## Foreword

{0.1} This Report, "The Role of Certification Authorities in Consumer Transactions," is a work product of the Internet Law and Policy Forum. The Forum has been established by a consortium of companies from Europe, the Americas, and Asia in order to provide a neutral venue in which commerce, government and the stakeholders in the Internet community may gather to develop solutions to the challenging law and policy questions of the Internet. Further information on the Forum may be obtained on the Internet atwww.ilpf.org.

{0.2} This Report was prepared by the Forum's Working Group on Certification Authority Practices. This Report has been prepared pursuant to the announced Work Plan and procedures of the Working Group on Certification Authority Practices. These materials are available from the Internet Law and Policy Forum at http://www.ilpf.org/work/ca.html. The Terms of Reference and the Work Plan are attached to this Report as Appendix 8. Pursuant to the Work Plan and the procedures of the Forum, the publication of this Report should not be considered to represent the views of any one or more of the Sponsors of the Forum or those companies or organizations nor should their participation necessarily be considered to endorse or recommend the contents of the Report in any manner. Any questions regarding this Report, the Forum or the Working Group may be addressed to info@ilpf.org or by contacting the Forum's offices in Montreal:

Internet Law & Policy Forum
World Trade Centre
Bureau 3280
380, rue Saint-Antoine Oues, bureau 3280
Montreal, Quebec H2Y 3X7
Canada
514.288.1966 (voice)
514.288.1177 (fax)
info@ilpf.org

{0.3} The Working Group, and the companies and other organizations participating in the development of this Report, included the following:

Working Group

Bruce Hunter, General Electric Info. Services
Hong Kong Telecommunications
Colm Dobbyn, Mastercard Corporation
Barbara Fox, Microsoft Corporation
Peter Harter, Netscape Communications Corp.
David Schellhase, Premenos Corporation
John Makaryshyn, Telus Corporation

Andrew Konstantaras, VISA Corporation
Jeffrey Ritter, ILPF Organizing Chair (ex-officio)

Additional Participants

CertCo
CommerceNet
DFN-CERT
Entegrity Solutions
IBM
Institut Jozef Stefan
Nortel Secure Networks
OECD Committee on Consumer Policy
Signet Systems
UNINETT

{0.4} Legal Rapporteur--Cooley Godward LLP, Palo Alto, California. The Cooley Godward team included Terrence P. Maher (Boulder, CO), Eric Schlachter (Palo Alto, CA) and C. Bradford Biddle (San Diego, CA), with assistance from Melissa Richards (Boulder, CO) and Janice Phillips (Palo Alto, CA).
Technology Rapporteur--Manny Pasetes, Premenos Corporation.

{0.5} Input on German law issues provided by Christopher Kuner and Dr. Matthias Karl of Gleiss Lutz Hootz Hirsch & Partners, Frankfurt, Germany.

{0.6} A list of CAs invited to participate in the process of developing this Report is also included on Exhibit A.

{0.7} The substance of this Report was completed in January, 1997, although portions have been updated since then. Except where otherwise specified, readers should assume that this Report is current through January 1, 1997.

## 1. EXECUTIVE SUMMARY.

{1.1} This Report represents a preliminary analysis of certain questions relating to legal issues involved in the emerging service business of certification authorities, particularly those arising in consumer transactions. The scope of this Report has been limited intentionally to focus on the selected legal environment in the United States, although additional information has been provided on German law, the directives of the European Commission and laws in other jurisdictions. In addition, this Report only addresses consumer transactions taking place in an "open system," where a CA provides services to any consumer desiring services without regard to the contractual obligations between the consumer or the merchant and any payment system. As a "pilot" project of the Forum, a more comprehensive analysis, though appropriate, was not within the scope of available resources.

{1.2} This Report analyzes the complicated relationships between CAs, merchants and consumers. In the absence of specific "digital signature legislation," existing legal principles indicate that:

* As between CAs and consumers who procure a digital certificate, the relationship is likely to be governed by existing contract laws. In particular, we believe that digital certificates will be treated as a service, not a good, and therefore the common law is likely to apply (instead of the Uniform Commercial Code or other rules covering "goods"). However, there are a number of reasons that the contracts formed between CAs and consumers will not completely resolve the matters that could arise from the relationship, and default rules will be needed.

* As between CAs and merchants who receive the digital certificate from consumers, the CA/merchant relationship is likely to be governed by existing tort law, not contract law. In particular, the "negligent misrepresentation" tort is likely to provide the most applicable set of rules to govern the CAs' liability to merchants if the digital certificate is incorrect.

{1.3} Within this context, we believe that a party's liability for losses arising from this structure should generally be connected to whether or not the party acted reasonably. As a result, generally if one of the parties acts unreasonably and the other parties act reasonably, the party acting unreasonably should bear the resultant loss. However, if all parties act reasonably and yet a loss is suffered, we believe that loss should be borne by the merchant. Further, if the consumer acts unreasonably, we believe that consideration should be given to limiting the consumer's losses, and any losses not covered by the consumer would then by borne by the merchant. In both cases, the merchant may be in the best position to take the necessary efforts to avoid the loss or, alternatively, to insure or otherwise spread the loss among all consumers.

{1.4} This Report provides some suggested parameters on what behavior should be categorized as reasonable. As with other issues raised by this Report, additional study should be done on these parameters.

## 2. INTRODUCTION.

### (a) **Summary of the Problem.**

{2.1} Despite its impressive size, scope and reach, the Internet has not yet become a predominant vehicle for consumer transactions. In part, consumers are reticent to use the Internet for commercial transactions due to perceived and actual security threats online. Merchants also have reasons to be concerned about online commerce -- the integrity, authenticity and nonrepudiability of electronic messages are not automatically ensured.

{2.2} One possible way to improve the integrity, authenticity and nonrepudiability of electronic messages is to develop a robust public key infrastructure ("PKI," also referred to as Public Key Authentication Framework) -- and in particular, foster the use of digital signatures in commerce. Appendix 6 to this Report serves as a brief primer on digital signatures, certificates, and public key cryptography; we suggest that readers who are not familiar with these concepts review this Appendix prior to reading this Report.

{2.3} One difficult problem encountered when using digital signatures is ensuring that the identity of a person who holds an encryption key pair is accurately known. Trusted third parties called Certification Authorities ("CAs", sometimes referred to as "intermediate systems" or "certifiers") offer a way to confirm that a public key belongs to the claimed owner. The CA does this by issuing a certificate which associates an individual with a particular public encryption key.

### (b) **Focus of this Report.**

{2.4} This Report addresses the use of certificates in consumer transactions, and thus does not explore the issues raised by the use of certificates in a business-to-business setting. Even within the framework of consumer transactions, however, the scope of this Report is limited. The issues implicated by digital certificates are extensive and complex, and certificates are being used in increasingly novel and imaginative ways. We briefly highlight some of the issues we have not addressed, and some of the major assumptions we have made, in Appendix 1, and readers will benefit by reviewing that Appendix prior to reading the main body of this Report.

{2.5} This Report focuses largely on what might be called the "open system" or "open loop" model. The open system model assumes that consumers will obtain a single "identity" certificate from an independent third-party CA and then use that certificate to facilitate transactions with potentially many different merchants.

{2.6} There are several reasons why we focused on the open system model:

{2.7} First, the open system model raises some extraordinarily difficult, and perhaps unprecedented, legal and policy questions regarding the rules that will govern a complex set of interrelationships between parties. By way of contrast, in closed

systems, the relationships between the relevant parties may be governed by contract law and/or existing payment system legislation and regulation--both relatively well-understood and predictable frameworks for analyses. However, if the applicable contract law or other laws fails in the closed system model, the default rules likely to apply are those discussed with respect to the open system model.

{2.8} Second, nearly all legal efforts to date which address PKI issues implicitly assume an open system model. The "digital signature" laws that have been enacted to date in the United States are largely aimed at promoting development of a PKI based on this independent third-party CA model. Similarly, U.S. government efforts at promoting the development of a PKI assume an open system model, as do the Digital Signature Guidelines published by the Information Security Committee of the American Bar Association's Section of Science and Technology. References to these documents are available in Appendix 5.

{2.9} Third, this project was initially conceived in Spring 1996. At that time, it appeared that industry efforts were being primarily directed towards developing open systems and therefore that open systems were going to be the prevailing business model. In fact, in the period during which this Report was written, the open system model has appeared to become an increasingly less viable business model. Instead, we believe that many consumer transactions which utilize certificates will occur in a "closed system" or "closed loop" model. A definition of closed systems and further discussion about the differences between closed and open systems can be found in Appendix 2. Closed systems primarily fall into two categories: systems where a payment mechanism serves to "close the loop" by forming contractual agreements with the relevant parties, and systems where certificates are used as an access control device to meter out usage of intellectual property or to limit access to proprietary resources.

{2.10} Despite our growing doubt over the desirability and viability of the open system model in the context of consumer transactions, this Report focuses on some of the difficult legal and policy questions raised by this model. We do interject discussion of closed systems where we believe such discussion is illuminating. Furthermore, because the lines between the models we have identified are blurry, and because new business models continue to evolve in the marketplace, we believe that some of our discussion concerning open system models will also be applicable in other contexts.

{2.11} This Report attempts to identify certain issues that are relevant to both entities participating in an open system-oriented PKI and to policymakers interested in shaping the continuing development of such an infrastructure. These issues include:

- {2.12} What practices should be expected of a CA in connection with that CA's relationship with consumers who are the CA's customers? What limitations, if any, should be placed on that CA's ability to disclaim liability for failure to adequately perform these practices?
- {2.13} What practices should be expected of consumers of CA services? Should potential liability for failure to perform these practices be limited in any fashion?

- {2.14} What practices should be expected of merchants who rely on certificates issued by a CA? What legal relationship should a CA have to merchants who rely on a certificate but who have no other connection with the CA? Should a CA's potential liability to merchants be limited in any fashion? What mechanisms could potentially be used to limit liability?
- {2.15} Which party in the relationship (CA, consumer, or merchant) is best able to assess and price against the risk of loss?

(c) **Goal of this Report**

{2.16} This Report is intended to be a concise, non-comprehensive summary and analysis of the emerging legal rules and business practices regarding CAs serving consumers in an open system. If successful, this Report will serve as a building block for further analysis of the issues and for the ultimate development of a set of legal and policy guidelines that may be consulted by both the public and private sectors.

{2.17} Ultimately, this Report will be most helpful if it contributes to the process of developing sensible, uniform and predictable rules in this area. As noted throughout the Report, there is a strong likelihood that the participants in a PKI will be confronted by a patchwork quilt of unpredictable rules, making compliance -- and even the process of analyzing rules with a view towards compliance -- difficult. The lack of uniform and predictable rules is a major deterrent to the development of a PKI and the participation by a substantial number of players. We view the development of clear and predictable rules as an essential step in the development of a robust electronic marketplace.

{2.18} This Report omits footnoting to enhance its readability by a wide range of audiences. Supplementary resources are listed in Appendix 5.

{2.19} While the members of the Working Group all have a commercial interest in the development of electronic commerce through a PKI, this Report has deliberately attempted to avoid favoring, evaluating or endorsing any particular standards, vendor, product or business model. CAs and working group members have been invited to submit their own written comments to this Report. Any comments that were received are attached as Appendix 9.

{2.20} This Report is for informational purposes only and is not intended to form an attorney-client relationship. Readers should seek professional legal counsel for advice regarding their specific situation.

{2.21} In total, this Report consists of this document and the following appendices:

Appendix 1: Scope and Assumptions of the Drafters of this Report.

Appendix 2: Analysis of Open vs. Closed Systems

Appendix 3: Survey of Laws Relating to Digital Signatures

Appendix 4: Comparison of Current Business Practices of Selected Existing CAs (including a list of known CAs).

Appendix 5 Bibliography of Selected Resources About Digital Signatures and CAs, including a list of passed and pending digital signature legislation and the location for obtaining electronic versions of some legal resources referenced in this Report.

Appendix 6: Description of Digital Signatures

Appendix 7: Analysis of existing CAs' compliance with existing legal systems (Note: this appendix is merely the structure for this analysis.)

Appendix 8: Terms of Reference and Work Plan for the Working Group.

Appendix 9: Written comments submitted by CAs and working group members.

{2.22} As a pilot project of the ILPF, this Report by necessity does not address or analyze all of the interesting or difficult questions related to CAs. The Working Group believes that additional work should be done in this area to address these questions.

## 3. BACKGROUND.

(a) **Glossary**.

{3.1} Discussions about PKI are notoriously burdened with acronyms and technical terms. The following is a non-comprehensive glossary of some of the key terms used in this Report.

{3.2} *Certificate* or *Digital Certificate*. A digital certificate contains information about the consumer (including the consumer's public key) and is signed using the CA's public key. See Appendix 1 for a more complete description.

{3.3} *Certificate Revocation List ("CRL").* A list of all digital certificates from a specific certificate authority that have been revoked.

{3.4} *Certification Authority ("CA").* A certification authority provides to consumers a digital certificate that links a public key with some assertion about the consumer (e.g., the consumer's identity, the consumer's account at a financial institution, the credit payment card number, etc.). CAs may offer other services such as time-stamping, key management services and CRL services.

{3.5} *Certification Practices Statement ("CPS").* A statement of the CA's practices with respect to a wide range of technical, business and legal issues that may be used as a basis for the CA's contract with the entity to whom the certificate was issued (in this

Report, normally the consumer). In an open system, the degree to which the CPS of the consumer's CA may provide a contractual basis governing the *merchant's* rights and obligations is unsettled. In a closed system, CAs will likely have the opportunity to enter into contracts with all parties to a transaction, and the CA's CPS will presumably be incorporated into such contracts.

{3.6} *Consumer*. An individual procuring goods or services online. In an open system, the consumer is often referred to as a "subscriber" upon the consumer obtaining a certificate from its CA. This distinction might be confusing in situations where both the merchant and the consumer have digital certificates that are used to conclude a transaction. In such circumstances, both parties are "subscribers."

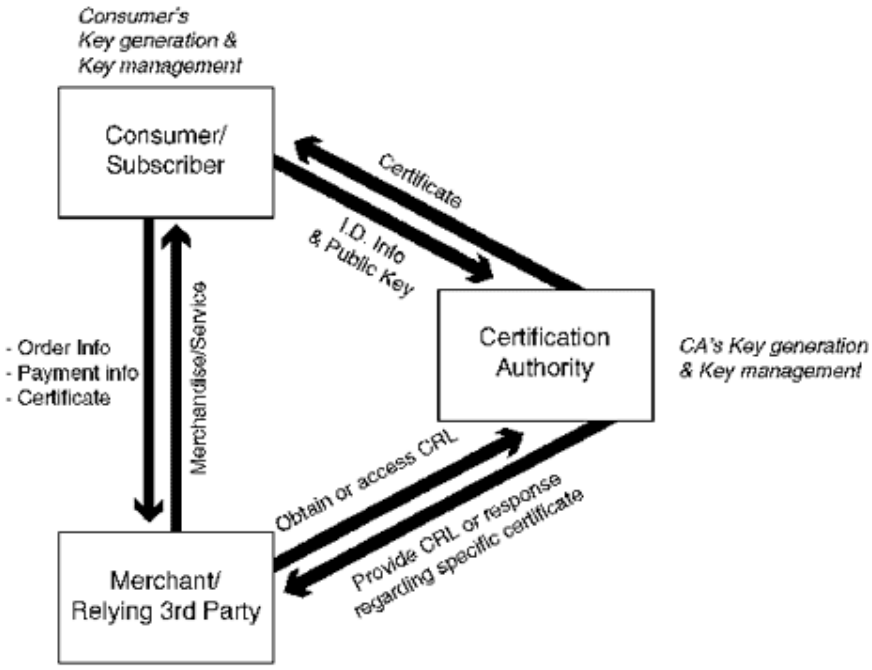
{3.7} *Merchant.* An entity offering goods or services online that will receive a certificate as part of the process of completing the transaction with the consumer. In an open system, the merchant is often referred to as the "relying third party."

{3.8} *Private Key and Public Key.* The use of digital signatures requires the creation of a pair of mathematically-related, large composite prime numbers. One of these numbers is arbitrarily called the public key and the other is called the private key. The private key is kept secure, while the public key is made publicly available. By definition, every public-private key pair is completely unique, so there is only one public key for every private key.

(b) **Model Internet Commerce Transaction Utilizing Digital Signatures.**

{3.9} Describing digital signatures and CAs proves to be a rather complex task. We have prepared the following diagram as a simplified way of illustrating the situation where the consumer delivers a certificate to the merchant as part of an online transaction. Readers should note that many complexities have been abstracted away from this diagram. This diagram also does not reflect the possible delivery of merchant's

certificates to consumers to authenticate the merchant's identity.




{3.10} In summary, the process generally may work as follows:

Step 1: Consumer generates a public and private key using a key generation system (either software or software combined with hardware) resident on the consumer's system.

Step 2: Consumer provides a CA with identifying information and the consumer's public key. The CA provides the consumer with a certificate.

Step 3: The consumer and the merchant enter into a relationship; the consumer delivers order information and possibly payment information (e.g., "allow me to read your online magazine and bill me at my home address" or "send me the following goods and debit account number 123456789" or "allow me to download your report in exchange for this contractual promise to pay you") digitally signed by the consumer using the consumer's private key, and the consumer's certificate signed by the CA's public key.

Step 4: The merchant verifies the certificate (and any certificates of the CA or its CAs) and checks the certificate revocation list (if one exists) to confirm that the certificate has not been revoked.

Step 5: The consumer and merchant complete the transaction.

(c) **Why Use Certificates?**

{3.11} There are three primary goals that can be facilitated by a PKI: authentication, non-repudiation and message integrity. To varying degrees, certificates can play a role in fostering these objectives. A fourth goal of a PKI, confidentiality, raises issues outside the scope of this Report.

{3.12} This Report focuses on the use of certificates to promote authentication. In this context, authentication means confirming the identity of a party. Merchants would desire authentication of consumers as a way to enhance the likelihood that they are dealing with the person who is in fact the true owner of the public key. This promotes merchant comfort that the transaction is legitimately placed and provides potential recourse in the event there is a problem.

{3.13} Conversely, although not dealt with specifically in this Report, consumers will want certificates from merchants to authenticate merchant identity. Consumers would desire authentication of merchants as a way to enhance the likelihood that they are dealing with the merchant who is in fact the true owner of the public key. This promotes consumer comfort that the ordering information (including terms about payment mechanisms) is not being collected by a party who intends to abuse the ordering information.

{3.14} Non-repudiation means that a person making a statement (such as a consumer placing an order) is not able to deny making the statement. If the mechanisms to authenticate identity work properly, the goal of non-repudiation would be facilitated; if identity is confirmed, there would be few grounds on which the consumer could say that the statement attributable to them was not actually made by them. While digital signatures may prove to be an excellent way to obtain non-repudiation, currently private keys are maintained in environments -- such as on hard drives or networks which are password protected -- where they could theoretically be expropriated with less effort than would be required to determine them through a brute force attack on the keys themselves. Hardware tokens, such as storing private keys on smart cards, would confirm that the user of a private key is the party authorized to do so; hardware tokens tied to biometric devices would provide even more assurance.

{3.15} Merely providing authentication helps reduce fraud, at least by permitting recourse in the event there is a problem. Non-repudiation would further reduce fraud by preventing parties from fraudulently denying making a statement that was made. However, few existing systems currently completely eliminate fraud; at most the systems reduce fraud, and uneliminated fraud becomes part of the cost of doing business.

{3.16} Finally, the public key listed in the certificates can be used to validate the message digest, which is a numerical representation of the document's contents to which the digital signature is attached. This tells the recipient of the message (and the certificate) that the contents have not been altered; it also could permit the sender to

prove the contents of its message as sent. In both cases, message integrity gives comfort to consumers and merchants that the message contents can be relied upon.

## 4. PROPOSED BUSINESS PRACTICES.

{4.1} In a consumer transaction involving digital signatures in an open system (as discussed in this Report), there are three principal entities whose rights and responsibilities affect the transaction: the consumer, the CA and the merchant. Other entities may play an important role as well, such as software and hardware providers, timestampers, notaries who assist CAs in the authentication process, and other providers of ancillary services.

{4.2} This section addresses, first, the question of what legal framework is most appropriate for analyzing the relationship between the three principal entities (CA, consumer and merchant) in an open system. The analysis in this section draws heavily from the extensive survey of existing laws found in Appendix 3, and readers may find it helpful to review that Appendix in conjunction with this section. In this section we conclude that the relationship between CA and consumer is most appropriately governed by contract, and generally endorse the proposition that CAs and consumers should be free to negotiate the terms of their relationship, subject to certain limitations. With respect to the relationship between CA and merchant, however, we assert that tort law may be the best framework on which to analyze allocating duties and liabilities. We suggest that attempting to bind merchants to contract terms incorporated by reference into certificates may be untenable as a matter of basic contract law, is economically inefficient and is contrary to sound public policy.

{4.3} Next we address our thesis that participants in a PKI must be obligated to act reasonably, and if a party acts reasonably that party should not bear a loss caused by another party's unreasonable behavior. This proposition prompts two questions. First, what constitutes "reasonable" behavior? Second, who bears the risk of loss if all parties act reasonably and yet a loss still occurs? We address each of these questions in turn, first highlighting some behaviors which we suggest could reasonably be expected of consumers, merchants, CAs and, more summarily, providers of ancillary services. Then we turn to the question of which party should bear the risk of loss in a "fault-free" situation. Acknowledging a long history of consumer protection legislation, we conclude that the liability of consumers should be limited even in a situation where the consumer has not acted reasonably.

{4.4} This section outlines a framework for discussion and more comprehensive study.

(a) **Tort v. Contract.**

(i) **CA/Consumer Relationships.**

{4.5} We believe that the relationship between CAs and consumers is best governed by contract. In an efficient and competitive marketplace, consumers can choose CAs based on the CAs' performance, terms of service, cost and other parameters, which in most situations will be spelled out in a contract that the consumer can choose or reject. Therefore, within the limits of general contract enforceability, and acknowledging that there are perhaps a few provisions where the market may not be sufficiently efficient, generally we would expect that the relationship between CA and consumer will be contractual.

{4.6} There are a large number of technical, business and legal issues a CA must confront, and therefore in some circumstances CAs will be tempted to develop long and extremely complex agreements. While there is no indication that the marketplace, working properly, will fail to reach the right result, it should be understood that significant burdens are being placed on consumers to analyze these contracts and still make rational choices. It is possible that consumers will be unable to properly distinguish between CAs because of this significant burden; in that case, it would be appropriate to evaluate alternatives to allowing contract law to govern the relationships between CAs and consumers.

{4.7} Despite the appeal of allowing the CA/consumer relationship to be governed by contract, there are many obvious problems with contract formation that dictate that gap fillers or other principles are required. Consumers could be afflicted with incapacities to contract (such as minor status). Consumers could not speak the language in which the contract was written (see Transborder Issues below). The contract could be unconscionable or a contract of adhesion under applicable law. Finally, portions of the contract may contradict local laws and therefore be void for public policy.

{4.8} Therefore, there is a compelling need for a default set of rules for this relationship, whether stated as default contract terms (such as the UCC) or as tort principles. These rules could be developed as a self-regulatory code, to be incorporated into the contract by reference, or by statutory law. It is unlikely that the electronic marketplace's need for uniformity and predictability will allow for less formalized alternatives.

(ii) **CA/Merchant Relationships.**

{4.9} It is less clear that the relationship between CAs and merchants should automatically be governed by contract. Merchants are seeking only the accuracy of information contained in a certificate (and, presumably, the performance of the underlying services necessary to verify such information). Imposing the obligation on merchants to review each "contract" they will be asked to enter into appears to impose significant transaction costs on the process. Not only may the merchant be dealing with multiple CAs, each with their own custom certification practices statements, but each

CA may choose to amend a certification practices statement over time, requiring a merchant to check each certification practices statement for each certificate received. We note that it may be cost-effective for a CA to specifically negotiate a mutually-executed contract with merchants who repeatedly use their services, but this may be an exception rather than the rule (but see Appendix 2, "Closed vs. Open Systems").

{4.10} In the absence of a specifically negotiated contract between CAs and merchants, the most efficient approach for allocating liability may be the existing negligent misrepresentation tort. It allows CAs to internalize the costs of their actions while not imposing large upfront transaction costs on the parties. Furthermore, it allows the CA to avoid liability by acting "reasonably" without allowing the CA to abuse the contract formation process by imposing excessive terms. However, CAs should be able to state their assumptions by qualifying what facts they are providing and what efforts the CA used to verify those facts. In this way, if the CA performed the services it promised to perform in a reasonable way, the CA should have no liability. If the CA acts negligently, the CA could incur liability to merchants. However, we recognize that this approach has limited applicability in civil law systems with tort law principles that are substantially different from those under United States law.

(b) **Obligation to Act Reasonably.**

{4.11} As a starting point for allocating losses, we believe each party has the duty to act reasonably. If a party fails to act reasonably, where the other parties have acted reasonably, then the party acting unreasonably should expect to bear the loss. Therefore, the discussion that follows focuses very much on reasonable behavior and, where possible, suggests standards that should be considered when determining if a party's behavior was reasonable. However, in acknowledging the important role consumers play in this process, we suggest that consideration should be given to the desirability of limiting consumers' losses even when the consumer does not act reasonably. Also, there are likely to be situations where all of the parties act reasonably and yet a party suffers loss -- these are dealt with in Section 4(g) below. We have not attempted to suggest loss allocations when more than one of the parties acts unreasonably.

(c) **Consumers.** {4.12} We suggest that the following behavior by consumers constitutes reasonable behavior:

{4.13} (i) **Provide Accurate Information.** Any consumer who provides false or incomplete information is acting unreasonably. Any consumer who fails to update information being certified is acting unreasonably.

{4.14} (ii) **Respond to Notices.** In systems where the consumer is given the opportunity to verify or accept a certificate, the consumer should review the certificate within a reasonable period of time and take all reasonable efforts necessary to correct errors promptly.

{4.15} (iii) **Keep Private Key Secure.** Consumers should use best efforts to keep their private key secure. Given that certificates may provide different levels of assurance regarding a consumer's identity, the consumer's efforts to keep their private key secure should increase with the extent of the certificate's assurance of the consumer's identity. Currently, however, many consumers would keep their private keys on a system which is accessible by entering a password which may be easier than the private keys themselves to determine via a brute force attack. Technologies such as hardware tokens (such as passcards or smart cards) or biometric devices would potentially increase the security of the private key's storage, but these technologies have not been universally deployed.

{4.16} Furthermore, consumers should strictly follow all instructions provided by hardware, software, and other equipment providers. Accordingly, entities which provide hardware or software products should be expected to provide clear and concise instructions to consumers detailing the steps that the consumer must take in order to keep their private key secure.

{4.17} (iv) **Generate Keys Securely.** If consumers generate their own key pairs, they must do so on a reasonably trustworthy system in a secure fashion. Again, it must be incumbent upon the suppliers of cryptographic hardware and software to clearly and succinctly convey to consumers the steps required to achieve this goal.

{4.18} (v) **Promptly Revoke a Compromised Key.** If a consumer's private key is compromised, that consumer, upon learning of the compromise, must promptly take steps to revoke the corresponding certificate.

(d) **Merchants.** {4.19} We suggest that the following behavior by merchants constitutes reasonable behavior:

{4.20} (i) **Require the Right Certificate.** All parties would be best served by permitting the establishment of "classes" or types of certificates that represent different factual assertions by consumers and levels of assurances by CAs. Assuming that CAs establish classes of certificates that make different factual assertions, the merchant should be responsible for requiring the appropriate class of certificate. For example, if the CA offers a class of certificates which contain information which the CA expressly states contains only unverified information provided by the consumer, it is unreasonable for the merchant to expect the CA to warrant the accuracy of the information contained in the certificate. In contrast, if the CA offers a class of certificates which expressly states that the CA has used substantial efforts to verify identifying information of the consumer, it is generally reasonable for the merchant to expect the information contained in this certificate to be true. So long as merchants are required to select a class of certificates suitable for their requirements, presumably an efficient market will force CAs to offer classes of certificates which meet these needs.

{4.21} It is possible that limited-purpose or specialized-purpose certificates will be issued by CAs. In these cases, it would be unreasonable for merchants to use the

certificate for identity purposes if such purposes are contrary to the specified purpose of the certificate. We note that many physical space certificates, such as driver's licenses and social security cards, are currently used for identity despite the fact that such certificates were not designed for that use.

{4.22} (ii) **Verify Certificates.** Similarly, it is unreasonable for the merchant to rely upon a certificate that by its terms has expired or to fail to verify the signature of the CA (and its CAs) unless the CA is self-certified. It is also unreasonable for a merchant to rely on a certificate that was designated for a different purpose (such as a certificate issued by a company for internal access control purposes).

{4.23} (iii) **Check the Applicable CRL.** Although there are schemes being implemented where no CRL exists as part of the infrastructure, if a CRL exists, certificates that have been revoked will be noted in a CRL. In such a case, merchants should bear the risk for failing to check the applicable CRL.

{4.24} We note that CAs are contemplating offering access to CRLs on a fee-for-service basis. Such an event would significantly alter the relationship between the parties by permitting CAs to impose contract terms on merchants and by providing financial disincentives for a merchant to check a CRL. We have not attempted to address this scenario.

{4.25} (iv) **Act on Other Information.** If the merchant knows or should have known that the information contained in a certificate is incorrect, then it is unreasonable for the merchant to rely on the certificate. It is expected that reasonable due diligence efforts required of the merchant will increase with the size of the transaction and the scope of parties' "out-of-band" (i.e., non-Internet) relationship.

(e) **CAs.** {4.26} We suggest that the following behavior by CAs constitutes reasonable behavior:

{4.27} (i) **Initial Consumer Authentication.** There are many means for CAs to initially verify the identity of consumers. We believe that there are no minimum standards that should apply; rather, the CA should specify what methods it undertook to authenticate consumers and the CA will be acting unreasonably if it fails to properly perform those steps. At the most basic level, a CA should be able to provide a certificate based only on information provided by the consumer, so long as the CA clearly expresses that the information contained in the certificate was not verified by a third party. Alternatively, if the CA undertakes to authenticate identity using a rigorous system of checks, its failure to implement those checks properly will be unreasonable. (This is not to say that the CA should become the absolute guarantor of identity, but it should perform the duties it sets out for itself.) As described above, we expect that the market will be efficient enough that merchant demand will force the CAs to undertake meaningful obligations to authenticate consumers.

{4.28} (ii) **Trustworthy Systems/Key Management.** CAs will handle much of their operations automatically and will be exposed to any number of computer-based risks, both internally and from outside threats. The losses attributable to system failures could prove to be diffuse and large. The problem could be particularly acute if the CA's private key was determined by third parties. A party who discovers the private key of a CA could produce an unlimited number of ostensibly valid but forged certificates. Moreover, if a CA's private key was compromised and the corresponding public key revoked, all certificates issued by that CA would be invalid. All of the consumers who utilized that CA would be forced to obtain new certificates.

{4.29} Depending on the CAs' contractual relationships with consumers, it is possible that CAs will not be forced to bear the costs of system failures -- particularly if the individual costs borne by each consumer are so small that they are overshadowed by the transaction costs of seeking recourse against the CA.

{4.30} However, despite the importance of ensuring proper system operation, it is not fair to expect perfect error-free operation. Given the dynamic evolution of the underlying technology, it does not make sense to codify specific minimum technology standards. Therefore, CAs should use reasonable efforts to make their systems trustworthy. In this context, the standards for reasonable efforts and trustworthiness will increase over time as technology improves.

{4.31} The problem of key management is particularly vexing and it is imperative that CAs take every possible precaution when generating, storing, and using their private encryption key. Particularly in light of the dynamic technological environment in which keys are generated and managed, we cannot currently articulate specific behaviors that would constitute reasonable precautions in this regard. Additional study should be done to suggest what efforts by CAs would be reasonable to keep their private keys private and what duties CAs have if they discover their private key has been determined by third parties or is no longer private.

{4.32} It may be appropriate for an industry standards setting body to form which can dynamically assess technological improvements and establish standards for reasonable deployment of technology to increase trustworthiness. If the industry does not develop such standards, it is likely that government regulation will be implemented to develop a licensing scheme.

{4.33} At a minimum, we expect that CAs will freely disclose the steps they are taking to make their systems trustworthy. Systems often achieve trustworthiness only by being subjected to public scrutiny.

{4.34} (iii) **Administrative Duties.** It is beyond the scope of this Report to deal with issues such as employee hiring and management, record keeping, bonding and insurance, and other ministerial functions. Although such issues could be critical to the successful operation of a PKI, we suggest that additional study should be done on these topics.

{4.35} (iv) **Certificate Revocation/Suspension.** CAs will be expected to revoke certificates promptly upon notification from consumers. Revocation typically occurs by maintaining a CRL. This CRL must be made available in such a way that merchants can check the CRL easily prior to accepting a certificate.

{4.36} It may not be fair for CAs to have obligations to independently verify certified facts on a continuing basis. While CAs should have a duty of inquiry if they receive information from a third party suggesting that a certified fact is incorrect, no independent efforts should be required unless the CA offers to do so as part of the terms of the certificate or in its agreement with consumers.

{4.37} Because of the relative harm that can be caused by issuing a false certificate compared with failing to issue a certificate that should otherwise have been issued, it seems appropriate to give incentives to CAs to fail to issue certificates if there is any doubt. Therefore, we suggest that the CA should be exonerated under applicable principles for any losses that occur because the CA elected not to issue certificates if the CA has any good faith belief that the certificate should not issue (there could be a breach of contract for this failure depending on the agreement between the parties). However, it seems prudent to require the CA to promptly notify the consumer if the CA does not feel it is in a position to issue certificates so that the consumer may resolve any confusion.

{4.38} (v) **Publish a Certification Practices Statement.** CAs should make available, in an easily accessible manner, a certification practices statement or similar document that clearly and succinctly states the practices which a CA employs in issuing certificates. A CA should follow the practices enumerated in its certification practices statement.

{4.39} (vi) **Make Its Certificate Available.** A CA must make its own certificate regarding its public key available to parties who wish to verify the certificates of consumers.

{4.40} (vii) **Financial Responsibility.** The question of how to ensure that a CA is able to bear the loss associated with its potential liabilities is beyond the scope of this analysis. We note, however, that a CA that fails to comply with its duties conceivably imposes significant losses on a large number of innocent parties. Ensuring that these parties could be compensated for their losses is an important public policy concern. Likewise, a CA that abruptly terminates its business could impose significant costs on its consumers and others. As a practical matter, it may be difficult to impose enforceable duties on an entity that is bankrupt or insolvent.

{4.41} It is conceivable that, with adequate disclosure, the market will properly assess the risks associated with doing business with CAs that lack capacity to bear losses attributable to them. As a policy matter, this approach will still require mechanisms to ensure accurate disclosure.

(f) **Third Party Suppliers.**

{4.42} Often overlooked players in the CA industry are third party providers of ancillary services, such as hardware, software, Internet connectivity, timestamping and authentication vendors. We suggest there should be consideration of the duties of CAs to exercise reasonable care in selecting suppliers. It may be that in some cases CAs should share liability with the third party providers, even though the CA itself did not specifically commit the action causing loss. Given that most third party suppliers will be in direct contractual privity with the CA, CAs should require meaningful covenants, warranties and indemnities from the suppliers in order to cover the situations where the CA is deemed responsible due to the third party's failed performance.

{4.43} Where the situation was clearly outside of the CA's control, it may be appropriate to allocate loss to these third party suppliers. This loss may be governed by existing legal principles, such as those generally described in Appendix 3. However, given the wide range of possible suppliers, it is not possible to summarize rules that would generally apply to all of them.

{4.44} Notaries or other authentication verification providers pose particularly difficult issues. A CA might disclose in its certification practices statement that one of its authentication methods is to rely on a written application from a subscriber that has been certified by a notary. If a notary certifies a false application, and the CA consequently issues a fraudulent certificate, should the notary or the CA bear any resulting loss? Certainly the fraudulent applicant should be primarily liable, but we suggest that, in this situation, merchants should also be able to recover from the CA, with the CA having a corresponding cause of action against the notary. It may be unfair to place the burden on a merchant to recover against a notary, who may be geographically distant from the merchant and potentially not subject to the jurisdiction of the merchant's local courts. Moreover, this allocation of risk will create incentives for CAs to exercise care when entering into relationships with notaries or other local authentication agents and potentially impose more rigorous authentication procedures than are typically required of notaries.

{4.45} Other issues are raised by third party service providers who supply the hardware and software necessary to a PKI. Implementing the cryptographic algorithms and techniques that underlie digital signatures is not an easy task. As discussed above, providers of hardware and software should provide users of their systems with clear, concise instructions on how to their system secure which, if followed precisely, would permit consumers to achieve the promised level of security.

{4.46} Some legal systems are spelling out specific rules that apply to these third party suppliers. For the more critical suppliers, this may be appropriate.

(g) **Limitations of Liability When All Parties Act Reasonably.**

{4.47} Under the standards suggested above, it is entirely possible that all parties will act reasonably and yet a loss will be suffered. Allocating this loss could prove to be essential to the widespread use of digital signatures and for establishing a robust role for certification authorities to support consumer transactions.

{4.48} In some ways, the Electronic Funds Transfer Act (discussed in Appendix 3) raises an interesting analogy. Credit card holders can behave entirely reasonably and yet their credit card number can be expropriated, resulting in losses. To limit credit card holder liability, the EFTA specifies that in most cases a holder will not be liable for more than $50 in losses prior to the holder reporting the expropriation of the number and for no losses incurred after reporting the expropriation. If a similar structure were made applicable to the digital signature context, we believe that consumers would be significantly more willing to adopt their use. Therefore, by analogy to EFTA and in accordance with our touchstone principle that a party that behaves reasonably should bear no risk of loss, we suggest that consumer liability be limited to a small dollar number, or to zero, if the consumer has behaved reasonably as outlined above.

{4.49} In situations where the CA has behaved reasonably, we have suggested a number of reasons why CAs should not be liable for losses. Stepping back from the specifics, there is no doubt that the specter of liability for breach of contract and for negligence significantly deter the entry of CAs into the market. At this point there are no efficient markets for insurance to spread risk throughout the industry -- meaning that CAs face meaningful unquantifiable risks of large losses. Placing risk of loss on CAs when CAs act reasonably would likely make those risks untenable, posing a grave threat to the development of the CA industry. However, as insurance markets and pricing models become more refined, it may be appropriate to revisit CAs liability when all parties act reasonably, as they may ultimately prove the best party to spread the costs among the relevant players.

{4.50} Having suggested that both consumers and CAs should have limited liability when they act reasonably, the risk of loss under this structure would fall on merchants. This would give merchants incentives to act "more than reasonably" if the underlying transaction is important to them. Since only merchants know how important the transaction is to them, placing the burden on merchants encourages them to scale their actions to their risk tolerance. In the consumer transaction context, merchants are also the ones being paid in the transaction by the consumer -- giving the merchant the opportunity to incorporate the business risk into their pricing models. By way of example, currently mail order and telephone-based merchants typically bear the risk of loss, as they are typically the party who can best allocate the net of loss among their customers.

{4.51} Regardless of loss allocation mechanisms, the most important step towards fostering the growth of an industry will be the establishment of clear and predictable rules for the parties. While we expect that consumers should and will always have

limited liability when they act reasonably, we expect that CAs and merchants will find a way to establish suitable pricing mechanisms under a regulatory and legal framework -- if the rules are predictable and clear. In light of the transborder discussions noted below, this is not a trivial problem.

(h) **Limiting Consumer Liability for "Unreasonable" Behavior.**

{4.52} In analyzing risk allocations between the parties, by way of analogy we note that EFTA provides consumers with liability limits even if consumers fail to act reasonably. EFTA's liability limitations apply both where the consumer acts reasonably and where the consumer does not act reasonably, although in the latter case the consumer will have to bear more risk.

{4.53} We believe that consumer protection is an integral step in encouraging the use of digital signatures. We have suggested that, as a general rule, participants in a PKI should bear liability when they act unreasonably and should be free of liability when they act reasonably. However, consider the situation where a consumer fails to adequately protect his or her private key, resulting in fraud. If our touchstone principle -- that parties acting unreasonably bear the resultant loss -- applies, the consumer would bear potentially unlimited losses resulting from that fraud. We are concerned that unlimited losses could be a major disincentive for consumers to participate in the system. Thus, we suggest that consideration be given to limiting consumer liability even in the situation where a consumer does not act reasonably.

{4.54} We do not suggest that EFTA should be reimplemented verbatim in a PKI. The consequences when a consumer does not act reasonably in the digital signatures context are arguably more significant than the consequences of consumer negligence in the credit card model. The success of a PKI depends upon the security of private keys. While we are not in a position to suggest specific dollar numbers associated with dollar caps, three principles are worth considering. First, like the EFTA structure, it may be appropriate to have tiered levels of dollar caps, depending on the severity of the consumer's actions. Second, the dollar caps should be high enough to encourage the consumer to act reasonably but low enough to avoid disincentivizing consumers from participating in the PKI. Finally, there should be no dollar cap for a consumer's intentional fraud.

{4.55} If consumer and CA liability is limited, merchants will face potentially unreimbursed losses even when they act reasonably. Presumably merchants would take this risk into account in their risk-benefit calculus when choosing to rely on a digital signature. In a large dollar transaction, the merchant may choose to obtain out-of-band assurances. In a small dollar transaction, the merchant may simply choose to accept this risk of loss.

{4.56} Insurance may eventually address the problem of unreimbursed losses. A private insurance market will not develop immediately, however, because there is not enough data to develop a pattern of loss experience and the existing legal framework is too

unsettled to allow these losses to be predicted. In the meantime, the suggestions described above could provide parties participating in a PKI with a reasonable degree of certainty, enabling them to make rational economic choices but without abandoning the policy of consumer protection.

(i) **Implied Warranties.** {4.57} This section discusses the existing framework of implied warranties and what the framework should be. Readers are referred to Appendix 3 for additional background information.

{4.58} (i) **To Consumers.** CAs deliver certificates to consumers. Assuming the certificates are merely memorialization of services performed, they would be subject to an implied warranty of workmanship -- which, although a contract-based remedy, permits the consumer to sue for the CA's negligence. While CAs should be able to disclaim implied warranties in their contracts with consumers, prospective contractual disclaimers of negligence are difficult to institute and therefore the implied warranty of workmanship may persist. Therefore, we do not believe any "new" implied warranties are needed in the consumer/CA relationship.

{4.59} (ii) **To Merchants.** We have asserted that no contractual relationship should be formed between CAs and merchants, in which case no implied warranties would be formed. However, as we have discussed, the tort of negligent misrepresentation appears to be an efficient mechanism to allocate losses between CAs and merchants. We would expect that, like any other situation, it will be difficult (and perhaps impossible in the absence of a contract) for a CA to prospectively disclaim this tort in advance.

(j) **CAs' Limitations of Liability for Breach of Contract/Negligence.**

{4.60} CAs may want to establish classes of certificates that, based on the different levels of effort exerted by the CA and differential pricing, have different dollar caps on liability. The rationale is entirely understandable -- a cheap certificate which contains unverified information provided by a consumer is not comparable with an expensive, extensively-verified certificate. With respect to consumers, while it makes sense for CAs to limit their liability for authorized certificates, it is unreasonable for a CA to unduly limit its liability for issuing *unauthorized* certificates. With respect to merchants, there is no contract formed between the merchant and the CA, so there is no basis for the CA to assert that such dollar caps should act as a bar on merchants' recovery for their damages under existing tort principles. However, in some circumstances, we could see how a court might find that stated dollar limits influenced whether or not reliance on the certificate was justified or reasonable.

{4.61} Almost all CAs attempt to disclaim liability for consequential and similar types of damages. With respect to consumers, subject to existing limits on the ability to disclaim these liabilities, this should be a matter of contract. With respect to merchants, if there is no contract formed between the merchant and the CA, there is no contract-based principles for the CA to assert limits to liability (there may still be limitations on tort liability, such as limitations on the awarding of consequential damages). If a contract is

formed with merchants, then principles of unconscionability should put strict limits on the powers of CAs to unreasonably limit their liability -- particularly for negligence.

{4.62} Except in test or demonstration situations, it is usually unreasonable for a CA to disclaim all liability for direct damages or to establish a dollar cap so low as to effectively deny plaintiffs all meaningful monetary damage remedies.

(k) **Transborder Issues.** {4.63} It is beyond the scope of this paper to comprehensively deal with the difficult issues of jurisdiction, venue, choice of law and conflicts of laws. It is certain that many consumer/CA/merchant relationships will be international in scope. These transborder relationships implicate complicated and arcane principles of law.

{4.64} One certain result is that the putative contract relationship between CAs and consumers will be undermined by the possibility that the contract will not be in the consumer's native language. The cost of translating a consumer/CA contract into foreign languages is significant; localizing these contracts to reflect general local rules regarding contract formation adds even more. As discussed in Appendix 3, there are many other legal systems that prohibit the contractual assent to certain provisions. As lawsuits derived from these relationships mount throughout the world, it is likely that the various entities will find themselves subject to an inconsistent patchwork quilt of rules. This problem will be exacerbated by the likelihood that the CAs will be dragged into a multiple of far-flung jurisdictions to defend actions.

{4.65} We believe a regulatory framework that fosters predictability will substantially minimize or eliminate this consequence. PKI and digital signatures have the potential to become an essential tool in electronic commerce. All of the respective players should invest in resolving issues raised by this Report by developing standards which can win acceptance in the marketplace while encouraging regulators that the needs of consumers are being protected.

## 5. Next Steps.

{5.1} This Report was undertaken as a "pilot project" of the Internet Law & Policy Forum; by its own terms of reference, the Report was limited in scope and not intended as a comprehensive discussion or treatment with respect to the role of certification authorities in open market consumer transactions under all legal systems. At the same time, in addition to a more comprehensive review of those systems, this Report has identified specific areas for action, through the venue of the Forum or other processes, which are recommended for consideration:

{5.2} (a) Development of a clear definition of the distinction in legal analysis required between open systems and closed systems, where the parties are all putatively bound to each other by contract, including analysis of how loss allocations should be made in a closed system.

{5.3} (b) Representative analysis of other legal systems, particularly those of emerging nations, regarding similar topics of law that might affect crossborder consumer transactions.

{5.4} (c) Completion of the analysis of the extent to which existing CAs are complying with the legal systems being enacted.

{5.5} (d) Analysis of the interplay between overlapping legal doctrines in a single jurisdiction.

{5.6} (e) Standards for CAs' treatment of confidential or private consumer information.

{5.7} (f) Extension of the analysis to other uses of certificates, such as in commercial transactions between merchants or as an access control device.

{5.8} (g) Analysis of whether existing legislative schemes resolve the legal ambiguities existing under current law.

{5.9} (h) Analysis of how loss allocations should be made in the situations where the merchant delivers a certificate to the consumer.

{5.10} (i) Development of standards about what qualifies as a trustworthy system as used by CAs, particularly to address key management by CAs and the CA's duties if it discovers its private key has been determined by third parties.

{5.11} (j) Development of standards for administrative duties of CAs, such as employee hiring and management, recordkeeping, bonding and insurance and other ministerial functions.

{5.12} (k) Analysis of liabilities of third party providers to CAs (particularly notaries, timestampers, PKI hardware and software providers and other integral players in the process).

{5.13} (l) Analysis of the effect of payment companies on the loss allocations between CAs, merchants and consumers.

{5.14} (m) Allocations of loss when more than one party in a PKI acts unreasonably.

{5.15} (n) Effect of charges for accessing CRLs on the rights and responsibilities of the parties.

{5.16} (o) Ability of third party hardware and software providers to disclaim liability or warranties when providing resources used in a PKI.

{5.17} (p) Establishment of appropriate dollar values and rules to cap consumer liability for acting unreasonably.

## Exhibit A

Certification Authorities and Related Parties Invited to Participate:

CertCo

CommerceNet

COST Computer Security Technologies

DBS/Denmark

DFN-CERT and DFN-PCA, Universität Hamburg, FB Informatik

Entegrity Solutions

GTE

Harbinger Corporation

IBM

Institut Jozef Stefan

MarketNet

Nortel Secure Networks

PGP

Signet Systems

SPYRUS

Sun Microsystems

Thawte Consulting

UNINETT

US Postal Service

VeriSign, Inc.

Parties that Provided Comments to this Report:

CertCo

COST Computer Security Technologies

GTE

IBM

Institut Jozef Stefan

MarketNet

Nortel Secure Networks

Signet Systems

SPYRUS

US Postal Service

## Appendix 1

## Scope And Assumptions

The issues implicated by PKI are extensive and complex. We have not attempted to address all of these issues in this Report, although many of them warrant additional analysis. The following list represents some of the major assumptions that we have made:

**(a)** We have not attempted to compare the desirability of centralized trust systems for PKI with other models for authenticating trading partners or improving the security of the Internet. Among these competing approaches to authentication are challenge-response identification; the "web-of-trust" model (found most prominently among users of Pretty Good Privacy); passcards and other hardware devices; biometric systems such as those developed by PenOp and Mytec Technologies; and Electronic Data Interchange over a value added network. There are strengths and weaknesses to each of these competing approaches that are currently being debated elsewhere. Conceivably some of these alternative models for authentication may be partially incorporated into a trusted third party (CA-oriented) PKI.

**(b)** Throughout this Report, we have focused only on consumer transactions utilizing the services of commercial CAs. There is no intent to suggest that consumer transactions are the most important or even best application for digital signatures or that commercial CAs should preclude government CAs. However, in this pilot project, we have not attempted to address all possible scenarios.

**(c)** We note that digital signatures and certificates are currently being deployed in a number of other interesting applications. For example, a number of vendors are using digital signatures and CA schemes as an access control device -- either as a device for metering access to intellectual property available on the Internet, or in the "Intranet" context, where certificates are used to regulate which employees are entitled to access proprietary resources. Another increasingly common use is authentication of the source and functionality of software distributed over the Internet. The issues involved in this context could be materially different than those found in the consumer commercial context, and we have not attempted to address them here.

**(d)** Similarly, we note that some legislatures are authorizing the limited use of digital signatures for specified government purposes, such as the filing of court documents, tax returns or architectural design plans or for signing medical records. We do not attempt to address the issues regarding the use of digital signatures for these specified, limited purposes.

**(e)** Throughout this Report we address certificates designed to confirm identity. In fact, certificates are capable of providing information about consumer attributes beyond simply that consumer's "identity" -- perhaps even on an anonymous basis. For example, a certificate could certify that a person was over 21 and therefore permitted to access

materials restricted to people over that age without disclosing the person's name. Although certificates are likely to find substantial uses in these ways, we have not attempted to address these issues.

**(f)** We have assumed that cryptographic devices sufficient to generate difficult-to-determine key pairs will be widely available across international borders. Currently the distribution of these devices is controlled by a number of governments, and such regulation is the subject of substantial debate. Further, we do not address any issues related to the escrowing of keys.

**(g)** Generally, we have assumed that consumers (and not other parties) will make the substantive decision about which CAs they will establish relationships with. However, it is possible that merchants or the payment systems (such as the credit card associations) will drive this decision by dictating which CAs' certificates they will accept, effectively forcing consumers to procure certificates from these CAs. Because it fundamentally alters the freedom of contract principles we have tried to support in this Report, lack of consumer choice over what CA is used raises a host of new consumer protection and other issues that we have not attempted to address here.

**(h)** We have assumed that CAs, if given the opportunity, would enter into contracts with merchants rather than rely on the default non-contract rules (i.e., tort principles under common law or statutory rules). We make this assumption because of the incentives CAs will have to disclaim warranties to merchants, to exclude consequential and other party-specific damages, and to impose dollar caps on liabilities. It is possible that CAs would not want to enter into contracts with merchants if these objectives cannot be met (for example, if the waivers or exclusions are unconscionable or fail of their essential purpose). However, we believe that CAs hope and expect that their relationships with merchants will be governed by contract or possibly by statute.

**(i)** We do not deal with issues related to agency law and actual or apparent authority. Certificates could at some point indicate a party's authority to act (see paragraph (e) above), but we do not address that here.

**(j)** Ensuring the long-term validity of a contract signed with a digital signature may require the services of a third party commonly referred to as a timestamper, who can specify when the message containing the digital signature was sent. We have not attempted to address issues related to timestamping.

**(k)** "Caching" occurs when remote information is duplicated and stored locally. It is likely that information being transmitted through the PKI will be cached both at the client level and at the proxy server level (internally in an organization or at their service provider's servers). This issue is mostly likely to be seen in the case of Certificate Revocation Lists, which merchants may cache (much like merchants used to keep hard copy printouts of revoked credit cards next to cash registers for real-time verification by cashiers). Caching creates the possibility that parties are knowingly or unknowingly relying on outdated information, and will also potentially implicate difficult issues under

copyright law or other intellectual property rules applicable to databases. We have not attempted to address these issues, although there may be technological methods that minimize this problem.

**(l)** CAs will acquire significant private information about its consumers. Not only will consumers directly submit personal information to the CA, but the consumer's conduct will leave a "digital trail" of information that, analyzed properly, would give insights into the consumer's affairs. We do not address the laws (or desirability of laws) relating to keeping this information confidential. We note, however, that the CA's disclosure of consumer information may be governed by the E.U.'s Directive on Data Privacy Protection (95/46/EC), among other rules.

**(m)** We have not addressed the bandwidth, computer and other costs associated with the use of digital signatures. We assume that senders and recipients of digital signatures, certificates or other electronic messages do not bear any marginal costs attributable to sending or receiving these files. In practice, per-byte or per-message pricing could become standard, making the marginal costs of using or verifying digital signatures greater than zero. In addition, the computational power required to generate and process digital signatures is significant and will continue to increase as the length of public and private keys increases. Significant marginal costs attributable to computer processing or bandwidth are likely to alter the way that senders and recipients perceive and use digital signatures in ways we have not attempted to address.

**(n)** We do not address evidentiary issues associated with digital signatures, such as the admissibility of digitally-signed documents, the appropriate evidentiary weight to be accorded such documents, and legal presumptions arising from the use of digital signatures. These issues can include whether a document signed with a digital signature satisfies the "writing" requirement under applicable statutes of frauds, whether an electronic record signed with a digital signature satisfies the best evidence rule, and so on. Though seemingly procedural, these issues can raise important public policy concerns. For example, some enacted U.S. state legislation creates a presumption that, under certain circumstances, the person who owns a particular key pair used to sign a document is the person who did in fact sign the document. Holding an individual presumptively bound by obligations entered into under their digital signature could be inequitable if the individual is the victim of the fraudulent use of such a signature.

These issues could also be significant in non-US jurisdictions that have extensive statute of frauds. For example, Germany has a set of legal rules ("Schriftform") similar to the statute of frauds in other jurisdictions. There are thousands of German statutory law provisions that require certain declarations to be given in written form; in such cases, "written form" is defined by statute to mean a written signature made by pen on paper. Important examples of such provisions in German law are consent to the use of personal data under the Data Protection Law, covenants and transfers with respect to real estate, and the transfer of shares in a limited liability company. Presumably digitally-signed documents will not qualify as being in written form under these laws.

**(o)** Generally, this Report does not address "cooling off" laws designed to give consumers the opportunity to reject transactions for some period of time following the execution of the contract.

**(p)** There are multiple conventions for the technical specifications of certificates. This Report only addresses Standard X.509 of the International Telecommunications Union, although the analysis may apply to other certificate conventions.

**(q)** Some visions of a PKI require that each participant obtain, register and use a unique "distinguished name." These naming conventions may implicate privacy concerns, agency law and even trademark law. We do not address issues related to naming in this Report.

**(r)** In order to analyze the CA's digital signature attached to a certificate, the party receiving the certificate must obtain the CA's public key. Just as there are issues regarding whether a consumer's public key belongs to the person who claims it, there could be issues about whether the CA's public key belongs to the CA who claims it. To resolve this, some visions of the PKI assume that a CA will have the CA's certificates signed by another CA whom the public can trust that its public key belongs to this CA. This Report assumes that, if a chain of certificates is developed to allow CAs to include certificates regarding the CA's signature, the "root certificate" -- that is, the certificate of the public key of the CA at the top of this chain -- can be trusted, whether it is issued by a government or private entity.

**(s)** We do not address the duties, if any, of higher-level CAs for the duties of CAs whose public keys are certified by the higher-level CA.

**(t)** The mechanisms by which certificates are delivered to potential relying parties can vary. This Report assumes that a consumer who is identified in a certificate will present that certificate directly to the merchant who intends to rely upon it. The Report does not analyze the situation where certificates are stored in a database or directory maintained by a certification authority or other third party and accessed by merchants on an as-needed basis.

## Appendix 2

## Open Systems vs. Closed Systems

{AP2.1} This Report focuses on an "open system" or "open loop" model of a PKI. The open system model envisions that consumers will obtain from an independent third-party CA a single certificate which certifies that consumer's identity. Consumers will then use that certificate to facilitate transactions with potentially numerous merchants.

{AP2.2} As discussed in the Report, the open system scenario implicates legal uncertainty and risk. This problem has attracted the attention of numerous state and national legislatures, and has been scrutinized by several private-sector legal groups. Nonetheless, the problem is far from being solved, and the open system model has not yet been implemented in the marketplace in any meaningful fashion.

{AP2.3} "Closed system" or "closed loop" models offer an alternative way to implement a PKI. Closed systems may fall into two categories: systems where a payment mechanism serves to "close the loop," and systems where certificates are used within a bounded context. In a closed system, a contract or a series of contracts identify and define the rights and responsibilities of *all* parties to a particular transaction.

{AP2.4} The existing credit card system provides a good example of how a payment system can "close the loop." A consumer can only use a credit card to purchase a good or service at a merchant who is authorized to accept such a payment device. The consumer's right to use the credit card for payment is based upon a contract between the consumer and the financial institution that issued him the credit card. The financial institution's right to issue the credit card is based upon a contract between the financial institution and a payment card company (*e.g.*, Visa, MasterCard, JCB or Europay). Similarly, the merchant has a contractual relationship with another financial institution, which in turn has a contractual relationship with the same payment card company. Therefore, there is a closed loop of contracts that define each party's rights and responsibilities with respect to the transaction in question.

{AP2.5} We describe this process because, by analogy, we think this process potentially could alleviate several or all of the legal problems of an open system. Particularly in the context of consumer transactions, it is very likely that merchants will have contracts with payment companies like credit card systems. Therefore, the CAs will have the opportunity to enter into agreements with payment companies that require payment companies either to pass CA-specified terms through to merchants or to share the risk with CAs. Solutions sponsored by payment companies (like SET) may help achieve the implementation of a closed system. While such a closed system would raise its own set of challenging legal issues -- such as determining the appropriate scope of existing payment systems legislation (*e.g.*, the Electronic Funds Transfer Act) -- it would avoid many of the difficult risk allocation questions inherent in an open system. Future analysis should address how payment mechanisms would affect this Report's analysis.

{AP2.6} A second type of closed system exists when certificates are issued and used only within a bounded universe. For example, the proprietor of an online "mall" might issue certificates to potential customers and to merchants. The proprietor, acting as a CA, has the opportunity to enter into contractual relationships both with consumers and with the merchants who will rely of the certificates.

{AP2.7} Similarly, a merchant might issue certificates directly to its customers. The owner of an online magazine, for example, might mail diskettes containing certificates directly to subscribers of the paper version of the same magazine. Such certificates could be installed the subscriber's web browser and used to access the online magazine, and perhaps to order related merchandise. The magazine vendor would be well positioned to determine whether such certificates would be sufficiently trustworthy for the purposes for which they were being used. Again, such a scenario does not implicate the difficult risk allocation questions associated with the open system model.

{AP2.8} We believe that there are pluses and minuses to both the open system and closed system models. Certainly, there is no intent to suggest that, because this Report focuses on open system models, open system models are superior to closed system models. Closed system models do have one significant advantage over open system models -- the legal issues related to transactions performed within closed systems are fewer and less ambiguous than in the open system environment, because closed system models raise few novel or esoteric issues under contract law. However, there are situations where the contracts governing the parties will fail, in which event the legal issues raised by the parties' relationships will be governed by the default rules, which are not well-understood but are addressed in this Report.

## Appendix 3

## Existing Legal Systems

{AP3.1} This Appendix analyzes selected legal systems and highlights how their existing rules and principles might affect the CA service industry. The analysis is complicated by several factors. First, due to the global nature of the Internet, CAs may operate on a global scale, and thus potentially be subject to the varying laws of many different jurisdictions. Second, even within a particular jurisdiction, legal systems may overlap. For example, a transaction between a merchant and a consumer using a digital signature may simultaneously be subject to contract law and related consumer protection legislation; tort law; legislation addressing payment issues; and to specific "digital signature legislation." Nonetheless, we believe a survey of a selected number of existing legal systems serves to illustrate the general legal context in which the CA service industry is developing. With this understanding, we can better understand how the existing legal systems will provide incentives and disincentives to using digital signatures in consumer transactions.

{AP3.2} This Appendix first surveys U.S. contract law, discussing the potential application of the Uniform Commercial Code and the common law of contracts, then provides an overview of contract law in certain international settings. This Appendix then addresses certain U.S. and E.U. tort law principles and concludes by addressing various "digital signature" laws and other laws relating to electronic commerce and electronic funds transfers.

{AP3.3} This Appendix does not attempt to cover all of the existing legal systems which are relevant to users of digital signatures or providers of CA services. Such analysis should be performed in subsequent studies. It may also be worthwhile to analyze more carefully the interaction between competing legal doctrines within a single jurisdiction.

{AP3.4} One of the most significant jurisdictions outside the US which has begun to concern itself with the legal implications of digital signatures is Germany, which is poised to enact one of the first digital signature laws outside the US. While in most non-US jurisdictions the lack of precedent, statutory law and legal commentary regarding digital signatures hampers discussion of their legal consequences, such material exists in abundance in Germany. Furthermore, Germany's position in this area is likely to be quite influential among other jurisdictions outside the US, making it useful as a point of comparison. Other jurisdictions which are actively analyzing digital signature issues -- and which could be the subject of subsequent study -- include Australia, Malaysia and Singapore.

{AP3.5} This Appendix discusses general legal principles and is not intended to be a comprehensive treatise of applicable law in the jurisdictions addressed. Exceptions to almost every rule discussed here can be found, but this analysis sets forth the basic rules that we believe would be applied by a decision-maker in the relevant jurisdiction.

(a) A Statement of the Legal Problem: Open vs. Closed Systems.

{AP3.6} As described previously, the use of digital signatures is seemingly straightforward. At a transaction's most basic level, the consumer and merchant independently establish relationships with a CA, each procures a certificate, the parties swap and verify certificates and the transaction is consummated. In practice, this process has the potential to create enormous risk for all the parties involved.

{AP3.7} This Report does not deal with the many issues related to consumers relying on the certificates of merchants; such an analysis is properly the study of a subsequent report. It is expected that many -- but not all -- of the issues addressed in this paper will be equally applicable to the situations where consumers are the relying third parties.

{AP3.8} As described in Appendix 2, this Report addresses "open" systems, where no contracts between the parties will exist except possibly in the process of obtaining or delivering certificates. In an open system, the relationship between the CA and the consumer, although important and multi-faceted, raises only a few complicated legal issues. Usually the CA will claim consumers are bound by contract to the CA's standard terms (usually contained in its certification practices statement). If something goes wrong, the contract would generally be the first source of operating rules to govern the problem. In addition to the contract, however, there may be tort principles or statutory guidelines that establish the default rules. There are also some general rules that may limit the provisions that can be contained in the contract, but again it is relatively straightforward to identify these rules.

{AP3.9} In an open system, the relationship between the CA and the merchant, however, raises some very complicated legal principles. To get a perspective on the complexity of the issues, the diagram in Figure 1 provides a road map for the subsequent analysis.

{AP3.10} Stated simply, the issue is whether, in an open system, the CA can form a contract with a merchant based on a relatively attenuated connection between the parties? Further, can a merchant benefit from any favorable provisions agreed to between the CA and the consumer? Finally, does the delivery of the certificate to the merchant give the merchant any rights to sue the person who placed the certificate into the stream of commerce (i.e., the CA)? These issues all are very difficult to resolve in analogous physical space situations, and this Appendix provides some thoughts on how some of the analysis might apply in the PKI context.

(b) Contract Law in the United States.

{AP3.11} The United States is primarily a "common law" legal system. Common law is a system of jurisprudence, originated in England and transplanted to the United States, based on judicial precedent and not legislatively-adopted statutory rules. Generally, legislative statutes supersede the common law, although some statutes are merely codifications of the common law. This section first addresses U.S. law applicable to the

sale of goods, and then addresses U.S. law applicable to contracts for services. Both are relevant to an analysis of contract aspects of the role of CAs in consumer transactions.

{AP3.12} (i) The Uniform Commercial Code. The Uniform Commercial Code ("UCC") is a set of standard rules in the United States prepared by the National Conference of Commissioners on Uniform State Laws and the American Law Institute. Each state in the United States is free to adopt the UCC rules as part of their statutory framework; in practice, most states adopt most of the proposed rules. The UCC is the comprehensive body of law in the United States governing the sale of "goods" both between merchants and consumers and among merchants. The UCC has proven very influential both in the United States and internationally, with many jurisdictions adopting rules based on or similar to the UCC. In addition, in the United States many courts look to the UCC as persuasive authority, even when it does not specifically apply.

(1) Goods vs. Services.

{AP3.13} To identify the applicable body of contract law, it must be determined whether the certificate issued by a CA to a subscriber, for further delivery to a merchant, is a "good," a "service" (or the memorial of services), or a mixture of a good and a service.

{AP3.14} If the certificate is a "good," then Article 2 of the UCC applies and a number of default rules will apply (as described later in this section). Importantly, Article 2 will impose a number of implied warranties on the CA's activities and will impose procedural hurdles on limiting disclaimers of those warranties. On the other hand, if the CA is providing a "service," Article 2 does not apply.

{AP3.15} Section 2-105(1) of the UCC defines "goods" as "all things . . . which are moveable at the time of identification to the contract for sale . . . ." In the sense that certificates are moveable (both in electronic form and if printed out), they could be deemed to fit within the definition of goods.

{AP3.16} However, in some ways, the certificate merely is the tangible memorial of the services performed by the CA, which may include processing of the consumer's information, verification of the factual statements made by the consumer and maintenance of a Certificate Revocation List ("CRL"). In this regard, the certificate is not the critical element to the transaction; rather, the CA is selling its services, and the certificate is evidence that such services were performed.

{AP3.17} Courts may treat the CAs as selling a mixture of services and goods. In such "mixed" cases, there are a number of different ways to decide whether or not Article 2 applies:

{AP3.18} * Many jurisdictions use a "predominant factor" test, which looks at whether the parties intended that the transaction was predominantly for the sale of goods. If so, Article 2 will apply to the entire transaction. If not, the common law will apply.

{AP3.19} * Some jurisdictions use a "final product" test, which looks at the product remaining when a contract is completed. If the final product involves delivery of a good, Article 2 will apply to the entire transaction. If not, the common law will apply.

{AP3.20} * Some jurisdictions attempt to determine which classification best serves public policy.

{AP3.21} * Some jurisdictions divide mixed sales into "goods" and "services" components and then apply Article 2 to the goods component and the common law to the services component.

{AP3.22} Because jurisdictions apply so many different rules in analyzing whether something is a good or a service, it is likely that jurisdictions will reach different results on how to categorize certificates and to what extent Article 2 applies to them.

{AP3.23} In general, we believe that it is both likely and desirable that the certificate be viewed as evidence of the CA's performance of a service, meaning that the relationship between consumer and CA should not be governed by the rules contained in Article 2. The certificate is ultimately only valuable as evidence of the CA's performance of the services and the CA's willingness to stand behind its efforts. However, if the consumer and merchants are transacting goods, the consumer's delivery of the certificate to the merchant could be governed by Article 2 under either the predominant factor or final product test. Because of this, we also think it is possible that the relationship between the CA and the merchant, to the extent it is governed by contract law, could be governed in part by Article 2. Therefore, while we believe the analysis in Section (b)(ii) of this Appendix is more relevant to the CA/consumer relationship, the rest of this section completes the analysis of how Article 2 would apply to the various relationships.

{AP3.24} If an agreement for the sale of goods is silent on an issue, the relevant provision of Article 2 will be automatically incorporated into the agreement. However, the parties are free to vary most of the UCC provisions by contract, and many choose to do so.

(2) Contract Formation.

{AP3.25} Contract formation requires an offer, an acceptance and consideration. Under the UCC Section 2-206, an offer is a manifestation of a willingness to enter into a bargain, made so as to justify another person in understanding that assent will conclude the contract. Acceptance may consist of any conduct sufficient to show agreement, including performance if performance is a reasonable mode of acceptance. A contract may exist despite the fact the offeree does not expressly signify acceptance. In general, the UCC makes the formation of contracts easier than it was under the common law -- if the parties intended to contract, the court will enforce their agreement.

CA/Consumer Relationship

{AP3.26} In general, the CAs are likely to attempt to form contracts using the same formation process found with shrinkwrap licenses. Both involve mass-market transactions in which one party attempts to unilaterally bind the other to unnegotiated terms through conduct or performance. The U.S. Court of Appeals for the Seventh Circuit recently analyzed this issue in ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (1996), a case involving a software company's use of a shrinkwrap license contained inside the packaging. The ProCD Court found an offer and acceptance had occurred pursuant to UCC Section 2-206. The offer was implicit in the vendor's placement of software on the shelf for sale. The acceptance was the buyer's retention of the software after having reviewed the terms of the license and having had the opportunity to return the software. As a result, a contract was created which included, as its terms, the terms of the shrinkwrap license.

{AP3.27} Assuming the shrinkwrap license approach works, CAs will have little difficulty forming an agreement with consumers at the time when the consumers approach the CAs for certificates, at which point the contract will be formed when the consumer performs the requisite act. Alternatively, given that many CAs are now preinstalling certificates in consumers' browsers or clients, the CAs may also choose to require browser licensors to use their software license agreements to pass through to consumers the terms specified by the CAs.

CA/Merchant Relationship

{AP3.28} In the case of the merchant/CA relationship under Article 2, it is difficult to determine by what terms, if any, the merchant intends to be bound. Currently, most operating CAs attempt to specify that the merchant's use of the certificate is subject to the terms and conditions established by the CA (generally in the form of a certification practices statement). A CA may place some language in the certificate incorporating by reference the certification practices statement. In turn, the CA will make the certification practices statement available (often online). Under such practices, the merchant's act of relying on the certificate is a somewhat tenuous manifestation of the merchant's intent to enter into terms -- many of which were incorporated by reference and not on the face of the certificate -- the CA unilaterally imposes.

{AP3.29} Generally, the UCC can fill the gaps where all the terms of a contract have not been worked out, but only when the parties clearly intend to be bound. The question, then, is whether the merchant's ambiguous acts demonstrate the intent of the CA and merchant to be bound to one another in contract.

{AP3.30} Even if the CA's issuance of a certificate is sufficient to constitute an offer to all those who might use it in reliance, and the merchant's use is deemed sufficient to show a manifestation of assent to the terms contained in the certificate, the contract must be supported by consideration. Sections 17(1) and 71 of the Restatement (Second) of Contracts define consideration to be some right, interest, profit or benefit accruing to

one party, or some forbearance, detriment, loss or responsibility, given, suffered or undertaken by the other. In an open system, it is questionable if any consideration has been exchanged when the only interaction between the CA and the merchant is the certificate itself and possibly access to a CRL (which may not even be maintained by the CA).

{AP3.31} In sum, given the mechanics of the contract formation process and the UCC rules, we believe that merchants will have strong arguments to avoid the application of a CA's contract by asserting that no contract was formed. In addition, in light of our suggestions in the Report about the possibility of merchants bearing liability even if they act reasonably, it may be appropriate to avoid allowing the merchants to be inadvertently contractually obligated to bear additional risk.

{AP3.32} Although we believe this is unlikely, it is possible that merchants would desire to enforce the terms of the CA's agreement even if no contract is formed. In this case, the merchant would claim the benefits of an equitable doctrine known as promissory estoppel. Promissory estoppel requires that there be clear and definite terms (i.e. the terms of the certificate and perhaps the certification practices statement), the party urging estoppel (i.e., the merchant) acted to its detriment in reasonable reliance on the agreement, and fairness requires enforcing the agreement. However, the CA's agreement may contain terms (such as disclaimers of any accuracy or limits on liability) that would be sufficient to make the merchant's reliance unreasonable.

(3) Contract Terms.

CA/Merchant Relationship

{AP3.33} Assuming that a contract is actually formed between the merchant and CA, the next issue is to determine what terms are part of the contract. Terms may become part of the contract either by being contained within the actual certificate or by incorporation by reference into the certificate, so long as the merchant had notice of the terms and an opportunity to review them. There is no requirement that the merchant actually review the terms in order for the terms to become part of the agreement.

{AP3.34} Given the number of issues CAs might desire to address in their certification practices statements, the ability of CAs to incorporate terms by reference is very important to CAs. These documents legitimately can be dozens of pages long. On the Internet, it also becomes relatively simple to incorporate terms by reference through the use of hypertext links. Despite the general rule of contracts permitting incorporation by reference, it is entirely possible that courts will be reluctant to bind merchants to such voluminous terms that were only summarized in a certificate and then incorporated by reference by hypertext link. This might also support a finding that the agreement was unconscionable.

{AP3.35} In addition, if the UCC applies to the relationship between the CA and the merchant, under the UCC, to enforce certain disclaimers it is necessary that the disclaimer be conspicuous and that certain terminology be used in the disclaimer. These requirements may not be satisfied, and the disclaimer ineffective, through the incorporation by reference approach currently used by some CAs.

(4) Warranties and Limitations of Liability.

{AP3.36} Warranties are statements of fact made by a party to a contract which, if untrue, give rise to breach of the contract and an action for damages. Many vendors make express warranties in their contracts as an inducement to buyers; the UCC also specifies certain implied warranties which are automatically made by the vendor and included in any agreement unless properly disclaimed.

{AP3.37} Under the UCC, any disclaimers of warranties must be conspicuous and certain "magic words" must be used to disclaim certain implied warranties. So long as the disclaimers are not unconscionable, are conspicuous and use the proper "magic words," the CA and the consumer may contractually disclaim any warranties that would apply to the certificate.

{AP3.38} Many sellers find it desirable to limit their liability for damages. In particular, many CAs will want to disclaim liability for consequential damages, which are damages that are caused by an injury but are not the necessary result of the injury. CAs will also want to limit the dollar amount of damages they can be liable for. Consumers and CAs may agree to these types of limitations of liability in a contract so long as the waiver is not unconscionable, although again in consumer transactions, the waivers of consequential damages must be conspicuous.

{AP3.39} It is a more difficult issue determining whether or not, in the absence of a contractual relationship between CAs and merchants, UCC-based warranties (or the disclaimer of such warranties) extended in the CA's agreement with consumers will benefit, or limit the rights of, merchants. Section 2-318 of the UCC proposes three alternative rules governing the seller's warranty liability to third parties:

* seller's warranties extend only to persons in the buyer's family or household,

* seller's warranties extend to all natural persons who may reasonably be expected to use or be affected by the goods, or

* seller's warranties extend to all artificial as well as natural persons who may reasonably be expected to use or be affected by the goods.

{AP3.40} Many states have adopted one of these three official versions of Section 2-318, but several states have adopted their own variations. Given the multitude of approaches taken by the various states, it is likely that non-uniform rules will develop with respect to whether CAs will have warranty obligations to merchants under the UCC.

{AP3.41} In the absence of an effective contractual waiver or statutory limitation, CAs could be liable to merchants for all forms of damages (including consequential damages), and there would be no dollar cap on liability. If the CAs successfully form a contract with merchants, they can attempt to use the contract to disclaim warranties and limit their liability as discussed in the previous paragraph.

{AP3.42} Disclaimers of warranties and limitations of liability are also subject to UCC Section 2-719. Section 2-719(2) says that if a limited remedy fails of its essential purpose, other UCC remedies will be available, and Section 2-719(3) says that a party may limit consequential damages if not unconscionable. Some cases have held that 2-719(2) and 2-719(3) are dependent, meaning that consequential damages can be recovered, despite a limited remedy clause, when the limited remedy fails of its essential purpose. Other cases have held the sections independent, upholding the disclaimer of consequential damages even if the limited remedy fails of its essential purpose, so long as the disclaimer is not unconscionable. Once again, there is no predictability on this legal point.

(5) Unconscionability.

{AP3.43} UCC Section 2-302 specifies that an agreement will not be enforced when it is deemed unconscionable. Unconscionability can be found where the agreement is excessively one-sided, such as where the terms are unreasonably favorable to one party and the other party had little bargaining power and therefore an absence of meaningful choice. Unreasonably favorable contract terms include unfair limitations on consequential damages and excessive disclaimers of warranty. Courts may consider language barriers in evaluating the parties' relative positions. Courts may also consider if the party was unfairly surprised by the terms, such as in the case of a poorly educated party, hidden terms or a lack of a meaningful opportunity to read or understand the proposed terms.

{AP3.44} Unconscionability poses a meaningful problem to the contract formation between the CA and both the consumer and merchant. In addition to the importance to the CA of disclaiming implied warranties, excluding consequential damages and capping its dollar liability, the CA has many other terms it often will desire to include in its certification practices statement. The result could be a long, technical, complicated, legalese-intensive document.

{AP3.45} CAs' agreements with consumers could be deemed unconscionable because the consumer will often have limited sophistication to understand the terms of the contract and no bargaining power to negotiate over its terms. On the other hand, if a CA were to draft a "reasonable" agreement that it can legitimately argue could have been the outcome of a negotiated agreement, then the unconscionability doctrine may not apply.

{AP3.46} CAs' agreements with merchants could be deemed unconscionable because of the tenuous way in which the agreement is formed and the unreasonableness of

asking the merchant to review the agreement for each signature it desires to rely upon. On the other hand, the courts are less likely to treat merchants as lacking the sophistication to defend themselves, and merchants could always specifically negotiate an agreement if the merchant is uncomfortable with the CA's form agreement (meaning that merchants have some power to avoid the "take-it-or-leave-it" problem of most form agreements).

{AP3.47} The ambiguity over whether or not the CAs' agreements with consumers (and to the extent one is formed, with merchants) would be determined to be unconscionable is a particularly vexing problem for the CAs and is a major impediment to certainty in the industry. To attempt to resolve this problem, it could be appropriate for industry to undertake the effort of developing reasonable business practices which will establish industry standards that are not unconscionable.

(6) Proposed UCC Article 2B.

{AP3.48} A major overhaul of the UCC is currently underway, including the proposed addition of a new Article 2B to create new rules that apply to the sale or license of intangible informational "goods." If Article 2B is enacted, it is possible that a certificate would be covered under its rules. Many experts believe that Article 2B is the leading edge of an effort to resolve a global need for a commercial law structure for transactions in digital goods.

{AP3.49} Generally, Article 2B makes it easier for terms in standard form contracts which are not easily understood or known to the consumer at the time of contracting to be enforceable. Under the proposed rules, terms in standard form contracts, other than disclaimers of warranties in consumer transactions, will be deemed accepted by the licensee if, prior to or within a reasonable time after beginning to use the intangible, the licensee (a) signs or otherwise manifests assent to the form, and (b) had an opportunity to review the terms of the license before manifesting assent, whether or not the licensee actually read and understood the terms. If the terms are only available upon the initial use of the good (rather than prior to the acceptance of the good), the terms will only be enforceable if the licensee had the opportunity to return the good after reviewing the terms. Although Article 2B contains some limitations on contract enforceability (including, importantly, the doctrine of unconscionability), it places significant responsibility upon licensees to affirmatively reject terms by returning the goods if they find the terms unacceptable.

{AP3.50} However, Article 2B imposes a relatively strenuous "manifestation of assent" process for mass market transactions, which will require the CA to obtain express consent to certain terms of its agreement if the term would be objectionable to a reasonable licensee. This approach will require the CA to bring the potentially offensive term to the attention to the consumer or merchant and to obtain an express consent to that offensive term. If applied to CAs' agreements, this approach may seriously limit the ability of a CA to incorporate terms by reference into its certificates.

{AP3.51} Article 2B is still being considered by the National Conference of Commissioners on Uniform State Laws and the American Law Institute. Once adopted by these bodies, each state will make an independent decision about whether or not to adopt the article in whole or in part. It is expected to take several years for this process to be completed.

(ii) Services.

{AP3.52} The preceding sections discussed the legal application of the UCC to the relationships between CAs and consumers and CAs and merchants. This section discusses a similar analysis in the non-UCC context.

{AP3.53} In the United States, in contrast to the UCC's authoritative role in contracts for the sale of goods, there is no comprehensive uniform body of law governing contracts for services. As a result, each state's laws vary, although many apply variations of the common law.

(1) Relationship Between CAs and Consumers.

{AP3.54} Even if the relationship between the CAs and the consumers is categorized as a service relationship, making the UCC inapplicable, much of the analysis contained in the UCC section above will still be applied, by analogy, by the courts.

(2) Relationship Between CAs and Merchants.

{AP3.55} It must first be determined whether the CA and the merchant enter into a contractual relationship. Like the UCC, contract formation under the common law requires offer, acceptance and consideration.

Offer

{AP3.56} The first issue is whether the CA's certificate or any other activity by the CA constitutes an offer. Because the certificate may be distributed generally, it could be argued that the certificate is like an advertisement -- which generally is considered not to be an offer but merely is an invitation to make an offer. If the CA says on the certificate, however, that use of the certificate forms a binding agreement, it is likely that the certificate would be deemed an offer because such a statement would manifest the CA's intent to be bound.

Acceptance

{AP3.57} Generally, unless the offer specifies a manner of acceptance, any reasonable manner of acceptance is sufficient to form a contract. Silence alone cannot constitute acceptance, and the offeror cannot make silence a means of acceptance if the offeree did not intend silence to indicate assent. In the case of certificates, however, the merchant would do more than remain silent; it would manifest assent in accordance with the method for acceptance specified in the certificate -- e.g., by relying upon the information contained therein. Case law suggests that in some situations this is

sufficient to constitute acceptance, although other cases indicate that mere reliance on proposed terms is insufficient.

Consideration

{AP3.58} As discussed earlier in the UCC section, it is unclear if the CA and merchant exchange consideration. This applies equally in the case of agreements for services.

Conclusion

{AP3.59} We have already noted that it is more difficult to form a contract under the common law than it is under the UCC. Given that we think it is unlikely a contract between the merchant and CA is formed under the UCC, we believe it is even less likely that a contract between the merchant and CA will arise under a common law analysis solely by virtue of the terms contained in the certificate.

(3) Implied Warranty of Workmanship.

{AP3.60} Unless properly disclaimed, an agreement for services contains an implied warranty of workmanship; that is, that the services were performed in a workmanlike manner. In essence, this creates an obligation on the part of the party performing the services not to act negligently. Since negligence is a tort concept, courts are frequently faced with alternative claims from customers under service agreements for breach of warranty and for negligence. Principles relating to tort law in the PKI context are discussed in Section (d) below.

(4) Liability Limitations and Unconscionability.

{AP3.61} If a contract exists between the CA and the merchant, limitations of liability and disclaimers of warranty which became part of the contract will still be subject to principles of unconscionability such as those found in the UCC. As with the UCC, case law in this area demonstrates the absence of clarity over when form non-negotiated agreements will be enforceable and when they will not.

(5) Extension of Warranties to Merchants.

{AP3.62} In the absence of an agreement in place between a merchant and a CA, there exists an alternative argument under common law for a merchant to have recourse against a CA for losses suffered. The traditional rule in service relationships has been that one party is not liable to any party not in contractual "privity" (i.e., has entered into a contract with the party causing harm). However, this general rule has been relaxed by several jurisdictions. In the case of merchants, this means that in some situations merchants may be able to benefit from the warranties (if any) granted by the CA to the consumer.

{AP3.63} In some ways, the CA -- by providing a certificate regarding the accuracy of information -- can be analogized to information providers, who provide information both to parties in privity and to parties who have some affiliation with the parties in privity.

The landmark case of Ultramares Corp. v. Touche, 255 N.Y. 170 (1931), rendered by the highest court in the state of New York, held that information suppliers who fail to use reasonable care are liable only to parties in privity. The court reasoned that to extend this duty to parties not in privity would expose information providers to liability to an indeterminate class of people for an indeterminate amount. The Ultramares court was willing to extend the information suppliers' duty of care to third parties that the information provider knew were the ones for whom the information was being furnished. In the case of CAs, this could easily include the intended recipients (i.e., the merchants). However, mere knowledge that the party in privity intends to use the information commercially in dealing with unspecified third parties did not create a duty of care toward such third parties.

{AP3.64} There is a continuum across jurisdictions in their adherence to the privity rule. Among the theories deployed by jurisdictions:

* Liability extends only to those in privity.

* Liability extends where the third party was known.

* Liability extends where the third party was known but only if there was actual communication between the information provider and the third party.

* Liability extends to all foreseeable third parties.

* Liability extends based upon a balancing of various factors.

* Liability extends only when the parties not in privity are physically injured.

{AP3.65} Given that there is not a standard for whether or not information suppliers are liable to parties not in privity, it is unclear to what extent the CA could be liable to merchants based on a CA's contract with consumers.

{AP3.66} One additional theory under which merchants could attempt to claim the benefits of the CA's warranties to consumers is the legal doctrine of "third party beneficiary." Generally, to be a third party beneficiary: (a) the merchant must be identified in the promises between the consumer and the CA, (b) the merchant must have the performance of the promise rendered directly to the merchant, (c) there must be a relationship between the consumer and the merchant that supports an intent to benefit the merchant, and (d) either (i) the merchant gets the CA's performance as a gift, or (ii) the consumer has an obligation to the merchant which is being performed by the CA. While some arguments could be made for the application of this theory to benefit the merchant, it would not be a traditional application of third party beneficiary law.

(iii) United States Federal Law - Magnuson-Moss.

{AP3.67} The Magnuson-Moss Act governs written warranties provided with "consumer products" (i.e., tangible person property which are normally used for personal, family or

household purposes). The Magnuson-Moss Act requires that written warranties freely and conspicuously disclose, in simple and readily understood language, the terms and conditions of the warranty. Specific language must be included with any limitations of warranty or limitations of liability, and other restrictions regarding the manner of describing the warranty must be adhered to. While the Magnuson-Moss Act may apply to certificates, compliance with the Act is relatively mechanical.

(c) Contract Law in Certain Non-U.S. Jurisdictions.

{AP3.68} This section identifies some applicable European laws that could apply to transactions using digital signatures. As will be clear, although some general rules could apply in the consumer context, there are no comprehensive uniform rules that apply to consumer transactions in Europe or elsewhere.

(i) UN Convention on the International Sale of Goods.

{AP3.69} The UN Convention on the International Sale of Goods ("CISG") is the United Nations' counterpart to the UCC. However, the CISG applies to commercial sales only, not to consumer sales or service contracts, so its applicability to this Report is by analogy only.

{AP3.70} The CISG applies a predominant purpose test similar to the UCC's approach to determine whether its provisions apply to a particular agreement. The parties can contractually avoid the application of the CISG.

{AP3.71} Generally, it is slightly more difficult to form a contract under the CISG than it is under the UCC. For instance, the CISG requires a price to be specified in the contract. The CISG also requires that the acceptance mirror the offer on all material terms. If terms in the offer and acceptance differ, no contract is formed -- unlike the UCC, where a contract would be formed, but the conflicting terms would drop out and the UCC terms would fill in the gaps.

{AP3.72} The theory underlying the UCC is that parties rarely read the boilerplate in forms, and thus contracts should only consist of terms that the parties actually agree upon. The CISG, on the other hand, believes boilerplate terms are important, and a contract should not form unless all material terms are agreed upon.

{AP3.73} This difference provides insight into the philosophical underpinnings of the UCC and CISG that might impact the issue of whether a contract is deemed to be formed between CAs and merchants. Under the CISG, an offer addressed to specific people constitutes an offer if it is sufficiently definite and indicates an intention of the offeror to be bound. In contrast, an offer to many unspecified people is just an invitation to make an offer, unless contrary intent is clearly indicated. Under the CISG, any statement or conduct by the offeree indicating assent is an acceptance. The CISG is explicit that silence alone will not amount to an acceptance. Thus, the merchant's use of the certificate might be more likely to be deemed a valid acceptance under the UCC than it would under the CISG, which appears to require more formal assent to material

terms. As indicated earlier, we believe it is unlikely that a contract is formed under the UCC between merchants and CAs, so it is doubtful a contract would be formed under the CISG.

(ii) E.U. Directive on Unfair Contract Terms.

{AP3.74} European Union Directives are legislative acts articulating E.U. policy which are binding on the European Union's member states. The Directives are intended to establish uniform legislation throughout the European Union, so that entities doing transborder business will have to comply with only one set of rules. Usually, member states have three years to conform their laws with an adopted directive.

{AP3.75} The E.U. Directive on Unfair Contract Terms addresses non-negotiated consumer form contracts such as those used by CAs. The Unfair Contracts Directive states that unfair terms are unenforceable but such terms may be severed from the contract and the remaining terms enforced. The Unfair Contracts Directive defines unfair terms to be those terms that are: (a) not negotiated and which are contrary to the obligation of good faith or which impose a significant imbalance in the parties' rights, and (b) obligations under the contract to the detriment of the consumer. The Unfair Contracts Directive describes types of terms deemed to be imbalanced, including terms that the consumer did not have the opportunity to appreciate before the contract was formed. However, the Unfair Contracts Directive allows for the consideration of circumstances and the nature of the goods or services sold. Finally, if terms have conflicting meanings, the term will be interpreted most favorably to the consumer. As with the principles of unconscionability in the U.S., the Unfair Contracts Directive could significantly circumscribe the CAs' ability to rely on the terms of its contract.

{AP3.76} Germany has a long-standing set of laws ("Gesetz zur Regelung des Rechts der Allgemeinen Geschaftsbedingungen" or "AGB-Gesetz") similar to the E.U. Directive on Unfair Contract Terms. The AGB-Gesetz generally provides that contract terms which one party has unilaterally established in advance with the intent of using them in a number of future transactions must be clearly identified to the other party, who must be given a reasonable opportunity to review these terms and approve them in advance. If these conditions are not complied with, the terms and conditions will be disregarded and the entire contract will be governed by statutory law. The AGB-Gesetz is generally interpreted by the courts in a very consumer-friendly way.

{AP3.77} Under the AGB-Gesetz, it is unclear to what extent courts will allow parties offering goods or services on the Internet to bind purchasers to standard contract terms which take up many computer screens and which would require the purchaser to spend a long time online reviewing them. Further, lengthy and complex certification practice statements could very well be unenforceable under the AGB-Gesetz.

{AP3.78} (iii) German Consumer Protection Laws. A number of statutes designed to protect consumers could prove problematic when applied in the context of digital signatures and electronic commerce. For instance, the "Law on Revocation of Contracts

Concluded Door-to-Door" (Hausturwiderrufsgesetz) gives consumers a wide-ranging right to revoke contracts concluded "door-to-door" within a certain time limit. The extent to which this law would apply to online transactions concluded by consumers in their homes by digital signatures is a matter of debate in Germany. If it did apply, this law could allow consumers to invalidate transactions consummated using digital signatures. Similar issues arise with regard to the Law on Consumer Credit Transactions (Verbraucherkreditgesetz).

(d) Tort Law.

(i) Tort v. Contract.

{AP3.79} In general, parties are free to establish legal relationships with each other. This is done by contract. However, in common law jurisdictions, there are situations where, even when the parties do not enter into a contract, one party will owe a duty to the other party. The body of law imposing these duties is called tort law. There are situations where tort obligations can exist even though parties have entered into a contract governing their relationship. Indeed, in the United States, it is often difficult for merchants to prospectively disclaim, by contract or otherwise, tort liability for harms created by their products.

(ii) In the United States.

{AP3.80} The most likely basis for a tort action by a consumer or merchant against a CA is the tort of negligent misrepresentation. Generally, negligent misrepresentation requires the following elements: (a) there was a material misrepresentation, (b) the misrepresentation was false, (c) the information supplier breached a duty of care to provide accurate information to the party requesting information, and (d) the plaintiff suffered injury as a result. Many courts require the existence of some type of commercial relationship between the parties prior to imposing liability. Most jurisdictions do not extend liability to unknown third parties.

{AP3.81} The Restatement (Second) of Torts §552 (a highly persuasive summary of general U.S. law principles) states that one who, in the course of a business, profession or employment, or any transaction in which he has a pecuniary interest, supplies false information for the guidance of others in their business transactions, is subject to liability for the pecuniary loss caused by justifiable reliance on the information if he did not use reasonable care. In the case of CAs, the CAs will often be in a position to assert that merchants' reliance was not justified because of limiting language in the certification practices statement.

{AP3.82} Note that currently no standard of care currently exists for CA conduct so it is unclear what conduct will subject a CA to liability for negligent misrepresentation. The Utah Digital Signature Act contains some minimum standards, but these have not been universally adopted.

{AP3.83} Alternatively, some jurisdictions state that misrepresentations, even if innocent, will give rise to tort liability when the party disseminating the information had the means of knowing, ought to know, or had a duty to know the truth. These cases arose only in limited circumstances (primarily involving errors in aviation maps) and have been severely criticized by legal scholars.

{AP3.84} As with the discussion regarding extension of UCC warranties to third parties, jurisdictions have formulated a wide range of rules about who can assert tort claims for negligent misrepresentation and what the damages will be:

* The Restatements limit liability to loss suffered by a limited group of people for whose benefit and guidance one intends to supply the information for or knows the recipient intends to supply it to.

* The majority of jurisdictions allow no recovery for negligent misrepresentation for economic loss.

* Some jurisdictions allow recovery to those not in privity only for physical injury or economic loss caused by the use of a product.

* Some jurisdictions allow recovery for economic loss if there was a special relationship between the party acting tortiously and the injured party.

* Some jurisdictions take a broad view of the class of risks and the class of victims that are foreseeable.

{AP3.85} Currently, UCC Article 2B proposes to adopt an implied warranty regarding information which parallels the Restatements position. This approach has been criticized by some members of the drafting committee and certain legal scholars.

(iii) E.U. Directives on Products Liability.

{AP3.86} The European Union has adopted two Directives related to products liability that could potentially affect CAs. The "Strict Products Liability Directive" (85/374/EEC) imposes liability on manufacturers for injuries caused by defective products, even if the manufacturer was without fault. To recover, an injured party only needs to show damages, a defective product, and a causal relationship between the two. Under this Directive, damages are limited to personal injuries or property damage, but some E.U. member states permit recovery for pain and suffering or punitive damages as well.

{AP3.87} The "General Product Safety Directive" (92/59/EEC) requires manufacturers and suppliers to place only safe products on the market, to provide consumers with all relevant information related to risks associated with their use, and to inform consumers whenever use of a product may be dangerous. It also requires distributors to monitor the safety of products on the market, pass on information about product risks, and cooperate in actions taken to avoid such risks.

{AP3.88} It is unclear whether a certificate issued by a CA would be considered a "product" and thus within the scope of these Directives. Under the Strict Products Liability Directive, "products" are defined as "all movables . . . even [if] incorporated into another movable or into an immovable." Interestingly, electricity is expressly included as a "product." At least one United Kingdom case has suggested that software was a product under that country's implementation of this Directive, but its analysis focused primarily on the tangible nature of a floppy disk. We believe that it would be unlikely and inappropriate to categorize certificates as a "product" under these Directives, just as we concluded that it is unlikely that certificates will be categorized as a good under the UCC.

(e) Digital Signature/CA Laws.

(i) United States of America - State Laws.

{AP3.89} Several states within the United States are developing digital signature legislation. Several of the more important state efforts are surveyed here; a complete list of current state digital signature legislation is provided in Appendix 5. The Utah, California and Florida approaches represent three different approaches to the problem of developing legislation regarding digital signatures; many other states that have considered or have passed digital signature-related legislation have followed one of these three approaches.

{AP3.90} We have not attempted here to identify if any of these legislative efforts actually resolve some of the legal difficulties identified in the previous sections, although such an inquiry would surely yield some insight.

(1) Utah.

{AP3.91} The first state to adopt digital signature legislation was Utah, which enacted the Utah Digital Signature Act of 1995 (as amended) (the "Utah Act"). The Utah Act's stated goals are: (1) to facilitate commerce by means of reliable electronic messages; (2) to minimize the incidence of forged digital signatures and fraud in electronic commerce; (3) to implement relevant standards, such as Standard X.509 of the International Telecommunication Union; and (4) to establish uniform rules regarding the authentication and reliability of electronic messages.

{AP3.92} Under the Utah Act, a government agency assumes the obligations of being a "top level" CA and is charged with policy making, facilitating implementation of digital signature technology, and providing regulatory oversight. Licensing under the Utah Act is voluntary; however, licensed CAs are offered certain legal benefits. Utah may provide the same legal benefits to CAs licensed or authorized by other jurisdictions if the licensing or authorization schemes are substantially similar to the Utah Act and regulations.

{AP3.93} The Utah Act imposes certain duties on CAs and subscribers. Prior to issuing a certificate to a subscriber, the CA must confirm, among other things, that: (1) the

prospective subscriber is the person to be listed in the certificate; (2) the information in the certificate is accurate; and (3) the subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate. Neither the CA nor the subscriber can waive these requirements. By issuing a certificate, a CA makes certain warranties to the subscriber, including that the certificate contains no information the CA knows to be false and that the certificate satisfies all material requirements of the Utah Act. The CA cannot disclaim or limit these warranties. By issuing a certificate, a CA certifies to all who reasonably rely on it that, among other things, the information in the certificate is accurate and that the subscriber has accepted the certificate.

{AP3.94} By accepting a certificate issued by a licensed CA, a consumer certifies to all who reasonably rely on the certificate that the consumer rightfully holds the private key corresponding to the public key listed in the certificate, and that all representations made by the subscriber to the CA or otherwise incorporated into the certificate are true. A subscriber is obligated to indemnify the issuing CA for any loss or damage caused by publishing or issuing a certificate in reliance of: (1) a false and material representation of fact by the subscriber; or (2) the subscriber's failure to disclose a material fact done intentionally to deceive the CA or a person relying on a certificate or negligently. This indemnity obligation cannot be disclaimed or contractually limited in scope. By accepting a certificate, a subscriber also assumes a duty to exercise reasonable care to retain control of the subscriber's private key and to prevent its disclosure to any person not authorized to create the subscriber's digital signature.

{AP3.95} The Utah Act provides that, unless waived by the CA, a CA is not liable for any loss caused by reliance on a false or forged digital signature if the CA complied with all material requirements of the Utah Act with respect to the false or forged digital signature. A licensed CA is not liable in excess of the amount specified in the certificate as its recommended reliance limit for a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed CA was required to confirm. Furthermore, a licensed CA is only liable for direct compensatory damages and not for punitive or exemplary damages, damages for lost profits or lost opportunity, or damages for pain and suffering.

{AP3.96} If reliance on a digital signature is "not reasonable under the circumstances," the recipient of that digital signature assumes the risk that digital signature is forged.

{AP3.97} Several evidentiary presumptions arise under the Act, including:

(1) a presumption that a certificate digitally signed by a licensed CA and either published in a recognized repository or made available by the issuing CA or by the subscriber listed in the certificate is issued by the CA which digitally signed it and is accepted by the subscriber listed in it;

(2) a presumption that the information listed in a valid certificate and confirmed by a licensed CA issuing the certificate is accurate;

(3) a presumption that, if a digital signature is verified by the public key listed in a valid certificate issued by a licensed CA:

> (a) that digital signature is the digital signature of the subscriber listed in that certificate;
>
> (b) that digital signature was affixed by the signer with the intention of signing the message; and
>
> (c) the recipient of that digital signature has no knowledge or notice that the signer: (i) breached a duty as a subscriber; or (ii) does not rightfully hold the private key used to affix the digital signature; and

(4) a presumption that a digital signature was created before it was timestamped by a disinterested person utilizing a trustworthy system.

{AP3.98} Unless waived, a recognized repository, or the owner or operator of a recognized repository, is not liable for its failure to record suspension or revocation of a certificate unless more than one business day elapsed after notice was received. Otherwise, the repository may be held liable for any loss of a person who relied on a revoked or suspended certificate, up to the amount of the recommended reliance limit on the relevant certificate and including only direct compensatory damages and not punitive damages or lost profits, savings, or opportunity. Repositories are not liable for misrepresentation in a certificate published by a licensed CA.

(2) California.

{AP3.99} In contrast to the broad scope of the Utah Digital Signature Act, California has adopted legislation pertaining only to digital signatures affixed to communications with public entities. The Act provides that a digital signature (which is defined as an electronic identifier created by a computer) shall have the same force and effect as a manual signature if: (1) it is unique to the person using it; (2) it is capable of verification; (3) it is under the sole control of the person using it; (4) it is linked to data in such a manner that if the data are changed, the digital signature is invalidated; and (5) it conforms to regulations adopted by the Secretary of State. Any party has the option to use or accept a digital signature. The California Secretary of State is supposed to promulgate regulations implementing the legislation by March 1, 1997.

(3) Florida.

{AP3.100} Florida's "Electronic Signature Act of 1996" authorizes the Secretary of State to be a CA to verify electronic signatures and requires it to study the use of electronic signatures for commercial purposes.

(ii) United States - Federal Laws and Regulations.

{AP3.101} The National Institute of Standards and Technology ("NIST") has algorithm standards in place for digital signatures. The Digital Signature Standard, or DSS, uses public and private keys, and users can encrypt a signature only or the entire message. In support of the DSS, the General Accounting Office issued a decision that electronic signatures create a valid contract consistent with federal law. The Pentagon also notified NIST that the digital signature standard can be used by the Defense Department to sign unclassified data and -- in some cases -- classified da ***

## Appendix 4

## Certification Authority Services and Policies

### 1. Introduction.

This is Appendix 4 to the Report of the ILPF Working Group on Certification Authority Practices (the "Report"). This Appendix provides a "snapshot" of the industry's development by surveying the practices and policies of selected Certification Authorities ("CAs").

This Appendix first briefly summarizes the existing or prospective services of eight CAs who offer or plan to offer services which most closely match the consumer transaction-oriented model discussed in the Report. Additionally, this Appendix briefly summarizes the existing or prospective services of five other entities whose services differ from the consumer-oriented model discussed in the Report; these other entities illustrate the fact that digital certificates will be used for a variety of purposes in a number of distinct contexts.

Next, this Appendix surveys the practices and policies of certain consumer-oriented CAs in four legally significant areas: (1) subscriber authentication techniques; (2) the legal relationship established between CAs and a subscriber (including issues such as warranties, liability limitations, and legal duties imposed on CAs and subscriber); (3) the legal relationship established between CAs and relying non-subscribers (including warranties, liability limitations, and legal duties); and, (4) key management techniques (including key generation, key revocation, and root key authenticity and security). This discussion focuses primarily on four CAs which have disclosed their relevant practices and policies: VeriSign (which has disclosed a great deal of relevant information), and COST, Nortel and Signet Systems (which have made more limited amounts of information available). The other consumer-oriented CAs have offered little or no information concerning the policies on these legal issues.

This Appendix and its attachment are current through December 1, 1996. Numerous significant changes have occurred since December 1, 1996 that are not reflected in this Appendix.

This Appendix does not address other companies and organizations who have expressed a general intent to offer certification services. A list of the companies and organizations discussed in this Report, and other companies and organizations of interest, and their World Wide Web addresses are included in Attachment A to this Appendix.

## 2. GENERAL DESCRIPTION OF CA SERVICES.

### (a) Consumer-Oriented CAs.

**(i)** COST Computer Securities Technologies (Kista, Sweden)

*NOT YET ACTIVELY issuing certificates to individuals*

COST offers certification services derived from the Internet Engineering Task Force's (IETF) Privacy Enhanced Mail (PEM) model; COST has extended the PEM model in order to transfer certificates via the World Wide Web. COST's own certificate is self-signed. COST acts as a Policy Certification Authority (PCA) for national CAs in Sweden, Holland, the U.K., Germany, Switzerland, Italy, Spain, Austria, Ireland, Malaysia, and Singapore. Two U.S.-based servers are also incorporated into the COST hierarchy. COST currently certifies only other CAs, including company CAs. In the future, they plan to offer certification services directly to individuals. COST has articulated three identity-assurance policies: Low Level Assurance, Medium Level Assurance, and High Level Assurance. COST maintains certificate revocation lists for the CAs which it currently certifies. Additionally, COST offers several sophisticated hardware and software products for use by CAs and subscribers, including a smart card-based digital signature system. [After the cut-off date for this Appendix, Sembawang Media of Singapore launched a CA pilot project based upon the COST hierarchy. This pilot effort does include the issuance of certificates directly to individuals. Representatives from COST report that other COST-hierarchy CAs are also issuing certificates to individuals, but such certificates are currently not accessible online.]

**(ii)** EuroSign (United Kingdom)

*ACTIVELY issuing certificates to individuals*

EuroSign is currently offering an "EasySign" certificate, which involves only the subscriber's self-certification of identity. No certificate-related services (i.e., revocation or validation) are available. EuroSign appears to be a recent start-up with limited resources.

**(iii)** GTE CyberTrust (Needham, MA USA)

*NOT YET ACTIVELY issuing certificates to individuals*

GTE CyberTrust plans to offer three different types of CA services. Under its SETsign program, GTE will provide CA services for credit card and other major card-issuing organizations that want to use the Secure Electronic Transaction (SET) protocol. GTE plans to provide SET-compliant certificate services for cardholders, merchants and banks. GTE's CYBERsign program is designed to provide public key certification for individuals at three different identity assurance levels: name-uniqueness only, trusted third party verification, and in-person verification. GTE's Virtual CA program will provide

CA services for organizations that require CA capability but do not desire CA ownership responsibilities. [On Dec. 18, 1996 GTE CyberTrust announced that it has issued to Wells Fargo Bank the first operational digital certificates to comply with the SET protocol, and that it was providing Wells Fargo and participating merchants with a wide range of certificate management and support services.]

**(iv)** Nortel Entrust (Toronto, Canada)

*ACTIVELY issuing certificates to individuals*

Nortel is currently offering free "Entrust Demo Web Certificates" to the public. These X.509-compliant certificates use Nortel's proprietary public key technology and can be installed into certain web browsers. Nortel does not investigate the accuracy of identification information submitted by subscribers. The certificates carry a two-year expiration date; there are no procedures for revoking certificates. In addition, Nortel is offering free "no assurance" certificates for web servers. Nortel's focus appears to be on licensing its technology to other companies that engage in certification services, rather than on providing CA services itself. Nortel markets its Entrust products for use by others on private computer networks and on the Internet. [In January, 1997 Northern Telecom Limited spun-out the Entrust division into a separate company, Entrust Technologies.]

**(v)** Signet Systems (Brisbane, Australia)

*ACTIVELY issuing certificates to individuals*

Signet is involved with a pilot project associated with Australia's proposed National Public Key Authentication Framework (PKAF). Signet acts as a Policy Approval Authority (PAA), issuing certificates to customers and partners who further offer certification services. On July 1, 1997, Signet's PAA certificate will be revoked and replaced with the government-issued Policy and Root Registration Authority (PARRA) certificate envisioned by the PKAF. Additionally, Signet apparently is offering certificates directly to subscribers. The scope of certification-related services available online (i.e., certificate acceptance, revocation or validation) is unclear. Signet has articulated three increasingly rigorous policies under which it will issue certificates: personal, business, and legal/financial. Signet incorporates such policies into certificates via ASN.1 notation and ISO-registered object identifiers.

**(vi)** Thawte Certification Services (Durbanville, South Africa and Raleigh, NC USA)

*NOT YET ACTIVELY issuing certificates to individuals*

Thawte plans to offer three types of certificates, which it calls "Digital IDs." Basic Certificates will involve no identity assurance; Medium Certificates will involve "some documentation" in addition to self-certification of identity; and Strong Certificates will require personal presence at a Thawte office prior to issuance. Thawte had made Beta

Test Certificates available for installation in the beta release of Netscape Navigator 3.0. Beta Test Certificates required only self-certification of identity, and no revocation or validation services were available. Thawte no longer offers beta certificates, however. Thawte's website promises that the full panoply of certificates will be available on November 15, 1996, but no certificates were available as of December 1, 1996. Thawte also plans to offer server certificates.

**(vii)** United States Postal Service (Washington, D.C. USA)

*NOT YET ACTIVELY issuing certificates to individuals*

As part of the General Services Administration's Federal Security Infrastructure Program, the United States Postal Service (USPS) intends to act as a CA for members of the public who wish to interact electronically with the U.S. government and others. Subscribers will present identification at a local Post Office and receive a "smart disk" (produced by Fischer International Systems) to use to generate encryption keys. In addition to sending encrypted and digitally-signed e-mail, subscribers will utilize a proprietary secure browser (made by Frontier Technologies) to communicate securely through the Web. The system will use the government's Data Encryption Standard and Digital Signature Standard. No certification services are currently available to the public.

**(viii)** VeriSign (Mountain View, CA USA)

*ACTIVELY issuing certificates to individuals*

VeriSign offers "Digital IDs" (certificates) to the public, for use in web browsers and S/MIME compliant e-mail applications. VeriSign plans to offer four classes of Digital IDs, each with different levels of assurance of a subscriber's identity. Classes 1 - 3 are intended for use by individuals; Class 4 is intended for business use and will certify an individual's relationship with an organization as well as certify that individual's identity. Currently Class 1 and Class 2 Digital IDs are available. Under a Class 1 Digital ID, an individual self-certifies his identity. Under Class 2 Digital IDs, an individual's self-Reported information is automatically verified against a consumer database maintained by Equifax. Certificates can be revoked, and the validity of certificates can be checked, via VeriSign's website. VeriSign also offers Digital IDs for web servers, which are used to identify and authenticate particular servers and to encrypt information passed between a server and a web browser.

**(b) Non-Consumer-Oriented CAs.**

**(i)** CertCo, LLC (New York, NY USA)

CertCo, which is affiliated with Bankers Trust, plans to issue certificates through banks and other financial institutions beginning in 1997. Little information is available about their planned services, but evidently CertCo intends to coordinate a consortium of companies, each with certificate authority status. Each company in the consortium will

hold only part of the relevant root key, and each company will share in the liability risk associated with issuing certificates.

**(ii)** CivicLink (Chicago, IL USA)

CivicLink is a service which allows a user to access government records online. Currently some limited records from Prince George County, Maryland, Marion County, Indiana, and Los Angeles County, California are accessible. For Los Angeles County, limited electronic filing of court documents is possible. Electronic filing, available since May 1996, is accomplished using digital signatures or by fax via CivicLink. Ameritech Information Access (AIA), a joint venture of Ameritech and BC Systems Corporation (Canada), operates CivicLink and serves as a certification authority. Digital signatures created under this system are currently intended only for use in filing court documents with LA County. AIA indicates that they intend to expand the potential uses of their certificates.

**(iii)** Internet Commerce Group (Mountain View, CA USA)

Sun Microsystem's Internet Commerce Group offers Certification Authority services to customers of its SunScreen product line; the certificates are used primarily for access control. SunScreen is a turnkey security system comprised of hardware, software, and services, designed for complex commercial networks. Sun provides two certification services: *SunCA* (1024-bit certificates), and *SunCAglobal* (export-oriented 512-bit certificates). The self-signed public certificates of each of these CAs are published on the Internet Commerce Group's website. Certificate revocation lists, updated monthly, are also published on the website.

**(iv)** TradeWave TradeAuthority (Austin, TX USA)

TradeWave's TradeAuthority program performs certification services for customers of TradeWave's TradeVPI software system. TradeVPI allows businesses to set up "Virtual Private Internets" in order to utilize the public Internet to establish a secure private network. TradeAuthority is a self-certified online CA which issues certificates enabling users to access a particular VPI. Potential subscribers ask to become VPI members by filling out an online membership form using a proprietary TradeWave browser and submitting it to the TradeAuthority. The subscriber must then be approved by a designated Local Registration Agent (LRA) appointed by the VPI owner. The TradeAuthority then issues certificates to subscribers upon LRA approval. Certificates can be revoked by the LRA, and certificate revocation lists are updated daily. TradeAuthority uses public key technology licensed from Nortel Entrust.

## 3. CERTIFICATION AUTHORITY POLICIES.

### (a) Subscriber Authentication Techniques.

Three active certification authorities (VeriSign, Nortel Entrust and EuroSign) offer certificates that do not authenticate a subscriber's identity. Certificates are issued based solely on unverified information submitted online by a subscriber. GTE CyberTrust and Thawte have indicated that they intend to issue this type of certificate as well. It is unclear whether Signet offers this type of certificate.

VeriSign also currently issues Class 2 certificates, for which VeriSign automatically compares information submitted by a subscriber against a database maintained by Equifax before issuing a certificate online. A criminal could still defeat this system by submitting information that matches an individual's information in the Equifax database. GTE CyberTrust indicates that it plans a similar third-party verification scheme for some of its certificates. No other CA currently offers a similar service.

VeriSign's planned Class 3 certificates will require submission of a notarized copy of a signed application, in addition to registering online. The notary is required to check and list three forms of identification documents, including at least one with a picture. VeriSign generally will not process applications that fail to comply with this requirement. VeriSign will not investigate or otherwise certify notaries.

Signet indicates that under its "Personal" policy, subscriber identity will be verified based only on information the subscriber submits on an application form. Under, Signet's "Business" policy, identity will be authenticated using various specified business documents. Authentication techniques under the "Legal" policy have not been publicly specified.

The USPS has indicated that it will require "a picture ID" before issuing encryption keys. No other CAs have publicly detailed the steps they intend to take in order to authenticate the identity of subscribers.

### (b) Legal Relationship Between CA and Subscriber.

Three of the four CAs currently issuing certificates to individuals -- VeriSign, Signet and Nortel -- demand that subscribers manifest agreement to certain legal terms as a condition of accepting or using a certificate. EuroSign does not require assent to any legal terms as a precondition to obtaining a certificate. COST, while not currently offering certificates to individuals, had outlined some aspects of its approach to the CA/Subscriber legal relationship. GTE CyberTrust, Thawte, and the U.S. Postal Service have not publicly disclosed the legal terms under which they plan to offer their services, or the legal mechanisms they intend to use to implement such terms.

Nortel's legal agreement with subscribers is brief and straightforward. Prior to beginning the certificate-issuance process online, a potential subscriber is confronted with a web

page containing two paragraphs of legal terms. The potential subscriber must click on a button marked "acknowledge" in order to proceed to the next step.

Signet's "Certification Authority Service Agreement" with subscribers is a ten page contract which resembles a commercial software license in language and format. Signet intends for subscribers to manifest assent to this contract by signing a paper document. The agreement specifies that it is governed by Australian law.

VeriSign's "Subscriber Agreement" is presented to potential subscribers during the online certificate application process in much the same fashion as Nortel's agreement. In addition to containing a number of significant legal terms, VeriSign's agreement incorporates VeriSign's Certification Practice Statement (CPS) by reference. The CPS is a lengthy (83 pages when printed) hypertext document which details VeriSign's certification practices and policies and contains numerous legally significant provisions.

**(i) Warranties to Subscribers.**

Nortel's agreement indicates that Nortel "accepts no responsibility or liability" arising from use of its demo certificates and indicates that the certificates contain unverified information. Otherwise, its agreement does not explicitly address the issue of warranties.

Signet's agreement states that Signet "will endeavor" to provide certification services in accordance with certain stated goals, which relate primarily to availability of online resources. Signet does appear to accept liability for failure to meet certain service goals, with damages set at a fixed amount. However, the agreement also notes that Signet "gives no warranty or guarantee in relation to the performance, features or compatibility of co-operating electronic certification products or services." Furthermore, the agreement states that, subject to some limitations, "all terms, conditions, warranties, undertakings, inducements or representations whether express, implied, statutory or otherwise relating in any way to the provision of the Certification Service or other obligations under this agreement will be excluded."

VeriSign's subscriber agreement states: "AS STATED IN THE CPS, [VERISIGN] DISCLAIMS CERTAIN IMPLIED AND EXPRESS WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE" (throughout this Appendix, capitalization in quotes mimics the original). VeriSign does offer certain limited warranties, detailed in twelve separate sections of the CPS. Among other things, VeriSign warrants that it will follow certain key management practices and that it will follow certain identification authentication procedures for each class of certificate.

COST also that indicates that it is willing to offer some warranties. Under its Medium Assurance Policy, COST states that it will accept some limited liability as to the validity of certificates and the correctness of identification information in certificates, under circumstances negotiated with customers. Under its High Level Assurance Policy,

COST indicates that it accepts "full liability" as to validity and identification. The exact meaning of "full liability" is unclear and may have specific meaning under Swedish law. It is also unclear whether COST has issued any certificates to CAs under either of these policies (COST does not yet issue certificates to individuals).

(ii) **Liability Limitations.**

Concerning liability limitations, Nortel's agreement simply states that Nortel accepts no liability arising from the use of its certificates. Further, the agreement requires the subscriber to agree that to the following: "I will indemnify Nortel for any claim or liability arising from my misrepresenting myself to any third party."

Signet's agreement states that, with certain qualifications, "Signet will not be under any liability (including liability as to negligence) to the Customer or to any third party in respect of any loss or damage (including consequential loss or damage), however caused, which may be suffered or incurred or which may arise directly or indirectly as a result of or in connection with the provision of the Certification Services ...." In its description of its policies Signet suggests that liability levels will vary based on the relevant policy, but this is not currently reflected in its Service Agreement.

VeriSign's subscriber agreement states that VeriSign's CPS places limits on VeriSign's liability and that VeriSign refuses all liability for incidental, consequential and punitive damages. VeriSign's CPS also imposes dollar limits on damages of all types: liability for Class 1 certificates is capped at U.S. $100, for Class 2 certificates at U.S. $5,000, and for Class 3 certificates at U.S. $100,000. The liability caps are intended to apply to the aggregate liability arising from any particular certificate, regardless of how many transactions or parties utilized such certificate. If aggregate damages exceed the liability cap, the CPS states that the "available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction."

As discussed above, COST has indicated its willingness to accept limited liability under its Medium Assurance policy and "full liability" under its High Assurance policy. COST negotiates liability issues directly with customers and does not publicly release the details of its liability policies.

(iii) **Subscriber Legal Duties.**

As noted above, Nortel requires subscribers to indemnify Nortel. No other legal duties are expressly addressed in the Nortel agreement.

Under Signet's service agreement, a subscriber agrees to certain "customer responsibilities" such as "comply[ing] with all reasonable directions and instructions," agreeing not to use or permit others to use the "Certification Services" in order to commit a crime, and taking every reasonable precaution to avoid contaminating any

software or hardware with any "'viruses,' 'worms,' or 'trojans.'" The subscriber also agrees to not disclose any of Signet's confidential information.

Signet's agreement also imposes indemnity obligations upon subscribers for any liability arising out of (a) the use of the Certification Service by the subscriber or anyone authorized to use the service by the subscriber, or (b) "any software or hardware contamination" resulting from the subscriber's use of the service.

Signet's agreement does not mention or discuss any duties a subscriber might have to keep a private key secure or to revoke a compromised key.

VeriSign's CPS attempts to impose a number of legal duties upon subscribers. These duties are sprinkled throughout the CPS, but some of the more significant duties are imposed in portions of Sections 7.2, 7.3, and 7.4:

[T]he subscriber certifies and agrees with the [Issuing Authority (IA)] and to all who reasonably rely on the information contained in the certificate that at the time of acceptance and throughout the operational period of the certificate, until notified otherwise by the subscriber,

(i) each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and the certificate has been accepted and is operational (not expired, suspended or revoked) at the time the digital signature is created,

(ii) no unauthorized person has ever had access to the subscriber's private key,

(iii) all representations made by the subscriber to the IA regarding the information contained in the certificate are true,

(iv) all information contained in the certificate is true . . .

By accepting a certificate, the subscriber assumes a duty to retain control of the subscriber's private key, to use a trustworthy system, and to take reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use. . . .

BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER AGREES TO INDEMNIFY AND HOLD THE IA, VERISIGN, AND THEIR AGENT(S) AND CONTRACTORS HARMLESS FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE, AND ANY SUITS AND EXPENSES OF ANY KIND, INCLUDING REASONABLE ATTORNEYS' FEES, THAT THE IA, VERISIGN, AND THEIR AGENTS AND CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A CERTIFICATE, AND THAT ARISES FROM (I) FALSEHOOD OR MISREPRESENTATION OF FACT BY THE SUBSCRIBER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORIZED BY THE SUBSCRIBER); (II) FAILURE BY THE SUBSCRIBER TO DISCLOSE A MATERIAL FACT, IF THE

MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY OR WITH INTENT TO DECEIVE THE IA, VERISIGN, OR ANY PERSON RECEIVING OR RELYING ON THE CERTIFICATE; OR (III) FAILURE TO PROTECT THE SUBSCRIBER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM, OR TO OTHERWISE TAKE THE PRECAUTIONS NECESSARY TO PREVENT THE COMPROMISE, LOSS, DISCLOSURE, MODIFICATION, OR UNAUTHORIZED USE OF THE SUBSCRIBER'S PUBLIC KEY.

**(c) Legal Relationship Between the CA and Relying Non-Subscribers.**

As discussed in detail in the Report, the nature of the legal relationship between relying third parties and CAs is difficult to analyze. Of the CAs who have publicly addressed the legal questions surrounding certification services, only VeriSign and Signet have directly tackled this particular issue. VeriSign attempts to establish a contractual relationship with relying parties in three different ways. First, when a relying party checks the status of a VeriSign certificate, a statement is inserted just above the online "submit" button: "By submitting this query, I agree to be bound by VeriSign's CPS." Similarly, when one searches the VeriSign site for a particular certificate, the same statement is expressed just above the "submit" button. Additionally, VeriSign certificates have the following information in one field:

www.verisign.com/repository/CPS Incorp. by Ref., LIAB. LTD(c)96

It is unclear whether a binding contract can be formed in such a fashion, particularly in light of the sheer volume of the CPS.

Signet intends to establish direct contractual relationships with relying third parties. Signet's view is that accessing a certificate revocation list (CRL) is an integral part of the process of utilizing a certificate. Third parties who wish to rely on a certificate will enter into a "service agreement" with Signet prior to accessing Signet's CRL. This service agreement will be similar or identical to the service agreement signed by subscribers. Signet expects that Australian legislation will provide that parties who rely on certificates without checking CRLs will bear any resulting loss.

No other CA explicitly attempts to create a contractual relationship with relying parties.

**(i) Warranties to Relying Third Parties.**

If VeriSign forms a contract with relying third parties with the CPS as the contract terms, then the relying party could take advantage of the limited warranties VeriSign offers (described above) but would also be subject to the warranty disclaimers made in the CPS.

Similarly, relying third parties who enter into a service agreement with Signet will benefit from any warranties provided in the contract, but will also be subject to contractual disclaimers of warranties.

Nortel's legal agreement does not address this issue.

**(ii) Liability Limitations.**

As with warranty disclaimers, if VeriSign forms a contract based upon the CPS with relying third parties, then the liability limitations stated in the CPS would be implicated. If the VeriSign/relying third party relationship is not governed by contract, then, as discussed in the Report, only statutorily-imposed limitations of liability would apply.

Signet's relationship with relying third parties will be governed by a traditional contract; presumably any liability limitations in the contract will be enforceable, subject to the provisions of general contract law.

As noted above, both VeriSign and Signet do attempt to limit by contract their liability to third parties through indemnification and by requiring a subscriber to make express representations or warranties as part of a subscriber agreement. If enforceable against parties with sufficient assets, these clauses could shift liability to a subscriber under specified circumstances.

(iii) **Legal Duties.**

The VeriSign CPS imposes few or no legal duties on relying third parties.

Signet's service contract with relying parties will presumably impose similar duties on third parties as it does on subscribers (see Section 3(b)(iii) above). Additionally, Signet expects that Australian legislation will impose certain duties on relying third parties, such as a duty to check the relevant CRL.

No other CA attempts to impose legal duties on relying non-subscribers.

**(d) Key Management Techniques.**

A detailed analysis of the complex technical issues related to key management is not attempted here. Rather, certain key management practices of current CAs will be briefly discussed in an effort to highlight potentially significant legal issues.

**(i) Key Generation.**

Most of the currently-operating CAs rely on browser software to generate key pairs. A subscriber generates a key pair on its own computer using the browser software and transmits the public key to the CA. Thus, the CA never controls the subscriber's private key. In contrast, the USPS plans to issue subscribers a "smart disk" with which they would generate encryption keys.

**(ii) Key Revocation and Validation.**

VeriSign is the only CA which currently offers online key revocation and validation. COST publishes a CRL on its site, but does not publish formal revocation policies.

(iii) **Root Key Authenticity and Security.**

All currently-operating CAs are self-certified. VeriSign is the only CA that has gone to significant lengths to establish the authenticity of its public key. In March of 1996, VeriSign held a well-publicized "key ceremony" that was "designed to provide irrefutable evidence of VeriSign's secure technical and procedural infrastructure," according to a VeriSign press release. No other CA has publicly revealed its security standards; all appear to rely solely on their reputation to establish the authenticity of their self-published keys. The remaining CAs apparently publish their own public key exclusively on their websites.

## ATTACHMENT A:

### Companies and Organizations Offering or Planning to Offer CA Services, Companies Providing CA-Related Software, and Hardware and Other Notable Organizations

| Name of Company / Org. (Country) | Website |
|---|---|
| Atalla (Tandem) (USA) | http://www.atalla.com |
| American Bar Assoc. Information Security Committee | http://www.abanet.org/scitech/home.html |
| BBN Corporation (USA) | http://www.bbn.com |
| CertCo, LLC | http://www.certco.com |
| CivicLink (Ameritech Information Access) (USA) | http://www.ameritech.com/civiclink |
| CommerceNet (USA) | http://www.commerce.net |
| COST Computer Security Technologies (Sweden) | http://www.cost.se |
| Cylink (USA) | http://www.cylink.com |
| Datakey (USA) | http://www.datakey.com |
| DFN-PCA (Germany) | http://www.cert.dfn.de |
| Digital Secured Networks Technologies (USA) | http://www.dsnt.com |

| | |
|---|---|
| Enterprise Integration Technologies (EIT) (USA) | http://www.eit.com |
| EuroSign (UK) | http://www.eurosign.com |
| Federal Security Infrastructure Program (USA) | http://www.gsa.gov/fsi |
| Fischer International (USA) | http://www.fisc.com |
| Frontier Technologies (USA) | http://www.frontiertech.com |
| GMD - TKT.SIT (Germany) | http://www.darmstadt.gmd.de/TKT/security |
| GTE CyberTrust (USA) | http://www.gte.com/Cando/Business/Docs/Software/trust.html |
| Harbinger (USA) | http://www.harbinger.com |
| IBM Net Registry | http://www.internet.ibm.com/commercepoint/registry |
| ICE-TEL Project (Germany; international) | http://www.darmstadt.gmd.de/ice-tel/ice-home.html |
| IETF Public Key Infrastructure Working Group | http://www.ietf.org/html.charters/pkix-charter.htm |
| Internet Commerce Group (Sun Microsystems) (USA) | http://www.sun.com/security/product/ca.html |
| Microsoft (USA) | http://www.microsoft.com |
| Netscape (USA) | http://www.netscape.com |
| NORTEL Entrust (Canada) | http://www.nortel.com/entrust/main.html |
| OnWatch (Bell Sygma) (Canada) | http://www.public-key.com/index.html |
| PGP, Inc. (USA) | http://www.pgp.com |
| Premenos (USA) | http://www.premenos.com |
| Radguard (Israel) | http://www.radguard.com |
| RSA (USA) | http://www.rsa.com |
| Sembawang Media (Singapore) | http://ca.contact.com.sg |
| Signet Systems (Australia) | http://www.signet.org.au/index.html |
| Slovenian Policy Certification Authority (Slovenia) | http://www.e5.ijs.si/cert/sipca_cert.html |

| | |
|---|---|
| Spyrus (USA) | http://www.spyrus.com |
| Terisa (USA) | http://www.terisa.com |
| Thawte Consulting (South Africa) | http://www.thawte.com |
| TradeWave (USA) | http://andromeda.tradewave.com/tradewave |
| Trusted Information Systems (TIS) (USA) | http://www.tis.com |
| UNINETT (Norway) | http://www.uninett.no/pca/index.html |
| United States Postal Service | |

**Appendix 5**

**Selected Bibliography on Certification Authorities and Digital Signature Reference Material**


Theodore Sedgwick Barassi, "The CyberNotary: Public Key Registration and Certification and Authentication of International Legal Transactions," available at http://www.intermarket.com/ecl/cybrnote.html.

Michael S. Baum and Henry H. Perritt, *Electronic Contracting, Publishing and EDI Law* (1991).

Michael S. Baum, *Federal Certification Authority Liability and Policy* (1994). (Published by the U.S. Department of Commerce's National Technical Information Service as Report No. PB94-191202.)

C. Bradford Biddle, "Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure", 33 *San Diego Law Review*(1996), available at http://www.SoftwareIndustry.org/issues/docs-org/digsig.pdf.

Santosh Chokhani and Warwick Ford, "The Certificate Policy and Certification Practice Statement Framework," November 3, 1996, available at http://csrc.ncsl.nist.gov/pki/.

Carl M. Ellison, "Establishing Identity Without Certification Authorities," July 22, 1996, available at http://www.clark.net/pub/cme/usenix.html.

Paul Fahn, "Answers to Frequently Asked Questions about Today's Cryptography, Version 2.0" (September 20, 1993), available athttp://www.rsa.com/pub/faq/faq.asc.

Federal Security Infrastructure Program, NII Federal Information Security Infrastructure Program Management Office Action Plan, October 17, 1995, available at http://www.gsa.gov/fsi/action.htm.

A. Michael Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce", 75 *Oregon L. Rev.* 49 (1996), available at http://www.law.miami.edu/~froomkin/articles/trusted.htm.

Randy Gainer, "Allocating the Risk of Loss for Bank Card Fraud on the Internet", *John Marshall Journal of Computer & Information Law* (Fall 1996).

Michael J. Ganley, "Digital Signatures and Their Uses," 13 *Computers & Security* 385 (1994).

Information Security Committee of the Science and Technology Section of the American Bar Association, Digital Signature Guidelines. October 5, 1995 draft available

at http://www.state.ut.us/ccjj/digsig/dsut-gl.htm. See also April 16, 1996 and August 1, 1996 drafts.

Interagency Working Group on Cryptography Policy, Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure, May 20, 1996, available athttp://www.epic.org/crypto/key_escrow/white_paper.html.

International Chamber of Commerce (ICC) Report, Uniform International Authentication and Certification Practices [not publicly available]

International Telecommunications Union Recommendation X.509 (November, 1993). See http://www.itu.ch/itudoc/itu-t/rec/x.html for more information.

Internetworking Public Key Certification Infrastructure for Europe (ICE-TEL) Project Programme, dated October 1, 1995, available at http://www.darmstadt.gmd.de/TKT/security/ice/public.html[link down as of October 2, 1996]

Steven T. Kent, "Internet Privacy Enhanced Mail," 36:8 *Communications of the ACM* 48 (1993).

Brian Miller, "How to Sign on the Digital Line," Government Technology, June 1995, available at http://www.govtech.net/1995/gt/jun/features/elec.htm.

MITI Report [not available]

National Institute of Standards and Technology, Digital Signature Standard, May 19, 1994, available at http://www.nist.gov/itl/csl/fips/fips186.txt.

Dr. Jim K. Omura, "Digital Signatures and Certificates," available at http://www.cylink.com/products/security/digsig/.

Henry H. Perritt, Jr., "Cyberpayment Infrastructure," 1996 *J. Online L.* art. 6, available at http://www.wm.edu/law/publications/jol.

Bernard D. Reams, Jr., *Electronic Contracting Law: EDI and Business Transactions* (1996-97 Ed.).

Bruce Schneier, *E-Mail Security: How to Keep Your Electronic Messages Private* 98 (1995).

Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2d ed. 1996).

Standards Australia, Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia, SAA MP75--1996.

UNCITRAL Model Law on Electronic Commerce, available athttp://eclips.osc.edu/eclips/undocs/model_law.html.

Utah Digital Signature Act Illustrations, available athttp://www.state.ut.us/ccjj/digsig/dsut-egs.htm.

Utah Digital Signature Act Tutorial on Digital Signatures, available at http://www.state.ut.us/ccjj/digsig/dsut-tut.htm.

VeriSign Certification Practice Statement, Version 1.1 (August 22, 1996), available at ftp://ftp.verisign.com/repository/CPS.

Peter N. Weiss, "Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Towards Developing a Security Policy," 12 *J. Marshall J. Computer & Info. L.* 425 (1993).

Benjamin Wright, *The Law of Electronic Commerce* (2d Ed. 1995).

**Other Useful Digital Signature Resources**

CommerceNet PKI Task Force: http://www.commerce.net/work/taskforces/pki/pki.html.

Florida Department of State: http://www.dos.state.fl.us/digsig/index.html.

Georgia Digital Signature Task Force: http://www.cc.emory.edu/BUSINESS/gds.html.

Kaye Caldwell's Digital Signature page: http://www.SoftwareIndustry.org/software/issues/digsig.htm.

Matrix of State Laws: http://www.magnet.state.ma.us/itd/legal/matrix10.htm.

**Digital Signature Legislation (current to November 15, 1996)**

United States

Arizona Revised Statutes §41-121. Effective April 18, 1996.

California AB 1577. Enacted.

Connecticut General Statutes §19a-25a.

1996 Delaware Laws Ch. 509. Enacted July 12, 1996.

Florida Senate Bill 942. Became law May 25, 1996.

Georgia Digital Signature Act. Pending.

Hawaii Senate Bill 2401. Passed June 17, 1996.

Idaho House Bill 515. Enacted March 1, 1996.

Illinois House Bill 3394. Pending.

Iowa §48A.13. Passed 1995.

Kentucky House Bill 422. Pending.

Louisiana Revised Statutes Annotated §40:2144 (1995).

Massachusetts Electronic Record and Signature Act.

Michigan Senate Bill 939. Pending.

New Mexico Digital Signature Regulations. Proposed.

New York Senate Bill 7420. Pending.

Oregon Senate Bill 992. Died.

Rhode Island House Bill 8125. Pending.

Utah Digital Signature Act.

Washington Senate Bill 6423. Enacted March 29, 1996.

International

Proposed amendments to Articles 14 and 28 of France Law nº 90-1170 of December 29, 1990.

Proposed German Digital Signature Law.

**Relevant Non-Digital Signature Specific Legal Resources**

Uniform Commercial Code Article 2, available at http://www.law.cornell.edu/ucc/2/.

ProCD, Inc. v. Zeidenberg, available at http://zeus.bna.com/e-law/cases/procd.html.

Proposed Uniform Commercial Code Article 2B, available at http://www.lawlib.uh.edu/ucc2b/.

Ultramares Corp. v. Touche. Not available on the Internet.

Magnuson-Moss Act, 15 U.S.C. §§2301-12, available starting at http://www.law.cornell.edu/uscode/15/2301.html.

United Nations Convention on Contracts for the International Sale of Goods, available at http://itl.irv.uit.no/trade_law/documents/sales/cisg/art/.

E.U. Directive on Unfair Contract Terms. Not available on the Internet.

E.U. Directive on Products Liability. Not available on the Internet.

Electronic Funds Transfer Act, 15 U.S.C. §1693 et seq., available starting at http://www.law.cornell.edu/uscode/15/1693.html.

## Appendix 6

## Selected Bibliography on Description of Digital Signatures

This description of digital signatures has been reprinted with permission from Chapter 4 of *Online Law: The Spa's Legal Guide To Doing Business On The Internet* (1996), written by Thomas J. Smedinghoff and the Information Technology Law Department of McBride Baker & Coles and published by Addison-Wesley Developers Press.

To order "Online Law" or other SPA publications, contact the SPA at 1730 M Street, N.W., Suite 700, Washington, D.C. 20036-4510, or call 1-800-388-7478, or visit SPA's home page at http://www.spa.org.

### 1. USING DIGITAL SIGNATURES.

### (a) What is a Digital Signature?

A *digital signature* is an electronic substitute for a manual signature that serves the same functions as a manual signature and more. It is an identifier created by a computer instead of a pen. In more technical terms, a digital signature is the sequence of bits that results from using a one-way hash function to create a message digest of an electronic communication. The resulting message digest is then encrypted using a public-key algorithm and the sender's private key. A recipient who has the sender's public key can accurately determine (1) whether the sequence of bits was created using the private key that corresponds to the signer's public key, and (2) whether the communication has been altered since the sequence of bits was generated. Digital signatures look like an unintelligible string of alphanumeric characters. For example

----BEGIN PGP SIGNATURE----

Version: 2.6.2

owHtWX1sU1UUP+91G+22ysbHDHcBeZAVmq7L9iauNJ@UuhX2soUSpaufVsfu8tby1k
UXTGsGhAgsEY4
h9b+EPBgArBGNSELGpiNEFM5A80xIzEoPiPSEiMRFbPfR/ajW7rlBjR/Zbf0/eed9+5991
77j3ndS9C
WlcIlqe3Dflw45vqJ85+dZ5hPywt6u0jb5zYvRmy2drFnZKT17a/97n/Tt11d8dNmyvqV12K
7jt8Lxf

---END PGP SIGNATURE---

is the digital signature for the following e-mail message:

October 30, 1995

Dear Order Department:

We commit to purchase 10,000 widgets at your price of $175 per hundred.

Ship to: Industrial Products Co.
55 Retail Drive
Chicago, Illinois 60061

Sincerely,

Purchasing Department,
Industrial Products Co.

A digital signature is not a digitized image of a handwritten signature or a typed signature such as "/s/john doe." Moreover, unlike a handwritten signature which is unique to the signer but is presumably consistent across all documents signed, a digital signature is unique for each document "signed." This is because a digital signature is derived from the document itself. As a result, any change to the document will produce a different digital signature.

A digital signature can serve the same purpose as a handwritten signature in that it may signify authorship, acknowledgment, or assent, among other things. However, digital signature also serves important information-security purposes that handwritten signatures cannot. A digital signature allows the recipient of a digitally signed communication to determine whether the communication was changed after it was digitally signed. That is, a digital signature provides assurance about the source and integrity of the communication. Because a digital signature provides assurances as to integrity, it is to this extent superior to a handwritten signature.

**(b) How is an Electronic Communication Digitally Signed?**

Before a sender can digitally sign an electronic communication, the sender must first create a public-private key pair. The private key is kept confidential by the sender and is used for the purpose of creating digital signatures. The public key is disclosed generally by posting the key in online databases, repositories, or anywhere else the recipient of the digitally signed communication can access it.

To digitally sign an electronic communication, the sender runs a computer program that creates a message digest (or hash value) of that communication. The program then encrypts the resulting message digest using the sender's private key. The encrypted message digest is the digital signature. The sender then attaches the digital signature to

the communication and sends both to the intended recipient. A digitally signed communication might look like this:

Subject: Order

Author: rqz@ipc.com

October 30, 1995

---BEGIN PGP SIGNED MESSAGE---

Dear Order Department:

We commit to purchase 10,000 widgets at your price of $175 per hundred.

Ship to:
Industrial Products Co.
555 Retail Drive
Chicago, Illinois 60061

Sincerely,

Purchasing Department,
Industrial Products Co.

----BEGIN PGP SIGNATURE----

Version: 2.6.2

owHtWX1sU1UUP+91G+22ysbHDHcBeZAVmq7L9iauNJ@UuhX2soUSpaufVsfu8tby1k
UXTGsGhAgsEY4
h9b+EPBgArBGNSELGpiNEFM5A80xIzEoPiPSEiMRFbPfR/ajW7rlBjR/Zbf0/eed9+5991
77j3ndS9C
WlcIlqe3Dflw45vqJ85+dZ5hPywt6u0jb5zYvRmy2drFnZKT17a/97n/Tt11d8dNmyvqV12K
7jt8Lxf

---END PGP SIGNATURE---

The digital signature process can be made very easy. With a user-friendly interface, the sender can digitally sign a communication simply by clicking on buttons with a mouse. No special technical expertise is needed. The sender should, however, appreciate the legal effects and consequences of digitally signing an electronic communication.

### (c) Verifying a Digital Signature.

When a recipient gets a digitally signed communication, the recipient's computer runs a computer program containing the same cryptographic algorithm and hash function the sender used to create the digital signature. The program automatically decrypts the digital signature (the encrypted message digest) using the sender's public key. If the program is able to decrypt the digital signature, the recipient knows that the communication came from the purported sender, that is, the recipient has verified its authenticity. This is because only the sender's public key will decrypt a digital signature encrypted with the sender's private key.

The program then creates a second message digest of the communication and compares the decrypted message digest with the digest the recipient created. If the two message digests match, the recipient knows that the communication has not been altered or tampered with, that is, the recipient has verified its integrity.

### (d) Prerequisites for the Use of Digital Signatures.

The effectiveness of the digital signature process depends upon the reliable association of a public-private key pair with an identified person. The discussion thus far has made one critical assumption: that the public-private key pair of the sender does, in fact, belong to the sender. Any assurance of authenticity would be worthless if the public key used to decrypt a digital signature belonged to an impostor and not the purported sender.

Paper signature usually have an intrinsic association with a particular person because they are that person's own handwriting. However, public-private key pairs used to create digital signatures have no intrinsic association with anyone in particular -- they are nothing more than large numbers. When a recipient obtains the public key actually for a digitally signed communication, how can he or she verify that the public key actually belongs to the purported sender? An impostor could have generated the public-private key pair and entered that public key in a public database under the purported sender's name.

The solution to this problem is to enlist a third party, trusted by both the sender and recipient, to perform the tasks necessary to associate a person or entity on one end of the transaction with the key pair used to create the digital signature on the other. Such a trusted third party is called a *certification authority*.

## 2. CERTIFICATION AUTHORITIES.

### (a) Function and Role.

A certification authority (CA) is a trusted third person or entity that ascertains the identity of a person, called a *subscriber*, and certifies that the public key of a public-private key pair used to create digital signatures belongs to that person.

The certification process generally works in the following way. The subscriber:

1. Generates his or her own public/private key pair;

2. Visits the CA and produces proof of identity, such as a driver's license and passport or any other proof required by the CA; and

3. Demonstrates that he or she holds the private key corresponding to the public key (without disclosing the private key).

These three steps in the certification process are likely to vary somewhat from CA to CA. For example, one CA may require a subscriber to appear in person before the CA as part of the second step of establishing the subscriber's identity. Another CA may be willing to rely on a third party, such as a notary, to establish the subscriber's identity.

Once the certification authority has verified the association between an identified person and a public key, the certification authority then *issues a certificate*. A *certificate* is a computer-based record that attests to the connection of a public key to an identified subscriber. A certificate identifies the certification authority issuing it and the subscriber identified with the public key. The certificate also contains the subscriber's public key and possibly other information, such as an expiration date for the public key. To provide assurance as to the authenticity and integrity *of the certificate*, the certification authority attaches its own digital signature to the certificate.

The certification authority then notifies the subscriber that the certificate has been issued so as to give the subscriber an opportunity to review the contents of the certificate before it is made public. It is important that the subscriber be given an opportunity to double-check the accuracy of the contents of the certificate because the subscriber may be bound by any communication digitally signed with the private key that corresponds to the public key contained in the certificate or held liable for misrepresentations to the certification authority.

If the subscriber finds that the certificate is accurate, the subscriber may *publish* the certificate, or direct the CA to do so, making it available to third parties who may wish to communicate with the subscriber. A certificate is published by being recorded in one or more repositories or circulated by any other means so as to make it accessible to all intended correspondents. A *repository* is an electronic database of certificates -- the equivalent of a digital Yellow Pages. A repository is generally available online and may be maintained by the certification authority or by anyone providing repository services. Repositories are generally accessible to anyone.

Repositories contain other important information as well as certificates. If a private key is compromised or lost, such as through loss of the medium on which it is stored or accidental deletion, it is generally necessary to suspend or revoke the corresponding certificate so that others will know not to rely on communications digitally signed with that key. This information is also posted in the repository.

Once a certificate has been published, the subscriber may then append the certificate to any electronic communication. If the recipient wants to verify the connection between the sender and his public key, the recipient can look to the attached certificate for some assurance.

**(b) Who Can Be a Certification Authority?**

Certification authorities may include federal and state governmental entities, private persons or entities licensed to act as certification authorities by a state, and private persons or entities acting as certification authorities for commercial purposes. For example, the U.S. Postal Service has announced large-scale plans to offer services designed to facilitate electronic commerce, including functioning as an all-purpose certification authority. The USPS may be well suited to function as a certification authority: In transactions between companies or individuals, it is an objective third party with an established reputation for credibility. Through its nationwide network of post offices, the USPS can register public keys for applicants who appear in person. This will enable the USPS to provide an added level of security, such as photographs and fingerprinting, to ensure that each registered public key corresponds to a real person, not an alias or an assumed identity.

The Los Angeles Superior Court has established a limited-purpose certification authority in connection with an electronic filing and retrieval system that will rely on digital signatures to assure the authenticity and integrity of electronic court filings. The court will act as certification authority for its own personnel. Private parties authorized by the court will act as the certification authority for attorneys and litigants.

A number of private commercial certification authorities are also currently operating. These include the Net Market Company, an affiliation of shopkeepers on the Internet, and VeriSign, Inc., which issues certificates and provides related services to corporations and individuals for use in digitally signing documents for any purpose. Value-added networks may also serve as a limited local certification authority function for subscribers to their network.

**(c) Verifying a Certification Authority's Digital Signature.**

To provide assurances as to the authenticity of a certificate it issues, a certification authority digitally signs each such certificate itself. Anyone can verify the authenticity and integrity of a certificate issued by a certification authority by verifying the certification authority's digital signature using the certification authority's public key.

Note, however, that anyone who wants to verify authenticity has the same problem with the CA's public key as he or she has with any other public key. How does the person know whether the public key really belongs to the CA? The answer is that the CA has its public key certified by another, higher-level CA, which acts as a certification authority for it. That higher-level CA then digitally signs the certificate it has issued, verifying the connection between the lower-level CA and the lower-level CA's public key. The lower-

level CA may then make the certificate for its key available to anyone who seeks to verify the lower-level CA's digital signature.

The higher-level CA, in turn, needs to have its connection to a public key certified to an even higher-level CA, and so on and on. This process of higher and higher CAs certifying public keys is often referred to as *chaining certificates*.

Of course, the chain has to stop somewhere. Where it stops will depend on the importance of a communication to the recipient. Depending on the nature of the electronic communication, the recipient may not bother to verify the sender's signature, much less the lowest level CA's signature. If the communication is of greater importance, the recipient may trace the certificates up the chain until reaching a certificate issued by a CA he or she knows and trusts.

## 3. PROTECTING THE PARTIES TO THE TRANSACTION.

### (a) Certification Practice Statements.

Unless they are subject to state licensure and regulation, certification authorities generally do not adhere to any uniform standard or procedures for verifying the identities of persons for whom they issue certificates. Thus a digital signature is only as reliable as the certification authority is trustworthy in performing its functions. Consequently, a party needs some way to gauge how much reliance it should place on a digital signature supported by a certificate a particular CA issued. For example, if a certification authority verifies identity based on any single piece of identification, the third party might be more cautious in its reliance than it would if the certification authority requires the subscriber to appear in person with a driver's license and passport and to be fingerprinted.

To help recipients of a digitally signed communication gauge their level of risk, the particular procedure a certification authority follows in issuing certificates may be stated in a *certification practice statement*. A certification practice statement may also include information about the practices the CA follow in its operations and about the details of the security of its system.

Certification practice statements may serve an important function for a certification authority as well. A certification authority that follows its announced practices may be able to avoid a claim that it was negligent in failing to do more to connect a user to a public key.

### (b) Certificate Revocation Lists.

With public-key cryptography, each person has to keep his or her private key confidential and secure. This is easier than two people trusting each other to keep a key secret, as in conventional cryptography; nevertheless, the security of private keys is a problem. It is inevitable that someone's key will be lost or compromised, either through

carelessness or a successful cryptanalytic attack. In addition, there are times -- such as when a person dies; a company goes out of business; or an employee quits, is fired or transferred to a new position -- when a key may no longer be needed or used. Thus, there will be times when a key needs to be revoked before it expires.

A key is revoked by revoking its certificate. The problem is how to notify people that they should no longer rely on a key. The solution to this problem is the *certificate revocation list or CRL*. A CRL is simply a database of certificates of keys that have been revoked before their expiration date. A CRL may be part of the repository maintained by the certification authority. If a private key is lost, compromised, or no longer used for any other reason, the corresponding public key and its certificate would be placed on the CRL. Before relying on a public key, a person should verify its status by checking the CRL.

**(c) Certificate Expiration.**

It is possible for a cryptographic key to be compromised even though its holder conscientiously safeguarded it. With a little luck and a lot of motivation, keys can be broken through what is known as a *brute-force attack*. In a brute-force attack, every possible key is tried until one decrypts the ciphertext. The longer the key length, the longer it takes to try all the possible keys. For example, for a key that is 56 bits long, it would take approximately 10 hours to find the key. For a key that is 128 bits long, it would take $5.4 \times 10^{18}$ years to find the key.

Thus, one way to guard against a successful brute-force attack is to use a long key. Another is to change keys periodically.

As with revoked keys, there must be some way to let people know when a key expires. This can be done simply by including a validity period in the certificate for a public key. Anyone who then consults the certificate for that key will know whether it has expired.

Once a key and its certificate expire, the use simply creates a new key pair and has the public key certified.

Encryption keys generally expire after a relatively short time; this raises the question of how a digital signature can be verified after the public key has expired. For example, if a company enters into a twenty-year lease, how can the integrity of the digitally signed lease be verified when the corresponding certificate has already expired?

One solution is to have the digital signature date/time stamped. The date/time-stamped version of the digital signature could be used years later to enforce the original contract. The date/time stamp would establish the date and time at which the document was signed, and thus establish that at such time there was a valid certificate connecting the signer to the public key.

**Appendix 8**

**Selected Bibliography on Working Group Terms of Reference and Work Plan**

The Development Committee, recognizing the importance of certification authority practices to online commerce, has commissioned a Working Group on Electronic Commerce which is executing, as a demonstration project, the following project.

1. **Business Practices For Certificate Authority Services Terms Of Reference.**

   (Note: Subject to review and further approval)

2. **SCOPE.**

   This project shall have three main components, it shall:

   1. identify issues relating to authenticating Internet electronic commerce transactions using certificate authority services;
   2. review and analyze certificate authorities services and policies;
   3. recommend threshold policies and business practices for electronic commerce certificate authority services.

3. **WORK PRODUCTS.**

   This working group shall produce the following:

   A report on the existing practices of certification authorities with respect to the following issues

   - subscriber authentication
   - certification authority duties to subscribers
   - certification authority duties to relying third parties
   - associated discussion of disclaimers of warranties and limitations of liabilities.

   The report will identify and survey additional issues affecting certification authorities, such as key management policies and obligations and jurisdiction/choice of law issues.

   The report will include:

   - A bibliography of resources and reference materials related to digital signatures and certification authorities.
   - A comparative analysis of selected, existing certification authorities and their practices, plus a list of known certification authorities (and related industry participants).

- A consolidated, non-technical description of digital signatures and their functions, including alternative definitions.

The report will be presented in hard copy, as well as be available electronically. The Working Group will utilize on-line methods for reviewing work product, and engaging in informed dialogues regarding the ongoing activities required to reach the intended work products.

Other Considerations: The Forum must be sensitive to creating an actual or implied bias toward a particular technology (e.g., RSA, DSA, etc.) or certificate authority (e.g., VeriSign, Northern Telcom, etc.) in the staffing of this project as well as the drafting of any documents.

4. **WORK PLAN.**

Certain elements of the work product will be presented to the Development Committee for approval on 16 January, 1997 in London.

The work plan for the Development Period is in development and will be announced on or about 15 October, 1996 and posted to this location.