in technology will certainly create new possibilities not presently contemplated, the two primary business models currently vying for support are known as the "open PKI" and "closed PKI" models.

An open PKI model assumes that subscribers will obtain a digital certificate from a CA that will link their identity to their public key for all, or at least many, purposes. Thus, in an open PKI environment a person could obtain a digital certificate and then use it to order goods online from various merchants, sign legally binding agreements, or even file documents with a government entity. Subscribers could use their certificate for any transaction requiring a digital signature. This model assumes that many parties may rely upon a certificate and may not yet be known at the time of certificate issuance.[9]

In the closed PKI model, users would obtain a different digital certificate for each community of interests with which they interact online. For example, a user could have one certificate for transactions with their bank, a different certificate for communications with their employer, and yet another certificate for dealings with their health care provider. This model assumes that the party who relies upon a given certificate is also responsible for authorizing the issuance of that certificate. That is, the CA is also the relying party.

There are, of course, several ways to implement a closed system. The relying party could outsource the certificate issuance process but keep control of the process whereby the initial identification and authentication is accomplished. Alternatively, the relying party could also purchase or build a certificate server and issue the certificates as well. In either case, the party responsible for causing a certificate to be issued is also the party who will rely upon the certificate.[10]

The difference between the two models is significant. Under an open PKI model, it would be relatively easy for a person's certificate to be used to sign any document, which makes the consequences extremely severe if the user's private key is compromised. In a closed PKI, on the other hand, the risks to the user and the CA or relying party of an improperly signed document are more limited due to the system's more narrowly defined scope. Furthermore, the members of a particular community within a closed PKI system may enter into agreements that define the

[9] Professor Jane Winn of Southern Methodist University School of Law has called open PKI "stranger to stranger" electronic commerce. Jane Winn, *Open Systems, Free Markets and Regulation of Internet Commerce*, 72 TULANE L. REV. (Spring 1998). That is, the parties to a transaction may have no prior relationship other than the current transaction. In such a case, the data contained in or derived from a certificate is the foundation of "trust" upon which the transaction is based. *Id*.

[10] Examples of this would include an employer who issues certificates to employees for personnel purposes or a business that causes certificates to be issued to customers for purposes of conducting transactions with that business. The system is closed, in this respect, because the pool of intended relying parties is limited to a party of one. Such closed systems typically build in considerable safeguards that prevent the internal certificates from "leaking" beyond the direct control of the relying party. This is because, in part, the relying party seeks to limit the possibility of unintended third-party reliance on the certificate and potential liability that would follow for misidentification or other system failure or fraud.

rights and responsibilities of the members, which would further reduce the risks and uncertainty in such a system. It is possible that limiting the parties is the most effective risk reduction technique. However, the importance of limiting potential uses is also vital. The possible liability arising from a certificate capable of being used as the basis of a mortgage is significantly different from that of a certificate used only to access free newspapers for marketing purposes.

In reality, open and closed systems have many things in common as they are implemented in the market. In fact, it is becoming increasingly difficult to determine the difference. Open systems in which a certificate practice statement and various use or reliance limits are set within the certificate appear, on the surface, to be bounded. For purposes of this paper, such attempted restrictions are not deemed to "close" or meaningfully bound the possible uses, parties, or processes within a PKI. This is because of the weakness with which the attempted restrictions are implemented. There is no guarantee that a party will note or understand a given limit listed within a certificate. Several software programs exist that accept certificates without any rigorous check of the contents of the certificate or any requirement (or possibility) of verification by means of a certificate revocation list or an online certificate checking protocol. Therefore, open systems that attempt to employ limits on potential uses, parties, or processes for a given certificate are quite different from closed systems within which such limits are made reliable and enforceable. The concept of "cross-certification" is seen as a method of recognition between CAs in otherwise closed or non-interoperable systems.[11]

III. OPEN BUT BOUNDED PKI

OBB PKI entails the creation of reliable and trustworthy mechanisms that parties to transactions may opt into. These mechanisms of boundedness augment the certainty and trustworthiness of an open PKI approach. The openness within this system also provides a business and legal basis within which technical cross-certification can occur. Within the OBB system, various certificate uses may be openly conducted by several parties. Thus, disparate uses and communities may conduct transaction within the system and may leverage each other's certificates.

OBB PKI creates a framework facilitating risk management and fostering trust relationships. The diagram below illustrates some of the features and characteristics of the model. Parties to a PKI-facilitated transaction include, at a minimum, a CA, relying party, and subscriber. There are business incentives among multiple

[11] See, for example, the Entrust-led initiative with American Biometric Company, Bell Global Solutions, Chrysalis-ITS, Entegrity Solutions, General Network Services Inc., GTE CyberTrust Solutions Inc., Harbinger Corporation, Hewlett-Packard, KyberPASS Corporation, Tandem Computers, TradeWave Corporation, and Worldtalk to promote the benefits of cross-certification. *See Entrust Technologies Takes Leadership Position in Advancing Interoperability Among Public-Key Infrastructures* (visited May 15, 1998) <http://www.kyberpass.com/Press/Pressent1. html>.

subscribers, reliers, and CAs to conduct transactions with each other that require authentication and confidentiality. OBB systems, based on the PKIX Framework, can provide the foundation of trust for business and government transactions to take place over the Internet between many parties using methods that leverage the other parties' systems, create economies of scale, and lead to widely interoperable and acceptable electronic authentication in the private marketplace.

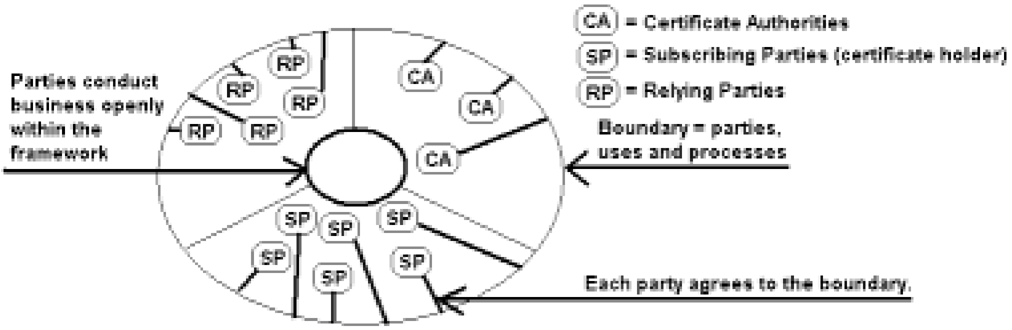
How does a given subscriber know which CA to trust or what the potential pool of relying parties could be for her certificate? How does a relying party know whether to trust a certificate unless they have caused it to be issued? How can a CA know what CP to reference within a certificate and certificate practice statement? These issues can be defined and resolved among the parties in an OBB system. The certificate policy would provide the mechanism that reflects the agreements reached by parties to the OBB system. Unlike a tightly closed system, a given certificate could be relied upon by multiple parties and for multiple purposes. Unlike a very open system, there would be meaningful limits placed upon the uses and overall pool of possible parties who could rely on the certificate.

The outer circle below represents the agreement among all the parties which defines these and other issues. This agreement, or set of operating rules, can be achieved or augmented by a CP and would be negotiated by the parties themselves or some subset of the parties rather than set by statute or regulation.

Unlike open PKI, OBB PKI would rest on an advance agreement by known parties. The agreement defines bounds on acceptable parties (who can issue, be issued, rely on, and store a certificate), uses (what transactions or other uses of the certificate are intended, permitted, and prohibited), and processes (what technical and business practice requirements and guidelines exist). Based on these boundaries, a number of serious business interactions in both the public and private sector may become more reasonably accomplished over the Internet.

Unlike some closed PKI, a number of different uses and parties, including various relying parties, are possible under an OBB PKI. To assure sufficient openness within the system, the parties determine the number and variety of applications that are permitted. To assure scalability, the system provides mechanism for growing numbers of parties to opt into the boundary. The PKIX Framework outlines the definition of this model. The boundary, and the open transactions and uses within the boundary, become elements of the CP. Use of such bounds can create a reliable PKI and may serve as an alternative to legislation or regulation.

Open But Bounded Public Key Infrastructure for Public and Private Uses


CA = Certificate Authorities
SP = Subscribing Parties (certificate holder)
RP = Relying Parties
Parties conduct business openly within the framework
RP
RP
RP
RP
RP
RP
CA
CA
CA
Boundary = parties, uses and processes
SP
SP
SP
SP
SP
SP
Each party agrees to the boundary.

of endless reliance by unknown third parties creates dangerous risk potential for both a certificate authority and a subscriber. The lack of a direct relationship between a relying party and a CA exacerbates this uncertainty. This is because the CA could be exposing itself to liability from countless unknown relying parties. Furthermore, existing systems allow parties to rely on certificates without checking with the issuing CA to determine whether the certificate was validly issued or whether it has been revoked or suspended.[12] The Utah Digital Signature Act attempted to address this uncertainty by creating liability limits for CAs that are licensed under the law and by creating an evidentiary rebuttable presumption that the subscriber in fact is responsible for messages signed with her digital signature.[13] The lack of contractual privity between the CA and the relying party further complicates quantification and evaluation of transaction risk and liability.

In their article, *Economic Modelling and Risk Management in Public Key Infrastructures*, authors David G. Masse and Andrew D. Fernandes assert that the creation of contractual relationships between the relying party and the certificate authority could form the basis of a trustworthy PKI.[14] The authors suggest that the contracts could be formed online in the following way:

> Forcing the third party to *pull* the public key certificate from the certification authority creates an opportunity to allow the third party and the certification [authority] to form a relationship. That relationship can be readily framed in a contractual setting. The pull request coming from the third party to the certification authority constitutes a legally valid offer on the part of the third party which the certification authority can then accept. The exchange of the digital offer and the digital acceptance then forms a legally binding contract between the parties into which the certification authority's certification practice statement is incorporated by reference . . . .[15]

In his article, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*,[16] Brad Biddle is highly critical of legislation that specifies open PKI.[17] In particular, Biddle focuses on the issue of whether legislation is needed to handle the question of risk allocation. Biddle states:

> Most online businesses are forced to rely on Webwrap agreements. Several recent court decisions have strongly suggested that they will be enforceable; a legislation-drafting effort underway [the Uniform Electronic Transactions Act] is close to settling the question. Webwrap agreements present a mechanism by which CAs can attempt to allocate risk contractually.[18]

[12] See, for example, the S/MIME protocol for secure electronic messaging at *S/MIME Central* (visited May 15, 1998) <http://www.rsa.com/smime>. Given the way in which this protocol is implemented within the e-mail clients of Netscape and Microsoft browsers, reasonable reliance on an invalid or revoked certificate is not unforeseeable because the verification mechanisms are not yet widely available or commonly understood by the public.

[13] UTAH CODE ANN. § 46-3- 309 (1996).

[14] *See* David G. Masse & Andrew D. Fernandes, *Economic Modelling and Risk Management in Public Key Infrastructures*, at 178 (last modified Apr. 15, 1997) <http://www.chait-amyot.ca/docs/pki.html>.

[15] *Id*.

[16] C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace* (last modified May 27, 1997) < http://www.acusd.edu/~biddle/ LMW.htm>.

[17] *Id*.

[18] *Id*.

Contracts can serve the purpose of creating a predictable legal infrastructure for PKI. This paper assumes that a system based on parties determining their rights, responsibilities, and allocation of risk among themselves is more efficient than legislative or regulatory pronouncements to create a workable electronic business system. If it is the lack of contractual privity between the parties that causes some people to seek legislation, then industry and government should focus on encouraging systems that allow for the creation of contractual privity rather than attempting to predetermine the business and legal details between transacting parties through public law. Unlike the Uniform Commercial Code, which was built upon decades of experience in the market, detailed and proscriptive digital signature laws attempt to pre-define relationships between parties that have not yet even arisen. It is highly unlikely that governments will guess correctly about the optimal shape of business relationships—especially in such a fast-moving and dynamic area as this. Existing commercial law, consumer law, and other areas of jurisprudence provide an adequate base upon which to forge private contracts. Systems that allow the creation of contractual communities of transacting parties are now needed. The OBB PKI is an example of one possible business and technical model that could help parties achieve this result.

PKI systems can be based on private contracts that are formed electronically. This article accepts that pure electronic contracts (that is, a contract created totally online with no paper, ink signature, or other widely understood and accepted evidence such as faxes) would be the most efficient business and technical solution. However, it also recognizes that the current state of the law raises serious questions about the enforceability and logic of such a system. The National Conference of Commissioners on Uniform State Law is now drafting the Uniform Electronic Transactions Act to define and clarify the legality of electronic transactions.[19] This area of law, however, remains somewhat murky for the moment.

One of the main issues of uncertainty remaining is the question of who has entered into the web-based contract. Once digital signature or other adequate electronic authentication systems are commercially accepted, such a system could form the basis of this needed identification. In the meantime, there are hundreds of years of experience backing handwritten signatures. Thus, it may be appropriate that in the first instance the system of contracts that enables each party to participate within an OBB PKI should be executed by traditional pen-and-paper methods. Once the initial contract is executed and on file, the terms of the contract can (among other things) authorize subsequent contracts to be signed using a specified digital signature system.[20]

[19] National Conference of Commissioners on Uniform State Laws, *Uniform Electronic Transactions Act* (Mar. 23, 1998) <http://www.law.upenn.edu/library/ ulc/uecicta/eta1197.htm>.

[20] The legal doctrine known as the "equal dignities" rule supports this approach. *See* 68 AM. JUR. 2D SEALS § 7 (1993); William H. Danne, Jr., *Construction of Statutory Provision Governing Rejection or Waiver of Uninsured Motorist Coverage*, 55 A.L.R. 3d 216 (1974). The rule provides that to create or transfer authority to execute a document requires an instrument of equal dignity. *See* 68 AM. JUR. 2D SEALS § 7 (1993). For example, if a document requires a written signature, then the authority to transfer the power to sign may only be done via the written signature of the original authority. *Id*. While it is arguable whether use of a digital signature involves a true delegation of authority, there are practical reasons to choose use of a paper-and-ink signed contract to initiate participation within the model system.

Eventually, once there is sufficient experience and market penetration of electronic authentication systems, the issue of creating enforceable online contracts to opt into OBB-type systems will become more certain. In addition, legislative reforms underway at the National Conference of Commissioners on Uniform State Law will further clarify electronic contracting law. In the meantime, there exists a need to move cautiously in this area, such as by requiring an ink signature on a paper contract to start the electronic process. However, more risk-tolerant parties or parties with less liability exposure may wish to jump directly to online contracting systems. In this case, some method of pre-authentication of the electronically contracting parties becomes the chief concern, perhaps based on a shared secret, such as an account number or a password.

In the end, such decisions should be driven by the business case and informed by the comparative analysis of the risk, cost, and benefit of security options. Where the analysis so dictates, higher levels of reliability derived from established methods will be seen as cost-effective, risk-reducing methods to achieve the benefits of a given online transactional business system. When the costs are not justifiable due to relatively low expected benefits or shallow risks, then less reliable methods will be seen as appropriate.[21]

2. *Enabling Sound Decision Making*

The main impediment to electronic commerce today is not a lack of technical ability—rather, it is a lack of trust by would-be participants in the electronic commerce marketplace. The mistrust centers on whether the electronic commerce transactions in the public or private sector will provide adequate privacy, security, and enforceability. One possible reaction to this view is that legislation and marketing is needed to instill trust in the citizens and customers of the world. The point of view of this paper, however, focuses on the creation of systems that deserve to be trusted because they are reliable protectors of privacy, security, and enforceability. The ability to make sound policy and operational decisions regarding the authenticity and reliability of electronic messages over open networks must be predicated upon the existence of trustworthy computer systems[22] and trustworthy business practices.

This requirement would ensure future signature verification, assurance of contractual privity, and other factors relating to agreement enforceability.

[21] A cost, benefit, and risk analysis driven by the business case for deploying an online transaction should also be the process by which a person decides to build a PKI in the first place. The OBB model focuses on methods of risk reduction and assumes that the corresponding impact on the cost and benefit calculation will make PKI a viable tool for business transactions that would be otherwise inappropriate or unwise. However, it is also possible that once all the costs and risks are examined, use of other non-PKI technologies or no technology will be viewed as the most reasonable choice for any given business system.

[22] The *Digital Signature Guidelines* contain an excellent definition and discussion of trustworthy computer systems:

> 1.35 Trustworthy system
>
> Computer hardware, software, and procedures that:
> (1) are reasonably secure from intrusion and misuse;
> (2) provide a reasonably reliable level of availability, reliability and correct operation;
> (3) are reasonably suited to performing their intended functions; and
> (4) adhere to generally accepted security principles.

INFORMATION SECURITY COMMITTEE, SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR

A commercially viable PKI must enable sound decision making for anyone who uses or relies on digital certificates issued by an outside certification authority. Put another way, the systems and processes surrounding the use of a digital certificate by a subscriber or the acceptance by a relying party must provide enough information upon which to base a reasonable and justifiable "trust decision." Calculating trust will in turn require well-defined and understood policies, strong technical implementations, and reliable business systems. For these trust decisions to be legally sound, they should be built upon a verification regime. The verification can be supported by such measures as independent audits, insurance,[23] bonds, technical standards, and CA accreditation and held together by agreements among all the parties.

The technical standards can be a powerful tool to implement legal and business risk reduction practices. For example, one could implement a system wherein the certificate included only the subscribers public key and information on how to check with the CA to get the identity of the subscriber. This eliminates the possibility of reasonable reliance by unknown or unintended reliers on a certificate and forces the creation of a direct relationship between the CA and the relying party during which expectations can be clarified and agreed upon. Another variation on this architecture would be to construct a certificate that amounts to an "offer." The offer may be to reveal the identity of the subscriber in return for some value or other agreement (as in the example immediately above), or it may be more sophisticated—such as an "offer" to insure reliance upon the certificate or to provide other "value added" services.

A well-drafted agreement among the parties can serve as the method by which uncertainties are diminished. Once parties to a PKI transaction are engaged in the process of coming to agreement, the meaning and role of a certificate can be established. The basis of the underlying transactions and the relationship between the parties can also be clarified, agreed upon and enforced through such an agreement. The basic requirements of an OBB system are: knowledge of and assent to the transaction(s) to be conducted; knowledge of and assent to the parties to the transaction(s); and agreement as to the rights and duties of each party, including technical and business practices. These agreements are the basis of the CP and the mechanisms adopted to enforce the policy.

Other relevant documents will include the certificate practice statement, if any, of the CA, and the individual contracts signed (on paper or electronically) by each party within the OBB system. The contracts signed by each party (the subscriber agreement, the certificate authority agreement and the relying party participation agreement) would all reference a single, primary document that brought all parties into privity and that filled in the details—whether directly or via incorporation. In this way, each party could sign a relatively short and static document once, but the basic rules and policies of the OBB system could continue to evolve. The body with decision power over these rules is effectively in control of the process. The CP, under the approach being asserted in this paper, would be the primary document in

ASSOCIATION, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND ELECTRONIC COMMERCE 54 (1996).

[23] The VeriSign Certificate Authority already provides an insurance policy associated with certain certificates. *See* <http://www.verisign.com/idcenter/new/idplus.html>.

an OBB system. However, whether the document is called a CPS, a CP, operating rules, a multi-lateral contract, or whatever, the point is that all the major parties who would be bound by the document should have an opportunity to participate in the drafting and evolution of the policies and rules under which they chose to operate. Clearly, an OBB that includes consumer-level certificates would pose the most difficult problems with respect to negotiating terms in the interests of that constituent group. In the end, as with so many other economic activities, there will unfortunately probably be inadequate attention to consumer interests leading to a reaction of government- mandated consumer protection.

B. How and Why to Set Reliable, Enforceable Bounds Within the Environment

The PKIX CP Framework document notes that a "certificate policy may be used by a certificate user to help in deciding whether a certificate, and the binding therein, is sufficiently trustworthy for a particular application." The Draft Model Certificate Policy now under consideration by the Federal PKI Steering Committee indicates that use of a CP can create the trust and assurance needed to utilize PKI for business purposes.[24] The Working Draft of Certificate Policies for the Government of Canada Public Key Infrastructure (GOC PKI) presents the concept of a certificate policy as an important document for relying parties who are deciding whether to trust a CA.[25]

The position of this paper is that the CP and any other related operating rules must be enforceable legally and objectively verifiable in order to be sufficient for several categories of business transactions sought to be accomplished by public and private sector stakeholders. Several difficulties are posed by using open PKI for certain serious business applications. Sensitive, high value, and mission critical applications will require risk control mechanisms that are adequate for the underlying systems. For example, the CA and the subscriber should be worried that potentially limitless parties may rely, to their detriment, on a fraudulent certificate. A relying party, similarly, should be concerned about the lack of a direct relationship with the CA or the subscriber and the consequent lack of contractual privity and other business arrangements that follow.

How much risk—monetary and otherwise—might be created by reliance on an open PKI certificate? Assessing this risk would be next to impossible under an open

[24] *See* MODEL CERTIFICATE POLICY, *supra* note 5. The *Model Certificate Policy* provides: "Government and private entities that are considering accepting electronic communications need assurance that the digitally signed messages they receive can be verified with reference to a certificate that is appropriately trustworthy for the intended purpose. There is an increasing recognition that this assurance can be provided through the use of a *certificate policy*." *Id.*

[25] *See* CANADA CERTIFICATE POLICIES, *supra* note 3, at § 1.3. The *Canada Certificate Policies* provide:

> When a certification authority issues a certificate, it is providing a statement to a certificate user (i.e., a relying party) that a particular public key is bound to a particular entity (the certificate subject). However, the extent to which the certificate user should rely on that statement by the CA needs to be assessed by the certificate user. Different certificates are issued following different practices and procedures, and may be suitable for different applications and purposes. . . . Certificate policy definitions are therefore used by:
>
> - A CA when it determines which certificate policy identifier(s) to include in a certificate;
> - A relying party when it decides whether or not to rely upon a given certificate;
> - A CA accreditation body when it accredits a CA; any accreditation has to assess the extent to which a CA that claims to support a particular certificate policy satisfies the provisions of that policy. In this sense, a certificate policy acts as a set of accreditation criteria.

PKI system that does not maintain information about the parties and substance of transactions that are predicated upon a certificate. The issuance of a certificate in an open PKI environment may leave both the CA and the subscriber in a position of making risk decisions with inadequate knowledge of potential relying parties and transactional or usage reliance. While this result is certainly not inevitable in an open system, it is much harder to protect against such a result without the risk management techniques employed by bounded and closed systems. Several public and private sector transactions that are sought to be accomplished online require higher levels of trust and assurance. Reliable information must be accessible to all the parties to a PKI-based transaction. To be deemed reliable, some types of information must be verifiable (as in the case of certificate validity or compliance audits) or enforceable (as with CP compliance or clauses in participating party agreements).

An OBB system can begin to provide a convenient method of making important information available to each party to a transaction and giving the parties tools they need to make sound risk decisions. Again, a very open system that merely attempts to assert terms within a certificate or, worse yet, in some remote document like a CPS, that purport to place limits on usage, liability, parties, processes, and other vital factors without creating a process within which the limitations can be credibly relied upon and enforced simply fails to provide an adequate basis of trusted information for important business or government online transactions. Once the parties come together in agreement on the contours of an OBB, the bounds can apply to the parties, the transaction types, the computer applications, and other technical processes. A bounded system can also provide the basis of more sophisticated payment models for certificate verification by designing a bounded system within which the relying party must pay a subscription fee to check certificate validity or accept liability for possible invalidity. In addition, the creation of a bounded community permits and facilitates other more advanced risk reduction possibilities.

Risk reduction could include: the ability to keep track of the total number, value, or risk of certificate uses for purposes of enforcing a limit; the ability to create automatic, routine, and periodic "out of band" communications to subscribers to establish that identities and practices have not changed; and the ability to know with a high degree of certainty whether, when, and how much recourse will be available in the event of a breach. While it is true that the X.509v3 certificate already includes the ability to contain reliance limits, notices of liability limitations, and other potentially relevant risk information, the mechanisms to assure that this information is understood, agreed to, and binding do not universally yet exist. The OBB business model suggests a method for imbuing meaning and enforceability into the good work that has already been done at the standards level by the X.509 community. The participatory aspect of getting the parties within an OBB system to agree on the varied purposes and particular mechanisms to bound their system directly addresses the infirmities of more open systems and the rigid limitations on parties and uses associated with closed systems.

An important principle is that the legal aspects of enforcing the bounds of the model under discussion should be based in private law, not public law. Whether a CP, a set of operating rules, or any combination of these or other rules, the parties should maintain total freedom of contract to opt into the system and to opt out, to amend the system, and to enforce or choose not to enforce the system. The parties should remain in control of their own transactions and their own affairs. It may be possible to achieve the quality control of CAs from government licensing. However, the position of this paper is that private agreements relating to accreditation and auditing based on evolving market-driven needs is the best way to assure not only CA quality control but also reliable, predictable, and verifiable performance by the other parties as well. It is acknowledged, however, that certain consumer protection measures may be necessary to correct market failures that might develop.[26] However, any such corrective action should be narrowly tailored to respond to sufficiently known problems in the market, not preemptive and regulatory requirements based upon bureaucratic guesswork.

Of course, some countries in the world may choose to enact more regulatory regimes for dealing with electronic commerce and PKI. That is unfortunate for the people of those countries. The United States should follow a policy of encouraging other countries to join our pro-market ways, but if a foreign jurisdiction insists on enacting regulatory proscriptions, then the U.S. should fight for foreign legal recognition of accepted industry practices for CA accreditation or other adequate private sector mechanisms.

This paper suggests three categories of mechanisms for defining and enforcing the bounds of an OBB system: legal, technical, and business. While any one or two of these categories are useful, taken together, these mechanisms can provide a robust suite of risk reduction techniques that are mutually reinforcing.

> **Legal example:** Each party to the system enters a legal agreement to abide by certain rules, including: a promise not to use or rely on system certificates for prohibited uses or outside the authorized parties within the OBB system; an agreement to abide by certain technical practices (see below); and a promise not to reveal information that is confidential within the OBB system (see below).
>
> **Technical example:** The CA public key that is necessary to verify the CA's signed certificate is not shared widely (such as by loading them into off-the-shelf web browsers); rather it is strictly kept within the circle of authorized users. This significantly reduces the risk that an unintended third party who is outside the system may rely on an OBB certificate. In order for an unintended third party to rely on a certificate, an OBB system member would have had to leak the key, or the party would have had to have hacked it or come by a hacked key. In other words, potential unintended third-party reliers who come across a leaked certificate and verification key from the signing CA would have significant notice that the key was not circulating through normal, reliable circles.
>
> **Business practice example**: Each party would comply with the everyday business practices, including routine information security safeguards by the user and relier, such as maintaining information designated confidential within the system. Depending on the risks and costs, such confidential information could include special data to be used in the subscriber's name field of the certificate in place of a common name (i.e., rather than "Rick Ricardi," the field might contain an alpha-numeric string that is unique within the system to that user; provided no OBB parties divulged that information, then no unintended reliance would be possible

[26] For example, if systems are created that pose an undue threat to the privacy, or vulnerability to fraud and crime of the customers, then government action may be required.

because would-be relying parties outside the system would have no way to determine who is the person or entity listed in the certificate).

V. TRADE-OFFS BETWEEN OPENNESS AND RISK AND LIABILITY

Given the current state of inexperience with all but embryonic commercial PKI systems, it is expected that parties who might participate in an OBB system would desire to strictly limit the type, number, and value of the transactions conducted.[27] One of the benefits, as has been mentioned earlier, of bounding a system is that the parties have unprecedented capacity to specify creative limits on permitted and prohibited uses of certificates. This can be an important tool for controlling and managing risk and liability. It must be recognized, however, that instituting risk reduction mechanisms is not without cost. For example, the business practice of using alpha-numeric code data that are not obviously related to the subscriber's "real name" would necessarily require additional processes at the sites of the CA and of each relying party to re-connect the certificate with the identity of the subscriber. This limitation would require on-the-fly collation of certificate "name" and the real name of the subscriber.

On the other hand, setting up servers to key off a code name rather than a natural name is rather trivial technically, and it may provide opportunities to convey important authority information. The entire process of using a certificate is machinable, so, unlike a desk clerk who may be attached to a client's real name, the server does not care whether it is looking for "John Eskew" or 345BCD. Virtually every account or authority based system can operate on user identification information that is different from the natural name, and in some cases, the non-name system data is the primary authentication matric (account numbers, biometrics, PINs, etc.). Therefore, this aspect of an OBB system can be a more direct method of keying authentication to authority, role, and attribute rather than physical identity.

Another potential negative limitation of an OBB system is the possibility of overly restricting permitted uses of a certificate to the point of inefficiency. On the positive side, as has been mentioned, restricting permitted uses and transactions can serve as a valuable risk reduction technique. However, the policies and rules of an OBB PKI need not directly specify the rights and responsibilities of the parties relative to the underlying transactions conducted by means of the system. The parties would be free to agree upon any expansion of permitted certificate uses within the system. Once a person, business, or government agency opts into the OBB system, each authorized participating party could be free to use and rely on system certificates in an "open" manner.

Each party within the OBB system could agree that their OBB digital signature is an enforceable signature for any and all purposes when used with any other party

[27] Today, the market is already moving toward more bounded systems that would remain potentially interoperable with other bounded systems. The VeriSign OnSite product and the GTE CyberTrust Customer Branded CA Services allow organizations to act as a "Local Registration Authority" (LRA). An LRA acts as the authenticator of certificate subscribers to pre-authenticate them to the CA. These directions in product and service offerings show a responsiveness among market-leading companies to a demand for more control over the people, processes, and uses of certificates for certain business transactions.

in the bounded system. The rules would establish the identities of the parties and set a baseline framework within which to reasonably rely on a digital signature, and the parties would be free to set any other transaction types, liability provisions, business obligations, etc. Depending on the needs of the parties, the OBB system could enforce certain requirements—such as online verification and aggregate value reliance limits over the life of a given certificate—but may remain silent as to prohibitions on the types, number, and frequency of certificate usage.

There is an obvious utility in permitting as many uses of a given certificate as practicable. The more uses a certificate can be put to, the more efficient that certificate can be. Similarly, as more communities are afforded the ability to leverage each other's certificates, including identity, role, authority, and other certificate types that are emerging, the more sophisticated and valuable PKI can become as a business tool. It is assumed that parties would desire maximum permitted uses of a given certificate within a given bounded system. It is further assumed that incremental steps toward increasing permitted uses is the prudent path forward during future testing and initial deployment. The optimal setting between openness and control of the parties and transactions within an OBB PKI should be based on factors of risk, cost, and benefit associated with the business uses by each party of the system. In setting the balance between openness and control, the liability will be easier to deal with the more controlled the system becomes.

VI. IMPLICATIONS FOR THE DRAFTING OF A CERTIFICATE POLICY AND RELATED CONTRACTS

A. OBB Certificate Policy Drafting Issues

The following section headings correspond to sections from the PKIX Part IV CP Framework. Implementing an OBB system would require answering the issues raised under each section.

Introduction

Community and Applicability

This section of a CP forms the crux of an open but bounded system. In this section, the permitted and intended users and uses are described.

sample language

"The permitted community for use of this certificate policy are the parties who have agreed to opt into this system by applicable Agreement. Only parties who have signed an applicable agreement under this CP and who abide by this CP may participate in the community herein. Applicability, including intended, permitted and prohibited transactions and other uses for certificates issued hereunder must be in accordance with the applicable underlying agreements."

Contact Details and Specification Administration

This section, though short, is highly relevant. It stipulates the party authorized to administer this CP. In the case of a state government CP, one might expect such a contact to serve under the governor or other applicable leader of a branch of government. This becomes a more interesting question when multiple governments and the private sector agree to be bound by a given CP. Who, or what combination of parties, shall make the rules?

GENERAL PROVISIONS

Liability

The provisions under this section may vary depending upon the permitted parties, uses, and processes associated with the CP. Under the Government of Canada draft CP, for example, the liability limitations permitted vary depending on the level of assurance indicated by the certificate. The various levels of assurance from rudimentary to high are all comprehended under a single CP in the Canadian draft. Similarly, an open but bounded system could specify differing liability and obligation requirements depending on the permitted parties, uses, or technical processes that are intended or prohibited under any part of the CP. Whether such variations in permitted and prohibited subject matter are best left to the individual agreements or must be reflected in the CP itself would be a matter for the particular parties to the CP to determine.

Financial Responsibility

Issues such as indemnification of any party by any other party would be described under this section. As with the liability provisions, these obligations should be tailored to suit the particular permitted and prohibited uses and parties under a given part of the CP. For example, if under the CP, several levels of "boundedness" were specified, from tight control over parties and uses at one end of the scale to liberal permission for any uses with any parties to the CP at the other end, then it can be expected that the additional risks associated with the more open uses would also entail more stringent and contentious financial responsibility clauses.

B. Participation Contracts

Each party to the OBB system would execute a contract as part of the participation process. Each agreement would have certain clauses that are common. For example, each participant would need to be bound to the terms of the CP or other enforceable rules and policy documents, including amendments with notice and subject to governance votes. In this way, each party would only need to sign one agreement at one time, rather than needing to sign a agreement with every other party to the OBB. Due to scalability issues, the number could grow quite large over time and the main document might change from time to time to reflect newer technologies and thinking in the field. Linking each participant agreement to the main agreement by reference allows parties to avoid re-executing the agreements with every partner every time there is a change in the process or minor rule change.

The subscriber agreement may include, among other things:

- some indication of the intended, permitted, and prohibited uses of the corresponding certificate;
- warranties that the undersigned is in fact the person identified or authorized as the Subscriber;
- agreement to abide by required business practices, such as not to use the certificate with parties outside the OBB system, agreement not to disclose the code name within the name field of the subscriber's certificate, and so on;
- based on the scope of parties and transactions, the party can sign a clearly enforceable contract (paper or otherwise) indicating the subscriber intends for the listed digital signature to be her legal and valid signature for purposes of conducting the listed transactions with listed parties. Alternatively, in the case of an OBB within which no restrictions on uses apply, this clause might simply assert that "the following digital signature shall be my valid and enforceable signature for any and all purposes when used within the technical limits of and with any party to this OBB PKI . . .";
- liability of the parties.

The CA agreement may include, among other things:

- agreement to issue certificates to any authorized party under an OBB system;
- signed audit form by a suitable CA auditor warrantying compliance with the standards of the CP and any other applicable requirements [such as the CPS];
- liability apportionment;
- depending on the business model, the CA might be the only obvious party to come into sufficient contact with the subscriber that it makes sense to have participating CAs require each subscriber to complete, agree to, and submit the appropriate contract.

The relying party agreement may include, among other things:

- an agreement not to rely on certificates being used within the OBB for reasons other than permitted applications under the CP;
- agreement not to share the clear text names of participants to the OBB systems;
- a promise not to share the public key of the CA;
- apportionment of liability between the CA, the subscriber, and the relying party.

An open but bounded public key infrastructure system would be based on legal agreements, technical processes, and business practices among voluntary private participants. These types of measures permit parties to directly manage the risk, liability, and effectiveness of electronic commerce authentication mechanisms. The emergence of more complete risk and trust management tools such as the ones outlined as part of an OBB PKI for certificate usage among parties may be the single most important factor if PKI is to become a fundamental part of the growing secure online world of the immediate future.