The original Virtual Voting Rights Initiative never got on the ballot, because I lacked the million dollars needed to qualify it for voter consideration. I followed it up with a similar, but more complicated, Internet voting initiative in 2000. This one was called the "California Internet Voting Initiative," or CIVI. Still lacking the requisite million dollars to put it on the ballot, the CIVI also died. It still exists as a proposal.

California Internet Voting Initiative

(April 28, 2000)

INITIATIVE MEASURE TO BE SUBMITTED DIRECTLY TO THE VOTERS

The Attorney General of California has prepared the following title and summary of the chief purposes and points of the proposed measure:

ELECTIONS. USE OF INTERNET FOR VOTER REGISTRATION AND VOTING. INITIATIVE STATUTE. Authorizes use of Internet for electronic voter registration and for casting ballots in direct primary elections, statewide general elections, special elections, and other public elections. Specifies standards for Internet voting systems. Requires Secretary of State to test and certify voting systems to accredit means of identifying and authenticating voters, to protect voter confidentiality, and to adopt rules and regulations governing Internet voting procedures. Requires counties to offer Internet option to all voters. Criminalizes efforts to interfere with Internet election system; specifies penalties. Preserves traditional voting methods.

Summary of estimate by Legislative Analyst and Director of Finance of fiscal impact on state and local governments: One-time costs to local governments, probably several tens of millions of dollars statewide for initial establishment of Internet registration and voting systems, with ongoing annual costs probably ranging from the millions of dollars to the low tens of millions of dollars statewide. One-time costs to State of developing standards for Internet voting and registration and of implementing other provisions, probably in the tens of millions of dollars, with ongoing implementation costs that could reach several million dollars annually. State costs could be partly offset to the extent that fees are charged to local governments or private vendors seeking accreditation of Internet election systems.

TO THE HONORABLE SECRETARY OF STATE OF CALIFORNIA

We, the undersigned, registered, qualified voters of California, residents of _____ County (or City and County), hereby propose amendments to the Elections Code, relating to voting and petition the Secretary of State to submit the same to the voters of California for their adoption or rejection at the next succeeding general election or at any special statewide election held prior to that general election or otherwise provided by law.

PROPOSED LAW

The California Internet Voting Initiative

SECTION 1. In order to promote broader participation in the state's electoral processes, it is the intent of the People of California in enacting this act to legalize the use of the Internet for voter registration and the casting of ballots in all elections conducted by public entities in California, to establish the right of every California voter to register to vote and vote over the Internet from any platform anywhere providing Internet access, including, but not limited to, homes or offices, and to require that every public electoral

jurisdiction in California provide the means by which voters in that jurisdiction may vote in elections in that jurisdiction by means of the Internet from any platform anywhere providing Internet access, including, but not limited to, homes or offices. To implement this goal, it is the intent of the People of California to do the following:

(a) Authorize the use of the Internet for election purposes, including voter registration and the casting of ballots.

(b) Require the Secretary of State, within 90 days of the enactment of this act, to develop and adopt standards according to which the Internet may be used for these purposes.

(c) Allow for the casting of ballots and the registration of voters by electronic means over the Internet from any platform anywhere providing Internet access, including, but not limited to, homes or offices.

(d) Minimize the wrongful manipulation, fraudulent use, or violations of the integrity of the means by which the Internet is used for these purposes by requiring Internet voting systems to employ suitable technologies and practices, and establish suitable sanctions against those illegal acts.

(e) Adopt a policy of providing all voters with suitable means of identifying and authenticating themselves over the Internet from any platform anywhere providing Internet access, including, but not limited to, homes or offices, in order to perform the electoral functions covered by this measure.

(f) Adopt a policy of providing suitable means of assuring the confidentiality of information communicated under this bill.

SEC. 2. Division 16.5 (commencing with Section 116950) is added to the Elections Code, to read:

DIVISION 16.5. USE OF INTERNET FOR ELECTORAL PURPOSES

CHAPTER 1. GENERAL PROVISIONS

16950. Notwithstanding any other provision of law, a qualified voter in this state may register to vote and/or vote in a direct primary, statewide general, special election or any other public election conducted by the State of California or any electoral subdivision thereof, using the Internet, from any platform anywhere providing Internet access, including, but not limited to, homes or offices, using means that have been approved pursuant to Chapter 2 (commencing with Section 16955).

16951. For the purposes of this division:

(a) "election services" means voter registration and the casting of ballots.

(b) "ballot" means an electronic record containing all of, and only, the candidates for local, state, or federal office, and the state and local measures for which the voter is entitled to vote, in whatever order is mandated by law.

(c) "physical polling place" means a traditional, walk-in polling place.

(d) "system for delivering election services over the Internet" means an assemblage of computer hardware, computer software, and network resources, together with the internal processes and operational procedures whereby these components are utilized to deliver election services.

(e) "casting of ballots" means voting.

(f) "system availability" means the percentage of the time during which a system responds appropriately to legitimate and authorized requests.

(g) "master ballot information" means instructions for properly constituting the contents of ballots for the voters in a particular jurisdiction or set of jurisdictions.

(h) "the Internet" means the global, inter-connected network of networks originating from the ARPAnet.

(i) "over the Internet from any platform anywhere providing Internet access" means that voters may exercise their rights under this initiative to register to vote or vote from any device or by any means, now in existence or to be later invented or discovered, which allows them to access an Internet website through which they perform these activities, no matter where that device or means is located.

(j) "homes or offices" means places of residence, whether principal or not, including, but not limited to, single-family homes, condominiums, rental units, hotels, motels, and trailer parks, and places of work, including but not limited to, business offices, satellite and telecommuting workplaces, home offices, retail establishments, restaurants, medical offices, hospitals, or any other location, building, or place wherein any person, at any time, works.

(k) "public electoral jurisdiction" means any government agency responsible for carrying out public elections. Such agencies include, but are not limited to: the State of California, each of the state's counties, charter cities, general law cities, community college districts, and special districts.

16952. Unless a provision of this division expressly requires otherwise or is inconsistent with another provision of this code, each provision of this code that would otherwise regulate the casting of ballots, counting and reporting of ballots or registration of voters shall apply to this division, including, but not limited to, any civil or criminal penalties associated with those activities, any duties imposed on state or local elections officials, and any established timeframes.

CHAPTER 2. ESTABLISHMENT OF STANDARDS FOR INTERNET ELECTION SYSTEMS

16955. The Secretary of State shall establish standards for the use of the Internet for electoral purposes and shall approve and certify for use for these purposes systems that meet the criteria set out in Section 16956.

16956. To qualify for use in an election, a system intended for such use shall demonstrate the existing capacity to do all of the following:

(a) Provide for the secure identification and authentication of each eligible voter utilizing the system.

(b) Provide for the secure identification and authentication of all elections officials, electoral jurisdictions and of all network servers, application servers and all other relevant components of the computing base used for elections by the elections officials and electoral jurisdictions supervising and responsible for voter registration or voting, as appropriate.

(c) Protect the confidentiality and integrity of each voter's ballot.

(d) Provide for the effective disassociation of the content of a voter's cast ballot from the identity of the voter casting it.

(e) Prevent the casting of multiple ballots in any election or multiple registrations as a voter by any person.

(f) Provide protection against tampering, fraudulent use, illegal manipulation, or other abuse by voters, elections officials, any other government agent or official, or any other individual, group, organization, or association of persons.

(g) Be easy to use by the voters using it and by the elections officials operating it.

(h) Provide each voter using it to vote with a ballot containing all of, and only, the candidates for local, state, or federal office, and the state and local measures for which the voter is entitled to vote, in whatever order is mandated by law.

(i) Provide the means by which voters may cast write-in votes in electronic form for candidates whose names do not appear on the ballot but who have qualified for write-in status.

(j) Provide at least 98 percent system availability during the electronic voting period established by law and for as long after the close of the voting period as is required in order to assure the full and complete communication of all voting information.

(k) Be sufficiently scalable to provide voting access to all voters in the jurisdiction where it is employed, during the same hours when physical polling places are open for voting on election day.

(l) Be accessible to all voters, including all voters with disabilities, consistent with the Americans with Disabilities Act of 1990 (42 U.S.C. Sec. 12101 et seq.).

(m) Be capable of being upgraded as technology improves.

(n) Provide support for non-repudiation of all electronic electoral transactions involving voter registration and the casting of ballots between and among voters, elections officials, and electoral jurisdictions.

(o) Be readily available for an audit of its contents, results, and process by a competent accounting firm at a level sufficient to assure the integrity of the system according to generally-accepted accounting principles.

(p) Be capable of securely transmitting information over a network.

(q) Be capable of hosting and operating an Internet website that can securely and accurately carry out all the election functions authorized in this division to be conducted over the Internet (voter registration and voting) and of securely and accurately transmitting all elections data (including that from registration forms and ballots) collected and processed by it in performing these functions to the appropriate election authorities.

(r) Be capable of conducting recounts of ballots.

(s) Be capable of issuing electronic receipts to users to memorialize their registration and voting.

16957. (a) Before any system for delivering election services over the Internet may be used by voters, the Secretary of State shall perform the tests necessary to establish that the system in question conforms to the requirements of Section 16956 and the standards adopted by the Secretary of State pursuant to this division. The Secretary of State may contract with a recognized independent testing facility to perform the tests required by this section.

(b) The Secretary of State, or a recognized testing facility designated by the Secretary of State to perform the tests required by this section, shall examine each system proposed for use in the delivery over the Internet of election services and either accredit that it is fit for use or deny it accreditation within 90 days of its submission to the Office of the Secretary of State or to a testing facility designated by the Secretary of State to perform the tests required by this section.

(c) If approval is denied, the denial shall specify in writing the reasons for the denial and what specific remediations or modifications must be made to the disapproved system in order for it to qualify for subsequent accreditation.

(d) The Secretary of State, or a recognized testing facility designated by the Secretary of State to perform the tests required by this section, may, at their discretion, require a fee to be paid by the owner of the system sufficient to cover the reasonable costs of testing it for compliance with the requirements of this section.

(e) Once the Secretary of State has accredited a system for use in the delivery of election services over the Internet, it shall be designated as accredited by the Secretary of State for use by voters and all electoral jurisdictions within the state and may, immediately upon this accreditation, be used for this purpose.

CHAPTER 3. ESTABLISHMENT OF MEANS TO IDENTIFY AND AUTHENTICATE VOTERS

16960. The Secretary of State shall identify and accredit means by which voters are able to identify and authenticate themselves over the Internet in order to securely access and use the election functions covered by this measure (voter registration and voting). These means may include, but are not limited to, the use of digital certificates and signatures, other electronic signature methods, or biometric means, including voice, iris, or retinal scans, fingerprints, or DNA prints.

CHAPTER 4. VOTER REGISTRATION OVER THE INTERNET

16962. (a) The Secretary of State shall develop and adopt rules and regulations for the registration of voters over the Internet, from any platform anywhere providing Internet access, including, but not limited to, homes and offices, using one or more of the means of identification and authentication approved by the Secretary of State pursuant to Section 16960. The purpose of the rules and regulations developed and adopted by the Secretary of State under the provisions of this section shall be to make the process of registering voters over the Internet herein mandated as fair, honest, convenient, and accessible as possible.

(b) These rules and regulations shall assure that information used for the purposes of voter registration will be transmitted accurately, securely, and confidentially over the Internet.

(c) The chief elections officer in each county shall make available to all eligible citizens within that county the means by which they may, from any platform anywhere providing Internet access, including, but not limited to, homes or offices, register to vote.

(d) County and other elections officials may, at their discretion, make available the means to register to vote to all eligible citizens over the Internet from any platform anywhere providing Internet access, including, but not limited to, homes or offices, using their own staff and equipment or they may contract for the use or purchase of such means with one or more owners of accredited systems for delivering election services over the Internet. When a county chooses to itself provide the means to register to vote over the Internet from any platform anywhere providing Internet access, including, but not limited to, homes or offices, the system it creates and uses to deliver this service must meet the same standards set out in Chapter 2 of this Section and be approved for that purpose by the Secretary of State or a recognized testing facility designated by the Secretary of State to perform the tests required in Chapter 2 of this Section.

(e) Any attempt, successful or otherwise, to fraudulently register to vote over the Internet shall be prosecuted and punished in accordance with all existing laws against fraudulent voting registration, with additional penalties added according to the provisions of Sec. 16995 below.

CHAPTER 5. VOTING OVER THE INTERNET

16965. The Secretary of State shall develop and adopt rules and regulations for the casting of ballots over the Internet, from any platform anywhere providing Internet access, including, but not limited to, homes and offices, using one or more of the means of identification and authentication approved by the Secretary of State pursuant to Section 16960. The purpose of the rules and regulations developed and adopted by the Secretary of State under the provisions of this section shall be to make the Internet voting process herein mandated as fair, honest, convenient, and accessible as possible. These rules and regulations shall, at a minimum, assure that:

(a) the transmission of master ballot information from local elections officials into Internet voting systems and ballots cast over the Internet to local elections officials shall be done accurately, securely, and confidentially over the Internet.

(b) the system being used by a public electoral jurisdiction to provide Internet voting services shall provide a ballot to each voter choosing the Internet voting option that contains all of, and only, the candidates for local, state, or federal office, and the state and local measures for which the voter is entitled to vote.

(c) the identity and authenticity of the Internet voting system being used by voters is definitively established for each voter as part of the voting process.

(d) the ballots cast by, or at the instigation or direction of, any person attempting to cast more than one electronic ballot, or an electronic ballot and one or more other ballots at a physical polling place, by mail-in absentee ballot, or by any other means of voting, now or later to be authorized, with the intent to violate the integrity of the Internet voting system by casting one or more fraudulent ballots, or to unlawfully cast the electronic ballot of another voter, shall be disqualified.

16969. (a) Elections officials in every electoral jurisdiction, including, but not limited to, every county, shall make available to all eligible citizens within their jurisdiction the means to vote over the Internet from any platform anywhere providing Internet access, including, but not limited to, homes or offices, in all elections conducted by and within any electoral jurisdiction.

(b) County and other elections officials may, at their discretion, provide the required systems for voting over the Internet using their own staff and equipment or they may contract for the use or purchase such systems with one or more owners of accredited systems for delivering election services over the Internet. When a county chooses to itself provide the means for the casting of ballots over the Internet, the system it creates and uses to deliver this service must meet the same standards set out in Chapter 2 of this Section and be approved for that purpose by the Secretary of State or a recognized testing facility designated by the Secretary of State to perform the tests required in Chapter 2 of this Section

16971. Any voter may vote using an accredited system for delivering election services over the Internet selected by the electoral jurisdiction in which they are registered to vote, using one of the means of identification and authentication approved by the Secretary of State pursuant to Section 16960, from any platform anywhere providing Internet access, including but not limited to, homes and offices, during either:

(a) The same time period during which absentee ballots are accepted in that jurisdiction, or

(b) The same hours provided for voting at physical polling places on the day elections are held in that jurisdiction.

CHAPTER 6. ADDING BALLOTS CAST OVER THE INTERNET TO NON-INTERNET VOTES TO CALCULATE OVERALL TOTALS

16975. At each election, each public electoral jurisdiction shall tabulate the results of the ballots cast by voters within its jurisdiction over the Internet and add these results to its non-Internet voting totals to calculate the overall results.

CHAPTER 7. CONTINUATION OF NON-INTERNET-BASED ELECTION SERVICES

16991. Nothing in this division may be construed to relieve local elections officials from providing registered voters, who so choose, with the opportunity to cast ballots in the manner required by other provisions of this code or to continue to register voters, who so choose, in the manner required by other provisions of this code.

CHAPTER 8. PENALTIES

16995. Any person who interferes with the lawful operation of any electoral activity conducted electronically pursuant to this division with the intent of committing fraud or violating the integrity of any system used for these activities, including its internal code, contents, or results, is guilty of a crime for each occurrence, punishable by imprisonment in the state prison for 16 months or two or three years, or in a county jail for not more than one year, or a fine of not more than ten thousand dollars ($10,000), or by both that imprisonment and fine. In addition, as a condition of parole, any individual found guilty of a crime pursuant to this section may be prohibited from using any electronic network for a period of not more than the term of parole.

CHAPTER 9. DEFENSE OF THIS INITIATIVE

16996. The proponent(s) of this initiative shall have standing to defend this measure in court.
16997. Any challenge to this measure shall originate in the California Supreme Court.

SEC. 3. The Legislature shall amend and revise the Elections Code or any other related provision of law as necessary to further the implementation of Division 16.5 (commencing with Section 16950) of the Elections Code within the timeframes set forth in that division.

SEC. 4. The provisions of this measure are severable. If any provision of this measure or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

In June of 1999, I published an article in the "Policy Briefing" section of the website of the Progressive Policy Institute entitled, "Jump-Starting the Digital Economy (with Department of Motor Vehicles-Issued Digital Certificates)."

Jump-Starting the Digital Economy (with Department of Motor Vehicles-Issued Digital Certificates)

(June, 1999)

By Marc Strassman and Robert D. Atkinson

The emerging digital economy promises high-productivity, low-unemployment, and increased standards of living. However, citizens, companies, or governments will be unable to fully realize these benefits until individuals can easily and securely authenticate themselves over the Internet.

Currently, few Americans can do this; that is, they are unable to fully represent themselves over the Internet in a way that securely tells other people and companies that they are who they claim to be and allows them to be taken seriously when they state their intentions. As a result, few companies or governments have developed applications that could use online authentication; and likewise, since few online applications require authentication, consumers have little reason to obtain the means to sign documents digitally. The Progressive Policy Institute (PPI) proposes that state governments should help jump start this process by providing digital certificates to all citizens who want them through state Department of Motor Vehicles (DMV) offices.

Just as we couldn't do business of any kind--educational, commercial, or interpersonal--if everyone walked around under a mask, it will be impossible to take full advantage of the Internet's power to collect, store, and distribute information, and therefore conduct various types of transactions, until each of us can authenticate ourselves online.

Authentication is an issue not unique to the Information Age. Medieval princes could secure and authenticate their documents with hot wax and a signet ring, ensuring that the message could not be tampered with without the recipient knowing it. Today, corporations and governments use official stamps and seals to signify the authenticity of the documents they issue. Similarly, digital signatures can be used to identify and authenticate documents and other files transmitted over the Internet.

The analogy between hot wax and signet rings and digital signatures is really very close. The engraved images on the signet rings were the product of some of that time's most advanced technology, engraving and metal work. Only the rich and powerful had access to the tools to insure the security and privacy of their data transmissions.

While digital signatures are based on an idea similar to the medieval signet rings, unlike the rings, digital signatures are potentially available to everyone. Using some of the latest computer and encryption technologies, digital signatures reduce a message to gibberish

when it is tampered with, making it clear that the integrity of the document has been compromised, and allowing the recipient to disregard it.

Digital signature technology can be used to transfer into cyberspace the same, or a higher, level of assurance for legal and commercial purposes than has existed in common law, statutory law, and Uniform Commercial Codes for non-cyberspace transactions. By unambiguously and definitively establishing that a certain document has been "signed" by someone--or that someone has stated, indicated, and memorialized his or her intent to enter into an agreement of some type--digital
signature technology makes it possible for binding transactions that cannot be repudiated to take place at a distance electronically. In short, digital signature technology enables today's e- commerce (online retailing) to flower into e-business and e-government (online transactions of a wide range).

What Are Digital Certificates and Digital Signatures?

To understand the applications and implications of digital certificates and digital signatures, it is important to understand what they do and how they do it.

First, think of the digital certificate as a pen used to write a digital signature. It is a unique digital code--a sequence of letters and numbers--that exists on a person's computer or smart card and enables online identification. Certificates are provided by private companies that serve as certificate authorities (CA).

Then, think of a digital signature as the online equivalent to a signature you write with the pen. It is an encrypted and uniquely identified transmission that is attached to a signed document that becomes unintelligible if tampered with.

Here's how it works:

A person's digital certificate resides on their computer hard drive (or smart card). When a user wants to send a secure message or make any kind of online transaction requiring a digital signature, all he or she needs to do is access their certificate by clicking the appropriate icon on their Internet browser and entering their unique password. Employing the user's certificate, the computer will digitally "sign" a digest (an attachment to the document that the computer encrypts, or scrambles, using the sender's digital certificate). The signature is then added to the core document along with a "public key" that enables a certificate authority (CA), a trusted institution charged with supervising this process, to authenticate the signature.

When the message is received, the recipient checks with the CA to determine if the public key he or she has received is in fact the proper public key of the person sending the message. The recipient can then be assured that the message has indeed been "signed" with the claimed sender's digital signature. All of this, fortunately, is done by the computers in the background and is invisible to the user.

Using unique digital certificates to create digital signatures also allows both the sender and recipient to know for certain that the received message is identical to the sent message and that it hasn't been tampered with between its transmission and receipt.

It is important to note that the use of encryption for authentication does not raise the same law enforcement policy concerns presented by the use of encryption for confidentiality since only the digest, and not the message, is encrypted, and because the digest can be read by anyone using the sender's public key.

Online Authentication is Critical in Driving the Next Wave of E-Business and E-Government

Today, virtually all of the approximately $80 billion in annual consumer-based e-commerce involves transactions that do not require the user to authenticate him or herself. For example, buying a book from Amazon.com does not require that a person prove to Amazon that they are who they say they are; it simply requires that they provide a valid credit card number.

However, for a truly digital economy to fully emerge and provide the kinds of productivity and standard of living increases that are possible, a host of functions now conducted in-person or on paper must be able to migrate to cyberspace where transaction and processing costs will be a fraction of their current levels. For example, applying for a bank loan by phone costs $5.90, but using the Internet costs 14 cents. Similarly, the cost of a teller transaction at a bank is $1.07, while online it is one cent, and filing taxes online is at least 60 percent cheaper than filing paper copies.

A whole host of functions will depend on digital signatures if they are to be conducted online efficiently and on a widespread basis. These include applying for a loan or insurance; filing legal documents; applying for a permit, driver's license, passport, or other official government document; paying taxes; and even voting electronically. In short, a large share of transactions that now require our signatures for some form of identification could migrate to cyberspace--but only if digital certificates are in widespread use.

Yet, important as digital certificates and digital signatures are to the full development of e-business and e-government, they are not yet widely in use or even widely discussed. Melissa the MacroVirus got more publicity in three days recently than digital certificates have received in the last three years. The main reason for this is that digital certificates and their relation to digital signatures are neither self-evident nor easy to understand. As a result, the media tend to shy away from the subject.

The complexity of these tools and the relative difficulty of obtaining them have meant that few people do have them. Without widespread adoption by consumers, and with businesses apparently proceeding satisfactorily without them, few companies or governments have developed applications that could use online authentication. Likewise, since there are few online applications that require authentication, consumers have little

reason to obtain these certificates. Moreover, putting digital certificates on smart cards (a credit card-shaped piece of plastic that contains a microprocessor for performing calculations, and a certain amount of computer memory for storing data) only becomes a viable proposition if there are sufficient smart card readers in use to attract enough users to support them. The chicken-and-egg metaphor is the simplest way to describe the problem. The overall result is the one we confront now: hardly any smart cards or digital certificates are in use anywhere in the United States.

Nevertheless, increasingly powerful applications will become possible as we move deeper into the Information Age, and many of them can only be put in place, or put in place effectively, by using smart cards, digital certificates, and digital signatures.

Accelerating the Adoption of Digital Signatures

As powerful and useful as digital signature technology is, there are certain obstacles standing between where it is now and where it could be. Principally, there is the problem of properly issuing the digital certificates upon which the entire system depends. Candidates for digital certificates, like applicants for driver's licenses, passports, or green cards, need at some point to present themselves before trusted authorities and establish their identity, either on the basis of a personal relationship with the trusted authority, or by presenting various types of documents that allow them to receive a digital certificate in their own name.

Some say that the provision of digital certificates should be completely left to the private sector. Clearly, the private sector needs to provide the technology, but it can also do this in partnership with government, the same way the private sector helps the government accomplish many of its tasks, from supporting a strong national defense to building roads.

Perhaps the most compelling reason why a government role is necessary for a robust implementation of digital certificates relates to the very significant economic benefits derived from breaking out of the chicken-or-egg conundrum faster than market forces alone are likely to be able to do. In particular, the lack of knowledge of digital certificates--combined with the cost and inconvenience involved in asking millions of citizens to present themselves to separate "digital certification" agencies to establish their identity and apply for a digital certificate--means that the use of digital certificates will develop only slowly, at best.

Not only will this mean that a host of e-business applications will be slow to develop, the same will also be true for many e-government applications. Perhaps the strongest motivation for states to make it easy for citizens to obtain digital certificates is that these will go a long way in enabling the electronic delivery of government services. If citizens could use their digital certificates to interact with state and local governments, the efficiencies resulting from online and electronic transactions would allow government to more than recoup the costs associated with providing the certificates. For example, citizens could apply for licenses and permits, file taxes, submit regulatory and other legal

forms, and even vote online. Not only would state and local governments save millions, but citizen satisfaction with government would increase.

Fortunately, there already exists in every state and almost every community an agency whose job it is to establish and verify the identity of persons, and to capture that identity with a picture. This agency collects and stores what those in the identification business call "biometric indicators," such as height, weight, eye color, and hair color. They test your vision. They ask for your address. They make sure they know when you were born.

The Department of Motor Vehicles is already collecting quite enough information about each person to issue him or her a digital certificate. In fact, one can argue that it is the DMV that plays the baseline function of establishing authentication in the physical world. DMVs issue millions of driver's licenses and non-driver identification cards every year that people use to establish their identity in a myriad of applications. There is no reason why they shouldn't play this role in the cyber world. In fact, VeriSign, a leading provider of digital certificates, states: "Think of Digital IDs as the electronic equivalent of driver's licenses or passports that reside in your Internet browser and e-mail software." And indeed, the level of technological sophistication of the cards that embody these licenses varies from state to state.
In many states, such as California, these cards include a magnetic strip, a digitized photo, and a surface hologram, designed to thwart illegal modification of the card or the data it holds.

Given that state DMVs already have sufficient data to issue digital certificates, that they already issue cards used for identification, and that they already employ sophisticated electronic and anti-tampering technologies, these agencies are well positioned to issue digital certificates as part of their ongoing citizen identification and certification functions. And since they already carry out their work on a rolling basis, with staggered renewals of their cards designed to balance the work flow, expanding their role to one of establishing identity in the cyber world would mean a gradual and smooth introduction of this technology.

To maximize the usability of such Government-Issued Digital Certificates (GIDCs), every citizen/customer/user who elects to could receive their driver's license on a smart card, which in addition to a photo and printed information on its surface, would also contain a microprocessor and have the capacity to accept and store a digital certificate. Citizens/users would select their own passwords and--from their own computer at home or at work, or from a publicly provided one in a school, library or kiosk--generate and download their own unique digital certificate and private key.

This digital certificate would be a general-purpose digital certificate. There would also be room in the smart card for the user to allow other institutions, organizations, and companies to add "cardlets" that would entitle the cardholder to access his or her HMO records, to download e-cash, or to vote in elections. In order to assure security, these cardlets would be acquired by the holder on the basis of their general purpose digital

certificate and whatever additional information other organizations or individuals required for access to specific databases or transaction opportunities.

People without computers could still use the digital certificates in their smart cards in various offline ways, such as for applying for government permits at a public computer kiosk. Credit card companies would perhaps become one of the organizations providing specialized cardlets for the smart cards. The potential of smart cards loaded with digital certificates to improve access, cut costs, and improve the efficiency of transactions that individuals conduct in the physical world is significant.[1]

In addition to providing the digital certificate to everyone on his or her driver's license or smart card, the state could also make the certificate containing the private key available directly to users to store on their computer(s) at home or at work, or both.

Likewise, this baseline authentication could be used to acquire other certificates that could be used for other purposes. Just as the driver's license is not the only means of personal identification, particularly for transactions with greater potential liability, other digital certificates issued by the private sector would also be used. With both smart cards and browser-based digital certificates, users would have private passwords that would prevent others from using their certificates to impersonate them in cyberspace.

As for the risk and liability questions surrounding the issuance and use of digital certificates in smart cards, there is a "defense in depth" approach that can effectively address this issue.

To start with, smart card and digital certificate users ("subscribers," in the industry jargon) are allowed to make up their own passwords. This reduces their need to write them down on their card. If they do make this mistake, and if their card is stolen and used fraudulently, the subscriber is liable, since the card issuer exercised due diligence in seeing that it would not be misused. However, since the leading digital certificate system employs a Certificate Revocation List (CRL) technology, once one of their subscribers reports his or her card lost or missing, it can be revoked immediately, and anyone trying to use it will not be able to do so. This is like revoking a credit card, only faster and more certain.

The ability to instantly revoke a certificate also comes into play in the case of cards that are stolen and then attacked to discover their password. In addition to the revocation protection, the cards themselves are resistant to forced intrusion. Ten thousand computers working simultaneously for 22 hours are required to break a 56-bit key. Current cards employ 128-bit keys, and future versions will feature 256-bit keys, so it will take much longer to intrude into these--far longer than the time it takes to revoke the card entirely.

As for the previously mentioned private-sector participation, it makes sense for each DMV to outsource the actual provision of the digital certificates and the smart cards, as well as the management of the certificates, to one or more private companies with established track records in developing, deploying, and managing digital signature

technology. In the same way that state governments hire private companies to supply copying or phone services, or even today's driver's licenses, they would contract with established digital signature technology companies to provide the necessary components required to introduce and maintain the processes that constitute the digital signature system. Moreover, they could choose whatever parameters and technologies for authentication they think work best and are most cost-effective. In fact, different states may use different technologies.

Finally, the fact that DMVs would issue these cards would in no way prevent individuals who would rather obtain certificates from private providers from doing so. Rather, it would simply make it easier for individuals to obtain them. In addition, just as individuals now use multiple forms of identification (such as passports, birth certificates, and witnesses) for certain transactions--especially more sensitive ones (e.g., papers that need to be notarized)--some individuals would likely obtain multiple digital certificates that could be used in combination or individually, but the DMV-issued certificate serving as a baseline.

A Threat to Privacy?

Aren't digital certificates a step toward a national ID or a potential threat to privacy? Personal privacy has long been a core American value, and the proliferation of modern database technology has done nothing to eliminate this concern. In fact, it has only made it a more pressing matter.[2] Banks, merchants, HMOs, and the government all possess a lot of data about us and our habits, a fact that will not change in the presence or absence of a satisfactory means of issuing digital certificates.

Moreover, obtaining digital certificates from the DMV would be voluntary, and the state government would not itself serve as the certificate authority or know the passwords individuals choose to access the certificates. Also, just as driver's licenses are issued by states and not the federal government, under this proposal states would also issue digital certificates.

Finally, just as there are some transactions in the physical world that are anonymous and some that require identification, the same is true in the cyber world. Through the process of "anonymous authentication"--developed to allow voters to be authenticated online while maintaining the confidentiality of their electronic ballots and preventing their choices from being personally associated with them--other subscribers can also authenticate themselves as necessary while preserving certain aspects of anonymity in various other types of transactions. It will be important for state and local government to not require personal identification online when simple authentication will do. For example, a county may require that someone prove they are a resident before accessing a data base. In this case, a digital certificate would certify only that the person is a resident without revealing his or her identify. Fortunately, the technology is flexible enough to easily accomplish this. In addition, DMVs and the private digital certificate providers should establish a code of privacy that keeps the data they collect private. Overall, clearly

thought out and reasoned government policies should prove sufficient in most cases to address these and other similar concerns.

Summary

It would not be an abrupt change for state DMVs to begin issuing driver's licenses on smart cards, and to provide the means for each citizen who wants to to create and store a digital certificate on that card. It would be, instead, an incremental modernization which will set the stage for a rapid advance in efficiency and cost-saving within state government, for an explosion of e-commerce, and for the facilitation of countless everyday tasks for every certificate holder.

Endnotes

1. For example, one potential application for smart cards would be to enable consumers to register online for hotel reservations, and download the room key code to their smart card, which could then be used to enter the room without registering at the front desk.

2. See Randolph H. Court and Robert D. Atkinson, Online Privacy Standards: the Case for a Limited Federal Role in a Self-Regulatory Regime, Progressive Policy Institute (March 1999).

Marc Strassman is the chief proponent of the Digital ID Initiative.

Robert Atkinson is director of the Progressive Policy Institute's Technology, Innovation, and New Economy Project.

In March of 2000, I drafted a proposal to enact the recommendations of this think-tank piece into law.

Request to California's Office of Legislative Counsel to Draft an Initiative to Provide All Californians with Digital Certificates and Smart Cards to Hold Them

(March 11, 2000)

Request to Office of Legislative Counsel for the Drafting of an Initiative mandating that the Department of Motor Vehicles furnish all Californians with state-of-the-art smart cards pre-loaded with unique digital certificates and contract private industry to establish and maintain a Certificate Authority capable of managing these certificates

We, the undersigned registered California voter(s), hereby respectfully request that the Office of Legislative Counsel draft for us a proposed initiative measure that would have the following effect:

Section 1. It is the intent of the People of California in enacting this bill to mandate that the Department of Motor Vehicles adopt a policy of issuing driver licenses and state identification cards on state-of-the-art smart cards, these smart cards to be pre-loaded by the State with unique digital certificates. It is the further intent of the People of California that the State contract with private industry to establish and maintain a Certificate Authority capable of managing these certificates, and that no additional user fees be imposed on citizens for the provision of these smart cards and digital certificates, or for the transition to these new technologies, apart from the normal and customary fees already being charged for such cards in their "legacy" versions at the time this legislation is enacted.

To implement this goal, it is the intent of this bill to order: a. the Department of Motor Vehicles to provide all holders of driver licenses and state identification cards with state-of-the-art smart cards, such cards to include on or in them:

(1) all the data, insignia, seals, digitized photos, watermarks, holograms, etc., that are contained on the current version of these cards

(2) a magnetic stripe on the reverse side of the card, containing all the data now contained in that strip

(3) a microprocessor and computer memory capable of holding and using enough data to allow the card to be used for the normal range of purposes achievable by the latest and most-powerful smart cards, including, but not limited to, personal identification and authentication; access to physical locations; the paying of tolls and other transportation

charges; making phone calls from stationary pay phones; activating, securing, and being billed for the use of cellular phones; downloading and storing e-cash; making credit card purchases in the physical world and over the Internet (or other public or private computer network); conducting banking transactions over the Internet (or other public or private computer network), or with a teller on bank premises, or with an ATM; accessing one's own medical records online; doing any business whatsoever with the state government; and registering to vote, signing initiative and in lieu petitions, and voting in any and all elections conducted under the jurisdiction of the State of California over the Internet.

(4) a current, valid, unique digital certificate of at least 128 bits in length, including a private encryption key capable of securely digitally signing electronic documents.

(5) in order to enhance the general functionality and usefulness of these smart cards, the Department of Motor Vehicles should select, prepare, and issue smart cards capable of both "contact" and "contactless" use. Consideration should be given to working with industry leaders to create and use an "opti-smart card," that would employ laser-based mass optical storage capability in addition to the combined contact and contactless interface modalities required under this legislation.

b. the Department of Motor Vehicles will provide such a smart card containing digital certificates to all applicants applying for or receiving driver licenses or state identification cards beginning no later than 60 days after the enactment of this legislation.

c. the Department of Motor Vehicles shall begin a process of replacing all existing driver licenses and state identification cards with smart cards containing digital certificates no later than 90 days after the enactment of this legislation and shall complete this replacement process within 180 days after the enactment of this legislation.

d. the Department of Motor Vehicles shall, in addition to providing card holders with a copy of their unique digital certificate in the smart card provided to them, request from all cardholders and accept from each cardholder who desires the service herein referenced, one or more (up to five) e-mail addresses under their control or to which they have access, and send by e-mail to these addresses a current copy of the same digital certificate included in that person's smart card, in order to allow the cardholder to easily place their certificate on the hard drive of their computer, load it onto a floppy disk, or otherwise store it in order to maintain the security of the data and enhance their own convenience in its management.

Section 2.

The State of California shall enter into contracts with one or more established and generally-recognized providers of smart cards to obtain, prepare, load with digital certificates and distribute in a timely way to those entitled to them by this legislation the smart cards herein referenced.

Section 3.

The State of California shall enter into contracts with one or more established and generally-recognized providers of digital certificates to provide sufficient quantities of unique digital certificates (including private encryption keys of no less than 128 bits in length) to provide one such digital certificate to each new and current holder of a state-issued driver license or state identification card. Either the state shall secure for itself, and hence for the smart card holders, certificates good in perpetuity, or the state shall enter into such contracts as are required to provide such perpetual validity for the certificates, including undertaking to renew the certificates in a timely way under whatever arrangements may be required to effect such perpetual validity, at the State's sole expense.

Section 4.

The State of California shall assume the responsibility to see that the digital certificates referenced in Section 3 shall be properly loaded into the smart cards referenced in Section 2 (although it may, at its discretion, delegate this responsibility to the provider of the smart cards, the provider of the digital certificates, or to both jointly, with their concurrence).

Section 5.

The State of California shall assume the responsibility to see that the smart card/digital certificate combination in its entirety shall be safely and securely delivered, by USPS mail or by an established and generally-recognized provider of secure delivery services (e.g. Federal Express, UPS), in order to insure that the smart cards are properly delivered to their rightful holders in a timely and secure manner. Each recipient, in order to take possession of their personal state-issued smart card with digital certificate, shall be required to personally sign for the receipt of this card, although any individual may delegate this responsibility under the usual and customary practices for such delegation. The State of California, for its part, shall have the responsibility to use registered mail if sending the card by USPS or to use whatever level of service is required at an alternative delivery service in order to insure similarly reliable, accountable, auditable, and secure delivery of the smart card to its rightful holder/intended recipient.

Section 6.

The State of California shall additionally undertake to secure the immediate, ongoing and perpetual services of one or more recognized certificate authorities (CAs) to manage the use of the digital certificates issued by the state under the provisions of this legislation. The responsibilities of these CAs shall include, but not be limited to:

a. issuing the original, unique digital certificates
b. authenticating transactions conducted using the certificates it issues
c. developing and maintaining a Certificate Revocation List, in order to remove certificates that are no longer valid

d. educating its certificate holders and the general public about the workings of the digital certificate and digital signature processes
e. working diligently in cooperation with the business, educational, governmental, and other communities to maintain and enhance the security, convenience and usefulness of its certificates and services in order to find innovative ways to employ them in furthering the development of the state, the organizations and companies within it, and its people.

Contracts to provide these services may be entered into at the discretion of the state and with the acceptance of the certificate authorities under terms and conditions to be mutually agreed upon.

Section 7.

Nothing in this legislation shall be construed to prohibit or otherwise impede the use of the smart card/digital certificate combinations generated by and distributed under this legislation or of the digital certificates alone, from whatever platform on which they may be stored, by their rightful owners (and the holders of these certificates, once the certificates have been issued to them, shall be, under law, the owners of those smart cards and those digital certificates, not the State of California which issued them) for any lawful transactions they may choose to transact, including, but not limited to, transactions they undertake with other individuals, with commercial businesses, or with the State of California, or with any of its subdivisions, including, but not limited to, counties, cities, community college districts, or any special districts now in existence or later to come into existence.

As owners-in-full of these smart cards and digital certificates, their holders may use them for any lawful purpose they choose. If other entities, including, but not limited to, the State of California, any of its subdivisions, the United States Government, the government of any other state or municipality within the United States, the national, regional, provincial, state, municipal, or local government in any country other than the United States, any international, transnational, or supranational organization or entity, or any person, natural or otherwise, organization, group, or other entity of any type, now existing or existing in the future, real or virtual, engaged in lawful operations, chooses to allow the authentication for its purposes and the purposes of the holder of the smart card and/or digital certificate by means of the smart card and/or digital certificate issued to its holder by the State of California, the State of California shall raise no objections to this, initiate no legal action in the matter, and shall forever and in perpetuity hold blameless the holder of the smart card/digital certificate and any and all other parties to such a transaction for so using it.

Section 8.

Under this legislation, no additional user fees may be imposed on applicants for or users and holders of the new smart driver licenses or smart state identification cards, either for administering the production and distribution of these cards, for collecting the e-mail

addresses to which holders choose to have their digital certificates sent, for managing the transition to smart cards, or for the digital certificate which is to be included with the smart card, or for the smart card itself, apart from the normal and customary fees already being charged for the corresponding "legacy" cards at the time this legislation is enacted.

Section 9.

This legislation hereby grants to all institutions, individuals, government jurisdictions, agencies, and departments, and all persons, natural or legal, the absolute right to accept and/or to provide digital signatures in lieu of written signatures for any and all purposes as mutually agreed to by the parties to any transaction subject in any way to legal oversight by the State of California or any of its governmental or legal subdivisions.

The day after the Internet-based Democratic Primary election in Arizona, I wrote about putting democratic processes on a "real-time" basis.

Real Time Democracy

March 13, 2000

Thirty-five thousand, seven hundred, and sixty-five Arizona Democrats have proven that Internet voting is viable, cost-effective, secure, and a great way to bring the previously-uninvolved into the electoral process. Now that these facts have been established, the obvious next step is to bring Internet voting to all American citizens. This can be done through legislation, administrative decisions, or the initiative process.

But while we are doing that, we shouldn't forget three other ways in which the Internet can be put to work in the service of democracy. All of these steps, taken together, will move us closer to "real time democracy." They are:

1. the electronic signing of online petitions to qualify initiatives and referendums for the ballot, with a constantly-updated online display of the current number of valid signatures collected

2. the instantaneous inspection, certification and reporting of campaign contributions

3. the provision of systems allowing elected officials to constantly take the pulse of their constituents' legislative and policy issue preferences

The core Internet technology that makes Internet voting possible also makes it feasible to deploy and deliver these additional democratic services, the existence of which will facilitate and make transparent the inner workings and state-of-play of various parts of the democratic process.

Once the political parties and the state identification agencies (usually the Department of Motor Vehicles) can find the will and the time to sit down with the digital ID people who make Internet voting work, and possibly with the smart card manufacturers, it will be relatively straightforward to provide each citizen with a digital ID comparable to their driver's license, or as part of their driver's license.

This digital ID will, in conjunction with an installed Internet voting system, allow citizens to vote online, and also allow them to digitally and definitively sign online documents, including initiative petitions.

Using this same digital ID, all campaign contributors would be able, if required, to submit a description of their proposed contributions to the state or federal authority responsible for enforcing campaign finance laws. If the proposed contribution is legal, it will be certified as such by the controlling agency, the funds involved will be electronically transferred from the contributor's account to the recipient's, and the facts

of the contribution will be instantaneously posted on the agency's website, where everyone who wants to can see them.

Once the citizenry is equipped for electronic participation in elections, petition signing, and campaign contributing, it will have everything it needs by way of tools and training to allow elected representatives to set up websites that allow all their constituents, and only their constituents, to constantly keep their legislators informed as to how they feel about upcoming floor votes, possible trade-offs in legislative negotiations, and long-range priorities and concerns.

Using the technology already proven to work in Internet voting, it would be easy to construct a system that would let constituents cast advisory ballots on all manner of issues facing their representatives in the state capital. This system, like the Internet election systems themselves, would allow each citizen to cast a secure and, if they choose, an anonymous, ballot dealing with issues of interest to them and/or chosen by the official. The main difference between this procedure and a regular election would be that the electorate could cast their ballots on a daily or weekly basis., not a biennial one.

The results of these secure constituent polls could be made public, on a real-time basis, as each vote is cast. Elected representatives would be free to follow their constituents' expressed preferences, to take them into account, or to ignore them. The voters, of course, would be equally free to consider the responsiveness of their representatives to their digitally-articulated preferences in deciding, the next time they vote over the Internet, whom they wanted to represent them in the legislature.

The following month, I expanded this concept to include a full-array of e-government and e-democracy services to be facilitated by state-distributed digital identification. I called it the "Digital Identification and Government Initiative" or DIGI. Like some huge futuristic skyscraper, it may have been too complex and too innovative to be built right away, or all at once. But some of its provisions, such as those calling for a Chief Information Officer for the State of California, the electronic reporting of campaign contributions, spending money to upgrade the state's digital infrastructure, and the putting of some, if not all, official government forms online have, as of December, 2002, already been adopted.

Digital Identification and Government Initiative (DIGI)

(April 10, 2000)

Petition Requesting that the Legislative Counsel Bureau draft an initiative providing state-issued digital identification (SDI) for all Californians, allowing the use of this SDI for various governmental and electoral functions, establishing the office of Chief Information Officer of California, and providing for the implementation of policies designed to create a Digital Government for the State of California

We, the undersigned registered California voter(s), hereby respectfully request that the Legislative Counsel Bureau draft an initiative measure that would provide for the following:

1. The State of California will provide every California resident with a convenient and easy-to-use form of digital identification, which shall then be recognized by the State as valid for every kind of resident-state transaction.

The DMV and the Secretary of State will cooperate to issue every California resident, at no direct cost to them, a digital identification certificate or other appropriate means of unambiguously, easily and irrevocably identifying themselves online. Digital certificates downloadable to any competent digital device, including smart card-based driver licenses, may be used for this purpose. The State of California shall also provide, or contract out for the provision of, a competent Certificate Authority to manage the issuance, use, and revocation of these digital IDs. Business entities may, for a reasonable charge, also apply for and receive such a state-issued digital

identification (hereinafter "SDI") for use in its transactions with the State and other jurisdictions within the state.

2. Any and all official petitions used within the State of California must be posted online by the jurisdiction intended to receive them. Any and all such petitions may be signed online using the state-issued digital identification.

All local and state official petitions, including those used for initiatives, referendums, recalls, and in lieu signature collection, may be signed by registered voters online, using their SDI. Official sites providing registered voters with the opportunity to digitally sign all such petitions shall be built and maintained by the jurisdiction to which the petition is being submitted, although other sites for collecting digital petition signatures may also be build and operated by those collecting signatures on initiative, referendum, recall, or in lieu petitions. It shall be unlawful to collect signatures on such a petition and then, with fraudulent intent, fail to submit these signatures in support of the purpose for which they have been collected.

Means shall be devised and implemented according to which the ongoing totals of signatures affixed to petitions circulating online shall be displayed in real-time online ("Real-time Running Total Display System" [RRTDS]) on the official website of the jurisdiction to which the signatures are being submitted and the websites of such other individuals or groups who wish to display these running totals. Signers of petitions who wish to remove their signatures from petitions they have signed may, at any time prior to the petition's submission to the jurisdiction intended to receive it, do so, using their SDI for this purpose. Petition signatures collected online may be submitted electronically by their collectors at anytime after their receipt to the

appropriate jurisdiction, and they must be accepted, processed, and counted towards the required totals by election officials immediately upon their receipt, notwithstanding any existing laws or

regulations limiting the times when petition signatures may be submitted, received, verified, totaled, and these totals announced. Existing means of randomly checking, verifying, and certifying signatures and signature totals shall, in the case of signatures collected online by means of SDI, be replaced by a system of direct electronic verification of each digital signature in real time using the technology of digital signature verification made possible by the use of the SDI. Existing law shall continue to control the procedures for the receipt and processing of signatures collected offline.

Signatures collected electronically by the jurisdictions themselves may be revoked by their signers at any time up to the final deadline for the submission of these signatures. Signatures collected electronically by third-parties and submitted to the jurisdiction shall be accepted, processed and counted towards the required totals as they are received, but may also be revoked by their creators at any time prior to the closing of the signature-submitting period. The real-time running total shall be decremented appropriately to reflect the removal of a signature previously-counted immediately after it is duly revoked by the signer.

When any initiative, recall, or referendum petition qualifies for the ballot with more than 50% of its valid signatures having been collected electronically, the initiative, recall, or referendum so qualified must receive at least two-thirds of the votes cast for or against it in the election in which it is voted upon in order to pass.

3. A Real Time Campaign Contribution Disclosure System is mandated.

There shall be established a **Real-Time Campaign Contribution Disclosure System (RCCDS),** requiring and allowing all campaign contributions of over $100 to be reported online *before* being made, then vetted by the relevant authorities according to existing campaign finance laws, accepted if legal, rejected if not, and reported to and displayed on an official website built and maintained for this purpose by the state, county or other appropriate jurisdiction as they are made, in real-time.

4. All otherwise eligible California residents may use their SDI to register to vote online.

State, county and other election officials within the state must provide the means for all otherwise eligible California residents to so register, using online forms and their SDI.

5. Registered voters may change their party affiliation or any other item in their registration using their SDI.

State, county and other election officials within the state must provide the means for all otherwise eligible California residents to so modify their registration records, using online forms and their SDI.

6. Internet voting using SDI is legalized.

Registered voters may vote in all official elections within California over any electronic network capable of accepting and transmitting a secure digital signal, using their SDI. All political jurisdictions within the state must provide the means for every registered voter within their jurisdiction to access the Internet and use their SDI to vote online, if they so choose.

7. All official government forms must be available and signable online.

Any form used by any government agency of or in the state for official business between that agency and a resident or between that agency and a business must be available as an interactive form on the Internet and must be capable of being filled out and digitally signed, using the SDI of the resident or the business, submitted and accepted by the agency as equally valid as a form filled out in person, submitted by mail, fax, or any other offline means of delivery.

8. A Constituent Preference Expression System shall be established for use by residents and elected officials.

There shall be established a **Constituent Preference Expression System (CPES)** on which all state, county, municipal and other elected officials shall post questions for their constituents to vote on, using their SDIs, on a daily or weekly basis, at the discretion of the elected official. Questions to be voted upon may be submitted by the representatives or by any of their constituents. For representatives, questions should focus on legislative proposals expected to be voted on soon, long-term issues with which the body of which the elected official is a member will be dealing over the course of its term, and any other relevant matters. Elected members of the executive branch may post questions dealing with matters now or soon to be before them, issues of general concern to their constituents, or any other questions of interest to them or their constituents. Elected officials shall be under no compulsion whatsoever to vote or otherwise act in accordance with the results of these polls, but the results of these polls shall be published on the Net in real time and shall be archived for reference purposes and made available online in perpetuity.

9. Establish the office of Chief Information Officer of California, to be appointed by the Governor and confirmed by State Senate, with the responsibility and authority to oversee the implementation of the provisions of this initiative and to coordinate the establishment of Digital Government for the State.

10. Provide for the introduction of e-applications to carry out all existing government functions that can be performed more efficiently through the use of advanced IT technology, in conjunction with the methods of digital identification specified above.

Fully fund the implementation of the conversion to e-applications from existing legacy methods. Provide for the re-training and re-deployment of current state employees within the new IT infrastructure, or, in the alternative, their early retirement. Re-engineer the organization of state government in order to expeditiously provide existing services or new services as may be mandated by law in a cost-effective and maximally-efficient manner, by streamlining, integrating, and synergizing the mandates, responsibilities, and resources of all state agencies through the creation of an Integrated State Information Infrastructure (ISII), to be developed and managed by the state CIO.

11. Appropriate $60 million for interagency digital coordination and e-applications development.

12. Appropriate $20 million for coordination with Federal government and other states to develop applications in common.

13. Establish and implement procedures for e-procurement and the e-auctioning off of state surplus.

14. Address privacy concerns pro-actively and develop and implement systems to protect individual and commercial privacy rights.

15. Make all but private and confidential state data available easily to people online.

16 Provide incentives to agencies to save money with new IT systems by letting them keep the money they save. Allow for outsourcing of upgrades with a portion of savings thus generated going to companies doing the upgrades on spec or at a reduced rate.

17. Establish a public-private consortium to conduct Digital Government R & D, with findings put to use in government and commercial sectors and royalties from developed products and services shared by government and private participants.

18. Establish an "Institute for Virtual Government" to investigate the use of advanced expert systems, artificial intelligence, conversational avatars ("con avs") and other emerging and visionary technologies that could be used to optimize and enhance the operations of the Digital Government put into place under this legislation.

19. The proponent(s) of this initiative shall have standing to defend this measure in court.

20. Any challenge to this measure shall originate in the California Supreme Court.

21. **The**

22. The provisions of this measure are severable.

If any provision of this measure or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

23. The costs of implementing the provisions of this initiative shall be paid out the General Fund of the State of California.

The "conversational avatars" mentioned in Item 18 of the DIGI may be here sooner than we think, and we ought to be thinking about how we humans will relate to them now. Here are some of my preliminary thoughts on this subject.

Should Avatars Have Standing?

By Marc Strassman

Ever since the US Supreme Court decided so, you haven't had to be a human to be a person under the law. You could be a corporation, and have most human rights and a lot fewer human responsibilities.

With the advent of enhanced computer capabilities in the areas of graphics, speech synthesis and recognition, what used to be called artificial intelligence, and the greater availability of online identification and authentication, as well as wireless Internet connectivity, we now have the capability to create smart agents, or virtual persons, or avatars. These entities, composed solely of computer code, will soon be shopping for you, negotiating contracts, trading securities, arranging dates, giving presentations, and generally representing you in places you can't get to conveniently, or at all.

So why don't we let them be "persons" under the law?

In the late 70s, author Christopher Stone wrote a book entitled "Should Trees Have Standing?" in which he argued, provocatively, that elements of the natural world were entitled to legal standing in order to defend themselves against corporate depredations, with human conservators to represent their inherent rights as persons.

His arguments never really prevailed, and would sound as outré today as they did then. Still, his argument that entities other than humans and corporations can usefully be considered legal persons can now be applied to a type of entity whose emergence was not much foreseen at the time.

What a smart agent is.

Dynamics of ownership.

Multiple incarnations (Ganesh)

Relationships between and among smart agents.

Conservatorship and ownership of smart agents

Autonomy for smart agents

Ownership of property by smart agents.

Intellectual property rights of and for smart agents.

Let’s start the discussion before they arrive.

Here's one of the few times I leave the United States and talk about the larger picture of global techno-politics. Following this piece is a set of notes containing my procedural and substantive preferences for the next twenty years of human history.

Global Government the Answer to Global Corporatism

May 12, 2000

Despite the fact that many of them find governments as repressive and reprehensible as they find multinational corporations, the "anti-globalization" forces recently in evidence in Seattle and Washington, D.C., still sometimes suggest that governments can help them in their efforts to counter the pernicious effects of global capitalism, generally by implementing laws to limit the power of corporations to do one thing or another.

But they do not, in my view, go far enough. Against the overwhelming and growing power of high-technologized global capital and transnational corporations, what entity can possibly countervail but a vigorous, democratic, decentralized, powerful and equally high-technology global government?

Feared by many as a sword that would destroy individual freedom, such a democratic and electronic institution may now be the only shield capable of protecting the individual and collective interests and rights of 6 billion people against the increasingly seamless control now wielded over the economy of the planet and the minds of its inhabitants by the interlocking corporations that provide us all with food, transportation, entertainment, and visions of what life is about (consume entertainment, consume "fun", consume sex, consume, consume, consume).

Obviously, a Big Brother-like government that surveils, arrests without cause, tortures, disappears, and murders its citizens is a completely bad thing. But it hasn't required the existence of a world government for the emergence of this kind of behavior by separate national governments. Nazi Germany, Cambodia under the Khmer Rouge, Argentina's dirty war, and plenty of other genocidal regimes have reached this depth of depravity while remaining merely national jurisdictions.

Nor is the kind of non-world government that characterizes the present United Nations what I have in mind. This is truly a government-to-government operation, featuring an illustrious aggregation of world-class representatives and bureaucrats who can sometimes do useful humanitarian work but which has mostly been, since its founding in the aftermath of the Second World War, a reflection of the alliances and strains in world politics, not a means for resolving them nor an instrument to challenge existing power relations, either between states or between economic institutions and the people or nations they effect.

Recent visits to the government websites of various countries revealed to me that politics is politics and elections are elections, wherever you go. The website of Brazil led me to an electronic voting booth for candidates in one of its states. The website of a now-united Germany impressed me with its Flash graphics and thorough coverage. Just as

they are increasingly listening to the same music (or variations thereof), following the same news stories, and worrying about the same issues, in their local and global manifestations, world citizens are also having more or less the same electoral and political experiences.

Candidates are more or less honest and campaigns are more or less fair. Some issues involve matters that can convincingly be characterized as local. Others, like those involving world trade, investment, global pollution, and such, are clearly transnational in scope. As things now stand, citizens in specific localities elect governments that then negotiate with each other over those issues that affect them all. These government act as (classic) intermediaries, representing the desires of their (often conflicted) constituencies, taking into account the importuning of their campaign contributors, their desire to please the media, their own career considerations. Sometimes the results are advantageous for the majority of those affected, but not always.

These problems are endemic, and have characterized political life everywhere since the beginning of time. There has now arisen, however, a technology that is famously capable of disintermediating transactions, and does so already, on a global scale. It is the technology that now dares to speak its name as a solution for previously-intractable political problems: the Internet.

As we are already starting to see, the Internet has the ability to directly connect buyers, sellers, advertisers, customers, and even elected officials and constituents. As Internet technology continues to evolve and adds more and more capability to connect people and institutions in increasingly sophisticated and subtle ways, there is a corresponding increase in its ability to provide the infrastructure for a global government that is more, not less, supportive of individual freedom and human rights, while at the same time allowing everyone effected by a governmental decision to participate directly in the making of it.

It's not my intention to set out in any detail the form that such an electronic global government ought to take. I want merely to point out that only a powerful global government will have the ability to fend off the power grab of the international corporate armada, as well as to deal with issues of global scope such as resource depletion, population growth, environmental contamination and collapse. I also want to make the point that an Internet-based, democratic and participatory form of government can create systems of governance for all of us worldwide that are at least as supportive of human rights, personal dignity, and justice for all as the best of today's governments and could represent a significant improvement for many nations in comparison with their current system of governance.

An integrated, transnational, electronic democracy would allow for a worldwide concurrent evolution of our governments, economy, cultures, and lives in a way that would build upon and go significantly beyond the already-strong decline of the nation-state as the primary organizing tool for government and, in many cases, personal identity. The global economic system has long since evolved past its national stage. The multinational or transnational corporation is actually a "post-national" corporation. It draws on world capital for investment, executives, workers, and markets. Its managers and owners are loyal to their class and their corporations, and to the concept of a single world as the playing field for their economic exploits.

Meanwhile, national leaders, even the most talented and compassionate, and all those they lead, cannot successfully compete with institutions with limitless resources and limited responsibilities. Former California Senator Alan Cranston, such a strong defender of freedom that he became the only American citizen ever sued by Hitler (for intellectual property violations involving the American publication of Mein Kampf, if you can believe that), and many others associated with him worked for years on behalf of the concept of World Federalism. Under this model, nation states would unite like the thirteen original colonies did to form the United States. It was a shocking idea in its time, and, as you can see by looking around at the world, one which has never been realized.

Now we need something more, something deeper. To confront the powerful thesis of global capitalism organized through the post-national corporation and its attendant institutions, we need the antithesis of global government. We need a global government that is democratic, protective of individual and group rights, electronic, participatory and open. Only people who are using all the powerful technological and organizational tools that have raised the modern corporation to world ascendancy have any chance of controlling its power or turning that power, tempered and informed by their own desires, to their own, more humane, purposes. We must do that now, and move towards the creation, under the umbrella of that global government, of a global civilization that we can be proud of and which will nurture us, individually and collectively. We need to create a humane social infrastructure such as this, one which can and will endure and evolve as we move into the future, or forego that opportunity, and enter an extended era of brightly-lit slavery.

Notes for New World Government article

(composed while listening to Dvorak's Symphony, #9, "From the New World")

World Assembly 100 reps elected by all people 18+, geographically based

World Senate 100 reps elected by all people 18+, self-designated categories

Including: environmentalist, free trader, woman, man, sexual minorities, ethnicity, city dweller, Southern Countries, Mensa member, disabled, Greens

Each person picks one category; people can choose multiple categories with rankings and let the computer calculate most advantageous selections

Add Global Initiative, Referendum, and Recall

Add Internet voting

Add ICANN election as prototype and precursor

World Executive Council 10 members elected worldwide

7 votes required for action

generally carries out will of World Legislature (W Assembly, W Senate)

World Court from the one in The Hague

Unify world legal systems with variations retained for geographic and free-associations that want them.

Add Universal Code of Human Rights derived from an expanded Universal Declaration of Human Rights

Substance:

Eliminate all weapons of mass destruction and the means to produce them
Control world population
Eliminate poverty
Enhance culture
Develop science, medicine, and technology
Expand education at all levels
Peruse sustainable technologies
Explore and colonize space and the oceans
Eliminate internal combustion engines, cigarettes, nuclear power and red meat
Expand the Internet, pursue Kurzweillian human-computer merger

Add Real time democracy elements

By 2010, most elections in the developed world and many in the less developed world will be conducted over the Internet.

Notes 5-20-00

Sovereignty, Loyalty, Nationalism, and Brand Loyalty

More people wear a swoosh on their hats than flags

For national governments, think of it as friendly mergers needed to achieve world-class status (e.g., EU)

By August of 2000, the proposed Digital Identification and Government Initiative (DIGI) had evolved into the Digital Identification Initiative (DIDI), which was drafted by the Office of Legislative Counsel (OLC). The summary that follows below the DIDI was written by me, not the OLC.

DIDI empowered all registered California voters to sign any and all official petitions over the Internet, using digital certificates provided by the state. The existence of the DIDI in the summer of 2000 may have played some part in the decision of California State Assembly Speaker Robert Hertzberg to create the "Speaker's Commission on the California Initiative Process," which first met on October 30, 2000, in order to deflect and contain the reformist impulse behind my effort.

On January 22, 2001, I would testify before that Commission in support of Smart Initiatives, just as the OLC was completing the drafting of the text of the Smart Initiatives Initiative itself. A year after that, the Commission would issue its final report, in a non-downloadable PDF file containing scant reference to my proposals and full of suggested "reforms" that would strengthen legislative control of the initiative process, which had been initiated by the Progressives in 1911 precisely to give the people of the state the ability to legislate on their own, whenever they felt, as many did then and many do now, that the monied interests of the time had bought, and owned, their legislative "representatives," a contention that is pretty well borne out by the fate, so far, of Smart Initiatives.

Digital Identification Initiative (DIDI)

(August 3, 2000)

INITIATIVE MEASURE TO BE SUBMITTED DIRECTLY TO
THE VOTERS

The Attorney General of California has prepared the following title and summary of the chief purpose and points of the proposed measure:

(Here set forth the title and summary prepared by the Attorney General. This title and summary must also be printed across the top of each page of the petition whereon signatures are to appear.)

TO THE HONORABLE SECRETARY OF STATE OF CALIFORNIA

We, the undersigned, registered, qualified voters of California, residents of _____County (or City and County), hereby propose amendments to the Elections Code and the Government Code, relating to secure online identification and petitioning, and petition the Secretary of State to submit the same to the voters of California for their adoption or rejection at the next succeeding general election or at any

special statewide election held prior to that general election or otherwise provided by law. The proposed statutory amendments (full title and text of the measure) read as follows:

SECTION 1. This act shall be known and may be cited as the Digital ID Initiative.

SECTION 2. Chapter 8 (commencing with Section 9700) is added to Division 9 of the Elections Code, to read:

CHAPTER 8. ELECTRONIC PROCEDURES

9700. (a) Notwithstanding any other provision of law, any petition circulated pursuant to this division may be signed using a digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 of the Government Code.

(b) This section shall not be construed to preclude the collection of signatures for a petition by any other means authorized by law.

9701. (a) A proponent of a measure for which a petition is circulated under this division may collect digital signatures generated by digital certificate pursuant to Section 9700, by posting the petition at a website managed by the proponent for that purpose. A candidate for office may, under the provisions of this division, collect and submit signatures in lieu of paying all or part of a filing fee required to run for that office.

(b) A certificated copy of the petition, properly formatted and in compliance with all other standards required by this division, except as to signature spaces, shall be provided online to potential signers of it by displaying the document (other than its signature spaces) in a manner that securely presents an unalterable image equivalent to that normally required for paper versions of the petition, using document exchange and management software approved by the Department of Information Technology for this purpose.

[c] (1) The petition displayed as described in subdivision (b) shall provide a means whereby a user may generate a digital signature on the petition, using a digital certificate, as described in Section 9700, with software approved for this purpose. The signer shall also provide any additional information required by law.

(2) In order to prevent the submission of multiple signatures by the same individual, the computer system hosting the measure shall be programmed to accept only one digital signature generated by the single digital certificate issued to each eligible person, and to reject all subsequent efforts to sign the petition with that digital certificate.

(d) The identity of any person generating a digital signature on a petition pursuant to this section shall be protected as provided by law. No part of this chapter shall be construed to abrogate any right of privacy otherwise protected under law.

(e) Any person who digitally signs a petition pursuant to this section may withdraw that digital signature as provided in Section 9602, except that the request for withdrawal may be submitted by electronic means, using a digital signature generated by digital certificate.

9702. (a) The petition shall be submitted to the appropriate elections official for filing and validation either on electronic storage media delivered physically to the official or by transmission to the official over the Internet under secure conditions, as approved by the Department of Information Technology, at the discretion of the proponent.

(b) Notwithstanding any other provision of law, petitions for which digital signatures have been collected under this chapter may be filed with the appropriate elections official by the proponent, using the methods set out in Section 9702 (a), at any time prior to the final date for filing the petition and the digital signatures contained therein shall be validated or rejected by that elections official within three (3) working days of their receipt.

[c] Signatures generated by digital certificates under this chapter shall be validated by the elections official responsible for validating signatures for the petition in question, using the most rigorous methods of digital authentication available, in conjunction with, or using procedures approved by, the Digital ID Issuing Authority.

9703. (a) In the case of initiative, referendum, and recall petitions, any digital signature generated by a digital certificate and validated pursuant to Section 9702 shall be counted toward the total required to qualify the measure for the ballot in question. In the case of signatures to be collected and submitted in lieu of requiring a candidate for public office to pay all or part of a filing fee for that office, any digital signature generated by a digital certificate and validated pursuant to Section 9702 shall be counted toward the total required to exempt that candidate from having to pay all or part of the filing fee for that office. The tally of validated signatures collected shall be forwarded to the Secretary of State by the appropriate elections official on an ongoing basis.

(b) The Secretary of State shall provide and update information showing the number of validated digital signatures collected, based on the most recent information provided by the appropriate elections official or officials, at the official website of the Secretary of State.

9704. The Digital ID Issuing Authority and the Department of Information Technology may each adopt regulations to implement this chapter.

9705. (a) Any person who interferes with the lawful operation of the electronic processes specified in this chapter with the intent of committing fraud or violating the integrity of any system used for these activities, including, but not limited to, its internal, contents, or results, by any means, whether or not through the use of a

computer, or who attempts to impede access to an official petition website by means of a "denial-of-service" attack or by any other means, is guilty of a public offense for each occurrence, punishable by imprisonment in the state prison for a period of 16 months or two or three years, or in a county jail for not more than one year, or a fine of not more than ten thousand dollars ($10,000), or by both that imprisonment and fine.

(b) As a condition of parole, any individual found guilty of an offense pursuant to this section may be prohibited from using any electronic network for a period of not more than the term of parole.

SEC. 3. Section 16.5 of the Government Code is amended to read:

16.5. (a) In any written communication with a public entity, as defined in Section 811.2, in which a signature is required or used, any party to the communication may affix a signature by use of a digital signature that complies with the requirements of this section. The use of a digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all of the following attributes:

(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.
(5) It conforms to regulations adopted by the Secretary of State. Initiation regulations shall be adopted no later than January 1, 1997. In developing these regulations, the secretary shall seek the advice of public and private entities, including, but not limited to, the Department of Information Technology, the California Environmental Protection Agency, and the Department of General Services. Before the secretary adopts the regulations, he or she shall hold at least one public hearing to receive comments.

(b) The use or acceptance of a digital signature shall be at the option of the parties, except as provided in Chapter 8 (commencing with Section 9700) of Division 9 of the Elections Code and as provided in Section 11791 of the Government Code. Nothing in this section shall require a public entity to use or permit the use of a digital signature.

[c] Digital signatures employed pursuant to Section 710066 of the Public Resources Code are exempted from this section.

(d) "Digital signature" means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.

SEC. 4. Chapter 7.5 (commencing with Section 11790) is added to Part 1 of Division 3 of Title 2 of the Government Code, to read:

CHAPTER 7.5. DIGITAL IDENTIFICATION ISSUING AUTHORITY

11790. (a) The Department of Motor Vehicles, the Secretary of State, the Department of Information Technology, and the county registrars of voters, shall collaborate to establish the Digital ID Issuing Authority of the State of California, whose mission shall be to efficiently and cost-effectively provide California residents with a high-level digital certificate in an easy-to-use form.

(b) The Digital ID Issuing Authority of the State of California shall, either on its own or by contracting with a suitable private supplier or suppliers, develop, design, implement and maintain a system capable of establishing the identity of individuals with sufficient assurance to issue them the digital certificates called for in this division, of interacting with recipients of these certificates so as to allow them to personalize and secure for their sole use the digital certificates they are issued; of maintaining in good order the databases containing the digital certificates they issue and any other associated data necessary to the efficient functioning of the digital certificate system; of keeping this system current by adding new users as they are issued digital certificates, removing users whose certificates are revoked, or when a user becomes deceased or permanently relocates out of the state, and changing any relevant data about users in a timely manner; and of providing to all electoral and other state and local agencies, in an accurate and speedy manner, the authentication of the digital signatures generated by the certificates it has issued, whether in the context of official petitions, transactions with government, or transactions in the private sector.

(c) (1) The Digital ID Issuing Authority, in collaboration with each recipient, shall generate and issue an individualized digital certificate belonging solely to that recipient. Through the use of passwords, biometrics or other means, this digital certificate shall be rendered accessible solely to the person to whom it is issued, as specified in Section 16.5 (a) (3) of the Government Code, and cited in SEC. 3 of this division. The digital certificates created by the authority according to these procedures shall then be loaded onto smart cards that use the best generally available technology, and that shall be used as the substrate for the driver license or identification card issued by the Department of Motor Vehicles to each applicant/recipient of these licenses and cards, unless an applicant/recipient specifies that he or she does not wish to have either a digital certificate at all or does not wish to have a digital certificate installed on the smart card providing the substrate of their driver license or identification card.. A smart card containing the registrant's personalized digital certificate shall be provided to registered voters who have neither driver's licenses nor identification cards, as the substrate of their voter registration cards, unless the registrant specifies that he or she does not wish to have either a digital certificate at all or does not wish to have a digital certificate installed on the smart card providing the substrate of their voter registration card. Anyone eligible to receive a digital certificate on a smart card under the provisions of this division may, at their discretion, receive a smart card without a digital certificate as the substrate of the driver license, identification card, or voter registration card to which they are entitled. The smart cards provided under the provisions of this division may, as practicable, be

"contactless," allowing their use at a distance, and may include optical storage areas, allowing users to store and retrieve large amounts of data on and from their cards. There shall be no additional fees charged to users (holders of driver licenses, identification cards, or voter registration cards) for the provision of the digital certificate or smart card.

(2) For purposes of this subdivision, the following definitions shall apply:

(A) "Smart card" means a card with a built-in microprocessor and memory that is capable of receiving, storing, processing, and transmitting electronic data.

(B) "Substrate" means the physical material of an identification card, upon which information is placed.

[c] As part of the process by which a holder personalizes his or her certificate and through which the Digital ID Issuing Authority establishes the identity of the holder, each holder of the state-issued digital certificate may request the Digital ID Issuing Authority to send the holder, free of charge, a complete and accurate digital copy of his or her digital certificate by electronic mail to up to and including ten electronic mail addresses provided by the holder. Pursuant to this subdivision, the digital certificate holder may request, as part of their allotted downloaded copies, that some of these copies be transmitted to cellular phones and/or other mobile or fixed wireless digital devices of their choice. The Digital ID Issuing Authority shall comply with all such requests.

11791. (a) A digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 shall be accepted by any state entity that offers secure transactions over the Internet, as complete and adequate proof of an individual's identity, and as capable of generating a "digital signature," as defined in Section 16.5, for purposes of executing any form, document, or other instrument related to the transaction, and that digital signature shall be deemed to constitute that individual's assent to the terms of the transaction and shall be accepted as such by the state entity involved.

(b) A digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 may be used for any personal or commercial purpose for which identification is required, and for generating a valid and acceptable legal signature as required, as provided under Title 2.5 (commencing with Section 1633.1) of Part 2 of Division 3 of the Civil Code.

11792. The Digital ID Issuing Authority and the Department of Information Technology may each adopt regulations to implement this chapter.

11793. (a) Any person who interferes with the lawful operation of the electronic processes specified in this chapter with the intent of committing fraud or violating the integrity of any system used for these activities, including, but not limited to, its internal, contents, or results, by any means, whether or not through the use of a computer, or who attempts to impede access to an official petition website by means of a "denial-of-service" attack or by any other means, is guilty of a public offense for each

occurrence, punishable by imprisonment in the state prison for a period of 16 months or two or three years, or in a county jail for not more than one year, or a fine of not more than ten thousand dollars ($10,000), or by both that imprisonment and fine.

(b) As a condition of parole, any individual found guilty of an offense pursuant to this section may be prohibited from using any electronic network for a period of not more than the term of parole.

SEC. 5. (a) The California Supreme Court shall have original jurisdiction in any legal action or proceeding to challenge the validity of this act.

(b) The proponents of this act shall have standing to defend the act in any such action or proceeding.

SEC. 6. The Legislature may amend this act only by a statute passed by a two-thirds vote of the membership in each house of the Legislature that is consistent with and furthers the purposes of this act.

SEC. 7. The provisions of this act are severable. If any provision of this act or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provisions or applications.

Proposed Official Summary for the DIGITAL ID INITIATIVE

(August 11, 2000)

ELECTIONS. DIGITAL IDENTIFICATION AND PETITIONING . INITIATIVE STATUTE.

Provides that initiative, referendum, recall, and in lieu petitions may be signed over the Internet using digital certificates. Establishes Digital ID Issuing Authority to create and maintain a system for issuing and revoking digital certificates and for verifying the digital signatures generated using them. Provides for the issuance of smart cards holding these certificates as the substrate of driver licenses, state identification cards and voter registration cards. Authorizes the use of these state-issued digital certificates for use in transactions with government agencies and commercial entities. Criminalizes efforts to interfere with online petition signing; specifies penalties. Preserves traditional petition signing methods.

Smart Initiatives

I decided to improve the marketability of these increasingly complicated ideas by creating the "Smart Initiatives Project" to lobby for "Smart Initiatives," which involves allowing the use of digital certificates to digitally sign official documents, including initiative petitions. One major purpose of this should be obvious if you've been following the story. By making it legal to sign initiative petitions online, the one million dollar entry fee barrier blocking me and others who wanted to put political reforms on the ballot would, if not disappear, at least be lowered to a very considerable extent. Immediately before the emerge of the Smart Initiatives campaign, I prepared these arguments for providing every citizen with a digital certificate so they could securely do business with their government.

Why a Campaign for the Universal Distribution of Digital Certificates Makes Sense

(August 1, 2000)

Now arising is a proposal to require each state, through its Departments of Motor Vehicles, Information Technology, and Elections, and working with private companies, to issue to each of its citizens a high-level digital certificate, one that will allow its holder to identify themselves and be authenticated unambiguously and legally over the Internet.

Why this is a good idea:

1. Digital certificated citizens (DCCs) will be able to do business with government at all levels in a less expensive, more convenient, and more secure way than they now can off-line
2. DCCs could register to vote, sign official petitions, and vote online, increasing civic participation while drastically lowering government costs
3. General e-commerce, and m-commerce (mobile commerce) will be enabled much more extensively than at present, growing the economy, and generating new government revenues
4. These certificates could be used to remotely sign contracts, non-disclosure agreements, and other business documents, thereby speeding up and increasing the security of such transactions, while simultaneously lowering costs to all parties involved.
4. The Federal Trade Commission has recently proposed that Congress require all websites to adopt a privacy policy that includes the right of consumers to access data about them in the site's databases. It has been objected that sites would then have to cope with requests for consumer data from sources other than the real customer. Providing everyone with a digital certificate would solve this problem, removing it as an obstacle to the implementation of an equitable privacy policy, thereby enhancing the privacy status of millions of Internet users.
5. If everyone had a digital certificate they could use to unambiguously identify themselves online under a regime of non-repudiation, then it would be possible to build and operate a system that would require campaign contributions over a certain size (say, $100) to be made/reported online with features that would "vet" proposed contributions before they were made in order to exclude any contributions that are

illegal according to the operative laws of any time and jurisdiction, taking into account the identify and previous contributions of each potential contributor.

Why this hasn't been done until now:

1. **The Chicken and Egg Problem.** Digital certificates, in spite of their usefulness in identifying and authenticating individuals over the Net, are not yet widely used. One major reason for that can be found in the Chicken-and-Egg syndrome. Not many consumers bother to get digital certificates because not many merchants, either on- or off-line, offer them anything for using them or even allow them to. Off-line, the expense of providing the smart card readers that could accept digital certificates has prevented most merchants from acquiring this equipment, along with the fact that few customers express interest or present such smart cards. For their part, customers, operating in an environment where few merchants have smart-card readers, reasonably conclude there is no point in acquiring digital certificates or smart cards.

Now, either everyone, acting rationally, has failed to adopt smart cards and digital certificates because there are no good reasons why they should, or the market only needs to be catalyzed by the government issuing millions of digital certificates on smart cards, after which merchants will install the readers and citizen/consumers will use the cards and everyone will benefit from lower costs, more convenience, and greater security. We'll only know which it is if we experiment with it in a market/state big enough to show us which hypothesis is correct.

2. **The Black Helicopter Problem.** Civil libertarians constantly worry that once everyone is registered with a unique, unambiguous number, a nameless agency will begin abducting, or harassing, or imprisoning everyone, starting with them. They ignore the fact that government agencies and many private organization already have more than enough information to do this if they wanted to and weren't constrained from doing so by law, morality, custom, the media, and inertia. Giving people the ability to identify and authenticate themselves in transactions with banks, schools, hospitals, the government, and each other is not going to significantly increase the probability for individual or collective repression. In fact, by opening up the government process online, significant progress could be made towards creating a more inclusive, more responsive government, one much less likely to engage in the worrisome behaviors that some worry about.

What can be done?

If all goes well, in November, 2001, California voters will have a chance to vote on the Digital ID Initiative (DIDI), which will require the State of California to provide all its citizens with digital certificates, at no additional cost to them (except as taxpayers). It will also give them the right to use these certificates to digitally sign online initiative petitions.

Once legislatures in other states hear about this proposal, it's natural to assume that its reasonableness and significant benefits will persuade a number of forward-looking

legislators to adopt it as their own and pursue its swift passage in their own state legislature.

In the meantime, organizations and individuals who see the benefits of the universal distribution of digital certificates can spread the word about it. Getting this infrastructure of "remote assent" in place as soon as possible will mean we can rapidly move on to putting it to use in countless ways to improve our governance, our commercial business, and our lives generally.

Since I hadn't been able to solve the problem of raising a million dollars to qualify an initiative that might empower people through Internet voting, I decided to tackle that problem head on, with another initiative that would let registered voters sign initiative petitions (like mine for Internet voting) online, using digital certificates. Of course, I didn't have and couldn't raise the million dollars needed to put THIS initiative on the ballot either.

Here's the text of the "Smart Initiatives Initiative," which would have done this.

The Smart Initiatives Initiative

(August 3, 2000)

INITIATIVE MEASURE TO BE SUBMITTED DIRECTLY TO THE VOTERS

The Attorney General of California has prepared the following title and summary of the chief purpose and points of the proposed measure:

DIGITAL SIGNATURE. ELECTION PETITIONS. PUBLIC AND PRIVATE TRANSACTIONS. INITIATIVE STATUTE. Establishes a state agency to issue a digital certificate to any California resident. Requires certificate to generate a verified digital signature that can be used to subscribe to any authorized public or private sector electronic transaction. Authorizes use as driver license, identification or voter registration card at no additional charge. Requires election officials to validate and count digital signatures for candidacy, initiative, referendum and recall petitions if transmitted to a secure website provided by candidate or proponent. Preserves traditional signature methods. Imposes imprisonment and fines for violations of this system. Summary of the estimate by Legislative Analyst and Director of Finance of fiscal impact on state and local governments: Measure would result in unknown, major one-time costs to develop the systems, and could result in unknown major (probably in the range of tens of millions of dollars) annual net costs to state and local governments.

TO THE HONORABLE SECRETARY OF STATE OF CALIFORNIA

We, the undersigned, registered, qualified voters of California, residents of _____County (or City and County), hereby propose amendments to the Elections Code and the Government Code, relating to secure online identification and petitioning, and petition the Secretary of State to submit the same to the voters of California for their adoption or rejection at the next succeeding general election or at any special statewide election held prior to that general election or otherwise provided by law. The proposed statutory amendments (full title and text of the measure) read as follows:

SECTION 1. This act shall be known and may be cited as the Smart Initiatives Initiative.

SECTION 2. Chapter 8 (commencing with Section 9700) is added to Division 9 of the Elections Code, to read:

CHAPTER 8. ELECTRONIC PROCEDURES

9700. (a) Notwithstanding any other provision of law, any petition circulated pursuant to this division may be signed using a digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 of the Government Code.

(b) This section shall not be construed to preclude the collection of signatures for a petition by any other means authorized by law.

9701. (a) A proponent of a measure for which a petition is circulated under this division may collect digital signatures generated by digital certificate pursuant to Section 9700, by posting the petition at a website managed by the proponent for that purpose. A candidate for office may, under the provisions of this division, collect and submit signatures in lieu of paying all or part of a filing fee required to run for that office.

(b) A certificated copy of the petition, properly formatted and in compliance with all other standards required by this division, except as to signature spaces, shall be provided online to potential signers of it by displaying the document (other than its signature spaces) in a manner that securely presents an unalterable image equivalent to that normally required for paper versions of the petition, using document exchange and management software approved by the Department of Information Technology for this purpose.

[c] (1) The petition displayed as described in subdivision (b) shall provide a means whereby a user may generate a digital signature on the petition, using a digital certificate, as described in Section 9700, with software approved for this purpose. The signer shall also provide any additional information required by law.

(2) In order to prevent the submission of multiple signatures by the same individual, the computer system hosting the measure shall be programmed to accept only one digital signature generated by the single digital certificate issued to each eligible person, and to reject all subsequent efforts to sign the petition with that digital certificate.

(d) The identity of any person generating a digital signature on a petition pursuant to this section shall be protected as provided by law. No part of this chapter shall be construed to abrogate any right of privacy otherwise protected under law.

(e) Any person who digitally signs a petition pursuant to this section may withdraw that digital signature as provided in Section 9602, except that the request for withdrawal may be submitted by electronic means, using a digital signature generated by digital certificate.

9702. (a) The petition shall be submitted to the appropriate elections official for filing and validation either on electronic storage media delivered physically to the official or by transmission to the official over the Internet under secure conditions, as approved by the Department of Information Technology, at the discretion of the proponent.

(b) Notwithstanding any other provision of law, petitions for which digital signatures have been collected under this chapter may be filed with the appropriate elections official by the proponent, using the methods set out in Section 9702 (a), at any time prior to the final date for filing the petition and the digital signatures contained therein shall be validated or rejected by that elections official within three (3) working days of their receipt.

[c] Signatures generated by digital certificates under this chapter shall be validated by the elections official responsible for validating signatures for the petition in question, using the most rigorous methods of digital authentication available, in conjunction with, or using procedures approved by, the Digital ID Issuing Authority.

9703. (a) In the case of initiative, referendum, and recall petitions, any digital signature generated by a digital certificate and validated pursuant to Section 9702 shall be counted toward the total required to qualify the measure for the ballot in question. In the case of signatures to be collected and submitted in lieu of requiring a candidate for public office to pay all or part of a filing fee for that office, any digital signature generated by a digital certificate and validated pursuant to Section 9702 shall be counted toward the total required to exempt that candidate from having to pay all or part of the filing fee for that office. The tally of validated signatures collected shall be forwarded to the Secretary of State by the appropriate elections official on an ongoing basis.

(b) The Secretary of State shall provide and update information showing the number of validated digital signatures collected, based on the most recent information provided by the appropriate elections official or officials, at the official website of the Secretary of State.

9704. The Digital ID Issuing Authority and the Department of Information Technology may each adopt regulations to implement this chapter.

9705. (a) Any person who interferes with the lawful operation of the electronic processes specified in this chapter with the intent of committing fraud or violating the integrity of any system used for these activities, including, but not limited to, its internal code, contents, or results, by any means, whether or not through the use of a computer, or who attempts to impede access to an official petition website by means of a "denial-of-service" attack or by any other means, is guilty of a public offense for each occurrence, punishable by imprisonment in the state prison for a period of 16 months or two or three years, or in a county jail for not more than one year, or a fine of not more than ten thousand dollars ($10,000), or by both that imprisonment and fine.

(b) As a condition of parole, any individual found guilty of an offense pursuant to this section may be prohibited from using any electronic network for a period of not more than the term of parole.

SEC. 3. Section 16.5 of the Government Code is amended to read:

16.5. (a) In any written communication with a public entity, as defined in Section 811.2, in which a signature is required or used, any party to the communication may affix a signature by use of a digital signature that complies with the requirements of this section. The use of a digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all of the following attributes:

(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.
(5) It conforms to regulations adopted by the Secretary of State. Initiation regulations shall be adopted no later than January 1, 1997. In developing these regulations, the secretary shall seek the advice of public and private entities, including, but not limited to, the Department of Information Technology, the California Environmental Protection Agency, and the Department of General Services. Before the secretary adopts the regulations, he or she shall hold at least one public hearing to receive comments.

(b) The use or acceptance of a digital signature shall be at the option of the parties, except as provided in Chapter 8 (commencing with Section 9700) of Division 9 of the Elections Code and as provided in Section 11791 of the Government Code. Nothing in this section shall require a public entity to use or permit the use of a digital signature.

[c] Digital signatures employed pursuant to Section 710066 of the Public Resources Code are exempted from this section.

(d) "Digital signature" means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.

SEC. 4. Chapter 7.5 (commencing with Section 11790) is added to Part 1 of Division 3 of Title 2 of the Government Code, to read:

CHAPTER 7.5. DIGITAL IDENTIFICATION ISSUING AUTHORITY

11790. (a) The Department of Motor Vehicles, the Secretary of State, the Department of Information Technology, and the county registrars of voters, shall

collaborate to establish the Digital ID Issuing Authority of the State of California, whose mission shall be to efficiently and cost-effectively provide California residents with a high-level digital certificate in an easy-to-use form.

(b) The Digital ID Issuing Authority of the State of California shall, either on its own or by contracting with a suitable private supplier or suppliers, develop, design, implement and maintain a system capable of establishing the identity of individuals with sufficient assurance to issue them the digital certificates called for in this division, of interacting with recipients of these certificates so as to allow them to personalize and secure for their sole use the digital certificates they are issued; of maintaining in good order the databases containing the digital certificates they issue and any other associated data necessary to the efficient functioning of the digital certificate system; of keeping this system current by adding new users as they are issued digital certificates, removing users whose certificates are revoked, or when a user becomes deceased or permanently relocates out of the state, and changing any relevant data about users in a timely manner; and of providing to all electoral and other state and local agencies, in an accurate and speedy manner, the authentication of the digital signatures generated by the certificates it has issued, whether in the context of official petitions, transactions with government, or transactions in the private sector.

(c) (1) The Digital ID Issuing Authority, in collaboration with each recipient, shall generate and issue an individualized digital certificate belonging solely to that recipient. Through the use of passwords, biometrics or other means, this digital certificate shall be rendered accessible solely to the person to whom it is issued, as specified in Section 16.5 (a) (3) of the Government Code, and cited in SEC. 3 of this division. The digital certificates created by the authority according to these procedures shall then be loaded onto smart cards that use the best generally available technology, and that shall be used as the substrate for the driver license or identification card issued by the Department of Motor Vehicles to each applicant/recipient of these licenses and cards, unless an applicant/recipient specifies that he or she does not wish to have either a digital certificate at all or does not wish to have a digital certificate installed on the smart card providing the substrate of their driver license or identification card.. A smart card containing the registrant's personalized digital certificate shall be provided to registered voters who have neither driver's licenses nor identification cards, as the substrate of their voter registration cards, unless the registrant specifies that he or she does not wish to have either a digital certificate at all or does not wish to have a digital certificate installed on the smart card providing the substrate of their voter registration card. Anyone eligible to receive a digital certificate on a smart card under the provisions of this division may, at their discretion, receive a smart card without a digital certificate as the substrate of the driver license, identification card, or voter registration card to which they are entitled. The smart cards provided under the provisions of this division may, as practicable, be "contactless," allowing their use at a distance, and may include optical storage areas, allowing users to store and retrieve large amounts of data on and from their cards. There shall be no additional fees charged to users (holders of driver licenses, identification cards, or voter registration cards) for the provision of the digital certificate or smart card.

(2) For purposes of this subdivision, the following definitions shall apply:

(A) "Smart card" means a card with a built-in microprocessor and memory that is capable of receiving, storing, processing, and transmitting electronic data.

(B) "Substrate" means the physical material of an identification card, upon which information is placed.

[c] As part of the process by which a holder personalizes his or her certificate and through which the Digital ID Issuing Authority establishes the identity of the holder, each holder of the state-issued digital certificate may request the Digital ID Issuing Authority to send the holder, free of charge, a complete and accurate digital copy of his or her digital certificate by electronic mail to up to and including ten electronic mail addresses provided by the holder. Pursuant to this subdivision, the digital certificate holder may request, as part of their allotted downloaded copies, that some of these copies be transmitted to cellular phones and/or other mobile or fixed wireless digital devices of their choice. The Digital ID Issuing Authority shall comply with all such requests.

11791. (a) A digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 shall be accepted by any state entity that offers secure transactions over the Internet, as complete and adequate proof of an individual's identity, and as capable of generating a "digital signature," as defined in Section 16.5, for purposes of executing any form, document, or other instrument related to the transaction, and that digital signature shall be deemed to constitute that individual's assent to the terms of the transaction and shall be accepted as such by the state entity involved.

(b) A digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 may be used for any personal or commercial purpose for which identification is required, and for generating a valid and acceptable legal signature as required, as provided under Title 2.5 (commencing with Section 1633.1) of Part 2 of Division 3 of the Civil Code.

11792. The Digital ID Issuing Authority and the Department of Information Technology may each adopt regulations to implement this chapter.

11793. (a) Any person who interferes with the lawful operation of the electronic processes specified in this chapter with the intent of committing fraud or violating the integrity of any system used for these activities, including, but not limited to, its internal, contents, or results, by any means, whether or not through the use of a computer, or who attempts to impede access to an official petition website by means of a "denial-of-service" attack or by any other means, is guilty of a public offense for each occurrence, punishable by imprisonment in the state prison for a period of 16 months or two or three years, or in a county jail for not more than one year, or a fine of not more than ten thousand dollars ($10,000), or by both that imprisonment and fine.

(b) As a condition of parole, any individual found guilty of an offense pursuant to this section may be prohibited from using any electronic network for a period of not more than the term of parole.

SEC. 5. (a) The California Supreme Court shall have original jurisdiction in any legal action or proceeding to challenge the validity of this act.

(b) The proponents of this act shall have standing to defend the act in any such action or proceeding.

SEC. 6. The Legislature may amend this act only by a statute passed by a two-thirds vote of the membership in each house of the Legislature that is consistent with and furthers the purposes of this act.

SEC. 7. The provisions of this act are severable. If any provision of this act or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provisions or applications.

Five days after submitting the proposed initiative to the Office of the Secretary of State, I wrote to the Office of the Attorney General of California and asked them to name this proposal the "Smart Initiatives Initiative.

Faxed letter to California's Attorney General regarding the name of the Smart Initiatives Initiative

(August 8, 2000)

August 8, 2000

Initiative Coordinator Tricia Knight
Office of the Attorney General
1300 I Street
Suite 125
Sacramento, CA 94244-2550
FAX: 916-324-8835

Dear Ms. Knight,

I am writing to suggest that the initiative I submitted to you on August 3, 2000, be officially titled the "Smart Initiatives Initiative."

I know that the titles of initiatives need to be extremely neutral and non-partisan, without prejudicing the voters one way or another.

Despite the generally positive light in which "smart" things are viewed, I believe that it would still be fair to call this measure the "Smart Initiatives Initiative" because the system of petition signing established therein is based in large part on the use of smart cards, which are so called because of the computing power contained in these "computers-on-a-card."

It therefore makes sense, and shouldn't be considered positively prejudicial, to call, by extension, this new form of initiative a "smart initiative."

On another matter, do I have a choice as to whether I'd like this initiative to appear on the primary or general election ballot in 2002?

Sincerely,

Marc Strassman
Chief proponent
Smart Initiatives Initiative

Although it eventually generated a lot of material, the core idea behind Smart Initiatives was probably never so concisely expressed as in this "Mission Statement and Slogan," dated August 12, 2000.

Smart Initiatives Mission Statement and Slogan

(August 12, 2000)

The Smart Initiatives movement is working to give all citizens the right and the means to sign initiative and other official petitions online, with binding legal effect, using free digital certificates issued by state governments. Our slogan is "Political Reform through Internet Power."

At the same time, I prepared a slightly longer explanation of and brief for Smart Initiatives.

The Smart Initiatives Manifesto

(August 12, 2000)

The Internet makes possible, but hardly guarantees, a significant increase in freedom and self-determination, for those who care about such things. Giving actions taken over the Internet the force of law while giving every citizen adequate access to the Internet makes it possible to re-form democracy on a basis that is both intimate and national, even global.

Approximately half the states have in place the initiative process, whereby citizens or groups can propose laws that the state legislature sees fit, for whatever reason, not to pass. But it is difficult and expensive to qualify an initiative for the ballot. In California, it takes at least one million dollars to pay a professional signature gathering company to collect the 420,260 signatures necessary to qualify a ballot initiative.

This means that only either very motivated grass-roots organizations or people or groups with a lot of money can avail themselves of this procedure.

But if it were legal to sign initiative petitions right online, using digital certificates, then a good idea might be enough to propel an initiative onto the ballot. A replica of the official petition form, instead of being presented to harried pedestrians in malls where the owners have done everything they can to exclude signature gatherers and where they continue to object to the presence of citizens who might distract consumers, could be posted on a web site, surrounded by materials explaining the measure and exhorting citizens to sign it.

With this kind of privatization of public space, it is increasingly hard to find places where signatures can be gathered on petitions. Many state legislatures, jealous of citizens making laws they won't, worried that the Internet will disintermediate them the way it's rendered obsolete so many other twentieth century institutions, have tried to limit citizens' rights to collect signatures in public, while simultaneously ignoring calls to put the Internet to work in ways that would circumvent all the real-world obstacles to signature gathering.

Now comes the Smart Initiatives movement, seeking to add petition signing to the growing number of processes that are now being done faster, cheaper, and more conveniently over the Net. The Smart Initiatives Initiative, now pending in the Attorney General of California's office, would let initiative proponents put their measures into proper graphic form, then post them on the Net, where those who so chose could use a digital certificate issued by the state to digitally "sign" it.

No paper, no pen, no interfering with the property rights of mall owners or the United States Post Office. No heat, rain, cold, or table-carrying for petition circulators. No need to reduce the content of the initiative to a short slogan, since having it online along with

explanatory and exhortory materials will mean prospective signers can examine the legislation's text and its supporters' arguments at their leisure, 24/7.

And initiative sites can also include chat rooms for discussion of the initiative, FAQs (Frequently Asked Questions), links to related sites, audio and video clips discussing the measure, live webcasts (audio or video) of presentations on the initiative or debates between proponents and opponents, and so on, all of which would be difficult or impossible to bring to a mall and all of which would enhance the democratic process in general and the public understanding of every specific initiative in particular.

From the point of view of the election officials who need to sign off on the validity of the hundreds of thousands of signatures required to qualify a ballot measure, letting them be signed online with digital signatures ought to be seen as a dream come true. Currently, the paper-and-ink petitions submitted by initiative supports in one batch on the latest possible day allowed are not really checked very thoroughly. A small percentage of the signatures is checked, by hand, against the voter registration cards, and the results of this "random sample" are extrapolated to determine if enough valid signatures have been gathered.

But with digitally-signed petitions, the computers automatically, and almost instantaneously, authenticate the digital signatures. This means that EVERY signature can be checked and authenticated, or rejected as inauthentic. It means that the checking process has been automated, needing people only to program and maintain the machines that do the authenticating.

If phone calls were still handled by operators, if checks were cleared by back-room workers, these processes would be as slow and as expensive as checking signatures on initiative petitions is today. The guardians of this process will tell us that initiative petitions are different, are sacred, that error is not an option and that the old ways are best.

These are self-serving arguments and they are not adequate responses to the self-evident superiority of computerized methods, which are, in fact, already used throughout the election system, but haven't been applied to the signature gathering process because to do so would mean a quantum increase in the ability of ordinary citizens to legislate on their own behalf, something that those with a monopoly of this power don't want to share.

There are legitimate worries about certain aspects of proposed remote Internet voting technologies, principally regarding the difficulty in simultaneously authenticating the identity of an online voter while anonymizing the content of their ballot.

But using the Internet to collect digitally-signed initiative (or referendum or recall) petitions does not have the problem of simultaneous authentication and anonymization. When a person now signs a paper petition, their name obviously and necessarily becomes known to the election officials who need to verify the validity of their signature. Unlike an election ballot, there is no "content" created by their actions, no secret list of whom

they voted for or how they voted on ballot measures. The only "content" of an initiative is the signer's going on public record saying that they'd like to see that measure put on the ballot for a secret vote, up or down.

So the need to protect the anonymity of the voter isn't present with petition signing. And if a state currently protects the anonymity of the signer from the general public, as opposed to protecting it from the state, this can be done just as easily, even more easily, if the signatures have been gathered electronically, over the Net.

And as mentioned already, having the signatures in digital form means that every one of them can be checked and authenticated, then declared valid or not, in much less time than it currently takes to laboriously hand-check a small random sample of the submitted signatures.

So the digital signing of initiative petitions is faster, cheaper, and every bit as private as the current paper-and-ink method and allows for a more thorough validation process. Because it is all these things, it would improve citizen access to the content of initiatives and it would cut the cost of qualifying an initiative by several orders of magnitude.

But automating the signature gathering process will not mean that every proposed initiative would automatically qualify for the ballot. The same number of real people using digital certificates would still need to sign the petition. But having the Smart Initiative system in place would mean that a good idea that found favor with 420,260 Californians who find their way to that measure's website would qualify for the ballot, even without its supporters needing to raise a million dollars.

Still, this would only be the first step, since a majority of the voting public would still need to vote for the initiative when they encountered it on the ballot. But, at least in this first phase of the initiative process, putting it on the ballot, ideas and the will of the people could at least begin again to count for more than cash.

I followed this up two days later with more arguments in support of Smart Initiatives.

The Smart Initiatives Prospectus

(August 14, 2000)

As brick-and-mortar government evolves into e-government, giving citizens access to information and services online, it is essential for the maintenance of democracy that these same citizens gain equally free access to making government policy, as well as being recipients of it.

Giving actions taken over the Internet the force of law while giving every citizen adequate authenticated access to the Internet makes it possible to re-form democracy on a basis that is simultaneously both intimate and national, and even possibly global.

Approximately half the states already have in place the initiative process, whereby citizens or groups can propose laws that the state legislature sees fit, for whatever reason, not to pass. But it is difficult and expensive to qualify an initiative for the ballot. In California, it takes at least one million dollars to pay a professional signature gathering company to collect the 420,260 signatures necessary to qualify a ballot initiative.

This means that only either very motivated grass-roots organizations or people or groups with a lot of money can avail themselves of this procedure.

But if it were legal to sign initiative petitions right online, using digital certificates, then a good idea might be enough to propel an initiative onto the ballot. A replica of the official petition form, instead of being presented to harried pedestrians in malls where the owners have done everything they can to exclude signature gatherers and where they continue to object to the presence of citizens who might distract consumers, could be posted on a web site, surrounded by materials explaining the measure and exhorting citizens to sign it.

With the widespread privatization of public space, it is increasingly hard to find places where signatures can be gathered on petitions. Many state legislatures, jealous of citizens making laws they won't, worried that the Internet will disintermediate them the way it's rendered obsolete so many other twentieth century institutions, have tried to limit citizens' rights to collect signatures in public, while simultaneously ignoring calls to put the Internet to work in ways that would circumvent many current real-world obstacles to signature gathering.

Now comes the Smart Initiatives movement, seeking to add petition signing to the growing number of processes that are now being done faster, cheaper, and more conveniently over the Net. The Smart Initiatives Initiative, now pending in the Attorney General of California's office, would let initiative proponents put their measures into proper graphic form, then post them on the Net, where those who so chose could use a digital certificate issued by the state to digitally "sign" it.

No paper, no pen, no need to engage in negotiations about access. No heat, rain, cold, or table-carrying for petition circulators. No need to reduce the content of the initiative to a short slogan, since having it online along with explanatory and exhortory materials will mean prospective signers can examine the legislation's text and its supporters' arguments at their leisure, 24/7.

And initiative sites can also include chat rooms for discussion of the initiative, FAQs (Frequently Asked Questions), links to related sites, audio and video clips discussing the measure, live webcasts (audio or video) of presentations on the initiative or debates between proponents and opponents, and so on, all of which would be difficult or impossible to bring to a mall and all of which would enhance the democratic process in general and the public understanding of every specific initiative in particular.

From the point of view of the election officials who need to sign off on the validity of the hundreds of thousands of signatures required to qualify a ballot measure, letting them be signed online with digital signatures ought to be seen as a dream come true. Currently, the paper-and-ink petitions submitted by initiative supports in one batch on the latest possible day allowed are not really checked very thoroughly. A small percentage of the signatures is checked, by hand, against the voter registration cards, and the results of this "random sample" are extrapolated to determine if enough valid signatures have been gathered.

But with digitally-signed petitions, the computers automatically, and almost instantaneously, authenticate and validate the digital signatures. This means that EVERY signature can be checked and authenticated, or rejected as inauthentic. The digital signing of initiative petitions is faster, cheaper, and every bit as private and sure as the current paper-and-ink method and allows for a more thorough validation process. Because it is all these things, Smart Initiatives would improve citizen access to the substantive content of initiatives and it would cut the cost of qualifying an initiative by several orders of magnitude.

Automating the signature gathering process will not mean that every proposed initiative would qualify for the ballot. The same number of citizens, now using digital certificates, would still need to sign the petition. But having the Smart Initiative system in place would mean that a good idea that found favor with 420,260 Californians who find their way to that measure's website would qualify for the ballot, without its supporters needing to raise a million dollars.

Still, this would only be the first step, since a majority of the voting public would still need to vote for the initiative when they encountered it on the ballot. But, at least in this first phase of the initiative process, putting it on the ballot, ideas and the will of the people could begin to count for more than cash.

Using the offer of a free website from GeoCities, I built a rudimentary but colorful website for "The Smart Initiatives Project."

"The Smart Initiatives Project" Website

You can still go to "The Smart Initiatives Project" website at:

http://www.geocities.com/virtualorange/index.html

Around this time, I was invited to address the PKI Forum in Montreal, Canada. Here is the text of my remarks, followed by a link to the PowerPoint slideshow I used to accompany them, and a link to an audio recording of my presentation. This was my effort to persuade the assembled leaders of the Public Key Infrastructure industry to support my efforts for Smart Initiatives in order to build more and bigger markets for themselves and their authentication and identification security products.

To hear the presentation itself, go to:

http://sfm.lpbn.org:8080/ramgen/pkiforum-montreal091200.rm?usehostname

To see the PowerPoint slideshow that accompanied my presentation, go to:

Toward a Ubiquitous E-Democracy Powered by a Universal PKI, v. 1.5, 9-12-00.ppt

Toward a Ubiquitous E-Democracy Powered by a Universal PKI

(September 12, 2000)

At the risk of belaboring the obvious, let me remind us that the Internet has created a global system for the disintermediation of any process consisting of the transfer of information from person to person, organization to organization, or person to organization. And vice versa.

This means that any existing process involving the generation, collection, sorting, analysis, or distribution of information is subject to new dynamics, new cost structures, and the elimination of no-longer-needed individuals and organizations. Naturally, these unneeded entities resist their own demise. Nevertheless, a set of other people and other organizations, centering their operations in and over and around the Internet is emerging in every significant sector of life and work to challenge the hegemony of existing forms and working day-by-day to replace them with cheaper, faster, more accurate, more broadly inclusive ways of doing things.

Sometimes these new ways of doing things are explicitly illegal under existing law. Napster and the controversy surrounding it are an extremely good example of this. Millions of Napster users have used this system of peer-to-peer file exchange in order to augment their MP3 collections at no additional charge beyond whatever it costs them to access the World Wide Web. The Recording Industry Association of America, finding free music that doesn't pay them anything intolerable, took Napster to court, won, then saw the judge grant the program a stay until an appeals court can consider the case.

Let me briefly cite another case where the Internet was on the brink of undermining the entire election system of the US and, indeed, any country on earth, and where lawyers made it clear that such activity would not be tolerated. A number of

citizens, fed up with the fact that, in their opinion, elected representatives routinely received money for their legislative votes, mainly in the form of campaign contributions from parties with business before their bodies, decided that what was good enough for the legislator/goose should be good enough for the citizen/gander and put their votes up for auction to the highest bidder on eBay.

This move was praised by many as inspired street theater, but denounced harshly and authoritatively by election officials who sternly reminded these would-be vote sellers that what they were attempting to do was totally and completely illegal, and that they would be fined and/or imprisoned if they persisted in their errant ways. As far as I know, the "sell-your-vote online" movement died a'borning, under the legal onslaught unleashed against it by the protectors of the public vote.

This incident, by the way, provided piquant evidence of how fed-up with "representative" democracy many American citizens are and how, when they feel the need to do something about their frustration, it's the Internet they turn to. As we'll see later, there is a solution to this problem of citizen anger and apathy lurking in the Internet, and it's completely legal.

In both the Napster and vote-selling cases, the fundamental qualities of the Internet (its emerging near-ubiquity), its speed, low cost, adaptability to change, its ability to transfer vast amounts of information [when more and more of what there is is being recognized as fundamentally information] to millions of users worldwide almost instantaneously meant that like-minded, or complementary-minded, people could create a free market for exchanging commodities, in these cases MP3 files and votes.

Only the guardians of the music and the guardians of the votes stepped in, saying, "We own the music, and we control the voting process. Copyright infringement and vote tampering are serious crimes. You will do it our way or we will severely punish you. We shall be obeyed."

So far, the resolution of these conflicts is still up in the air, with vote selling apparently a dead letter right now, and Napster waiting further judicial rulings. But even if Napster is shut down and the code scattered to the four winds, there are other, harder to pin-down, applications that can duplicate its functionality. And as for vote selling, when Internet voting becomes ubiquitous and access to your ballot from any Internet connection through the use of a centrally-stored digital certificate by invocation of an easy-to-remember password becomes the key the electoral door, who can doubt that someone will create a market for the transfer of these passwords in exchange for money from individuals and organizations who have more money than they have votes?

This is not an argument in favor of abolishing Internet voting, but it is a cautionary observation that ought to inform our thinking about what the Internet can do and what it should be allowed to do.

One thing that I think it ought to be allowed to do is collect bona fide signatures from citizens who are willing to digitally sign initiative, referendum, and recall petitions online. The current initiative petitioning process is arcane in the extreme, costly, slow, prone to errors, and it cries out for some of the functionality that the Internet can bring to the automation of any process involving the manipulation of information.

The petitioning process, now with pen and paper, soon I hope with mouse and keyboard, is purely an information activity, and therefore ideal for being moved into cyberspace. Proponents formulate the idea, find language for it, work with others to edit and craft the proposed law. Officials receive documents, review them, certify them for timeliness and adherence to proper form and return them to the circulators. So far, this process hasn't cost too much.

Then the process of collecting the signatures begins. In California, 420,260 signatures need to be collected to put an initiative proposal on the ballot. That's 420,262 valid signatures. It's usual to collect many more than that, due to all manner of potential irregularities, including unreported changes of address, missing or incorrect information, illegible data, and so on. The going rate to hire a competent signature gathering company to collect the necessary signatures in California today is one million dollars.

And the problem is not all in the cost. Because it would be prohibitively expense to laboriously hand check all 420,260 pen-and-paper signatures, election officials make it only moderately prohibitively expense by using arcane formulas to randomly sample the inky scratchings on bleached dead trees that they've received by the heaping boxful, usually on the last possible day allowed by law.

This means that clerks must manually compare the small percentage of signatures actually being checked against the signature submitted by the voter when he or she originally registered to vote. I understand that they use quite modern scanning and screen projection methods to do these checks, but I somehow always imagine a lot of in-line skaters scurrying around a large concrete warehouse when I think about how the signatures are validated under the current system.

It was suggested, back in times when the implicit sexism of the stereotype was allowable, that if the telephone company (there was only one then) couldn't depend on new advances in telecommunications technology to handle the rapid increase in call volume, then it would take every woman in the United States working as an operator to accomplish the same amount of switching.

If we wanted the same performance out of our deregulated, multi-national, integrated data-and-voice networks today, and wanted to do it with humans, we couldn't do it at all, both because there wouldn't be enough of them and because they would not be capable of the fast, sophisticated data transformations which computers and networks are able to perform.

If we relied solely on human (mostly women, ironically) agents to process the manual signatures now used to qualify initiatives for the ballot, we'd end up with a process that is expensive, tedious, error-prone, and rag-tag. Wait a minute. That IS what we have.

But digital signature technology, which your companies have pioneered, established, and grown, could do away with all of these antiquated anachronisms. Instead of standing in the rain, being chased away by angry store owners, postal employees, and dogs, petition circulators could stay indoors or even vacation in Canada if they liked. Citizens, instead of being barraged by entreaties to sign petitions they've never heard about, don't understand, and don't care about, or brow-beaten by overzealous circulators, or frustrated because they are being asked to consider an issue and a resolution of it that may be of great moment when they are already a half-hour behind their hectic schedule, could read, study, and contemplate these proposed laws for as long as they liked from the comfort of their home or office (not on company time, of course).

They could access supporting materials, listen to or read opposing views, chat with others interested in the issue. Then, if they decided they wanted to put the measure up for a vote of the people, they would go to the proper page, invoked their stored digital certificate through the use of their unique, private, inviolate password, and digitally sign the petition.

[It's often said that what we call "e-mail" will soon just be called "mail," and what we call "e-commerce" will soon be called just "commerce." When Smart Initiatives come into general use, they will certainly speed the arrival of the day when what we now call "digitally signing" will be called "signing."]

Of course the advantages inherent in the digital signing of official petitions do not accrue only to their circulators and signers. They also ensue for the election officials formerly mired in the plethora of paper constituted by all those flat dead trees with ink markings on them. Now, instead of checking a small percentage of signatures, they can check all of them. Instead of relying on human eyesight and memory to encode and decode images and parts of images, fast, accurate, powerful servers will do all the encoding and decoding needed to determine the validity of the digital signatures. Valid digital signatures on the petition will be counted towards the required total. Invalid ones will be rejected. Totals will be calculated at the speed of thought. No fuss, no muss, no bother.

It's not just the telephone system that couldn't be run at its current level without computers and networks. It's just about every activity we encounter in our daily lives, including, among others, airlines, hospitals, public safety, telecommunications, national defense, the provisioning of food, the operation of our power grids. You get the picture. But there is one sector where computers and networks do not yet hold sway, and that is the elections sector.

The two domains that are linked by elections, politics and government, have been moving rapidly to adopt new technologies to better and more cost-effectively carry out their respective missions, namely electing candidates and administering bureaucracies. But the crucial connection between politics and government in a democracy, the elections by which the citizenry makes its choices between alternative candidates or propositions, has remained remarkably immune to the wildfire of "creative destruction" that the Internet has unleashed across the economy, society, and culture.

The reason for this technological lag is not technological, but political. The initiative process, frequently the agent of changes that are controversial, disruptive, or strongly-resisted, and that often involve the re-distribution of political power, are not much appreciated by the powers-that-be, especially elected representatives, and, sometimes, judges. Recent years have witnessed, and this year continues to witness, concerted efforts by political incumbents to limit and weaken the initiative process.

Things apparently got so bad that David Broder, universally-acclaimed as America's foremost political reporter, thought it necessary to write a book, called "Democracy Derailed," in which he railed against the initiative process as a tool for self-indulgent rich guys bent on having a little fun by spending a lot of money to persuade people to support their nefarious schemes. The book was not well-reasoned, in my judgment, but it was a bell-weather reflection of the fear held by many incumbents (in this case the incumbent "America's foremost political reporter") that letting ordinary people propose and vote on the laws and spending priorities they want their government to enforce and implement, respectively, is extremely inadvisable and had best be brought to heel, if not eliminated, as soon as possible, in order to preserve both democracy and the republic.

I disagree with David Broder on this. While the disproportionate influence of a few rich people in politics and government ought to be guarded against wherever it arises (and Broder, surprisingly, has nothing to say about the disproportionate influence of a few rich people wielded through the "campaign financing" system), the initiative process is remarkable in that it often provides the only means by which ideas and groups excluded from power can have an impact. Whether from the right or from the left, or any part of our new, multi-dimensional political spectrum, individuals and organizations with innovative ideas, fresh perspectives, or long-standing grievances can use the initiative process to bring their issues into the mainstream, have them subjected to discussion and debate, and offer them to their fellow citizens as a way of moving forward on the issue.

So I want to say that not only is the digital signing of initiative petitions a cost-effective, elegant, energy-efficient, and generally cool way of qualifying initiatives for the ballot, but the ease and cost-effectiveness that it will provide to initiative circulators will serve as a countervailing force against the growing crescendo of voices calling for higher signature counts and more restrictions on the rights of physical circulators.

Having made the case for the use of digital certificate technology as the preferred means of signing initiative petitions, I'd like to say something about actually converting this proposal into policy.

Ideally, the several state legislatures would immediately understand the value of these suggested technopolitical reforms, and enact them forthwith. Practically speaking, this is not going to happen, for two primary reasons. First, although it's improving, the general level of technical understanding among state legislatures is not yet in sync with the rapidly evolving Internet landscape. And second, no one likes to give up power, and state representatives are no exception. Making it easier for the people in their constituencies to make the laws under which they live would undermine their authority, their power, and their ability to collect "campaign contributions" from special interests. So the path to ubiquitous e-democracy through a universal PKI does not run through the state legislatures.

However, more than 20 states have the initiative process, established a century ago precisely to circumvent the recalcitrance of legislatures in thrall to that era's special interests. By laboriously and expensively collecting voter signatures on petition forms, it would be possible to place initiatives on the ballots in order to reform existing government procedures and replace them with a more popular and a more technologically-advanced alternative.

This is what I set out to do by creating the Smart Initiatives Project.

In the era of smart cards, smart roads, and smart bombs, I figured that the political system could use its own smartness upgrade. So, as I outlined earlier, Smart Initiatives would put the power of the Internet and PKI at the service of political reform, and allow governments to leverage technology to improve the responsiveness of the democratic process.

Right now, I'm concentrating my efforts on creating a Smart Initiative law for California. Having drafted a conceptual version of the proposal earlier this year, I collected the requisite voter signatures on it at UCLA, sent the draft to the Office of Legislative Counsel in Sacramento (the same group that writes laws for legislators and their committees), and a few short months later, got a nicely-written, legalistically-phrased document which is now called the Smart Initiatives Initiative.

It's kind of a boot-strapping operation, using the old initiative process to bring in the new one. As you can tell from its name, it is a proposal that seeks to change the very way such proposals are handled in the future. It is an attempt to use the tools of reform as they now exist to transform them into something more powerful, more useful, more capable of easy upgrades as politics and technology evolve. But it is a reform that, unfortunately, needs to employ the existing archaic, inefficient and expensive methods it would at least partially replace in order to reach the ballot and be considered by the voters of California.

It costs one million dollars to qualify a ballot initiative in California. If the Smart Initiatives project can raise that much money in a timely manner, the Smart Initiatives Initiative will go before the voters of California, probably in the spring of 2002. If it passes, the State of California will be required to establish itself as mega-Certificate Authority, and to provide every adult in California with a digital certificate on a smart card and also make the certificate accessible, through passwords known only to its user, from any suitable electronic device.

Now isn't that something every one of you here today would like to see happen?

The Smart Initiatives Project is also working to launch similar efforts in a number of other states with the initiative process, including Washington State, Oregon, Arizona, and Massachusetts. Qualifying a Smart Initiatives Initiative in these states is considerably less expensive than doing it in mega-state California. Given sufficient funding, it would be possible to bring Smart Initiative campaigns to over twenty states, and, if it passed, to have all those states be required to set up this same kind of CA and distribute millions more certificates to their citizens.

For better or worse, it all comes down to money. I've thought this up, written it, submitted it, pursued it, because I believe that democracy and every citizen would benefit from having the right to use Smart Initiatives. But I don't have one million dollars. As much as this effort is designed to replace existing ways of doing political business, the fact remains that we still have to do business the old-fashioned way in order to create the opportunity to do business in a new-fashioned way.

That means we have to operate within the constraints of contemporary political rules, the most important of which is, "you get what you pay for." Everyday, special interests pursue their corporate goals by financing candidates, especially incumbents, who are in accord with their views and who tend to look favorably upon the expenditure of public monies for the products of the aforementioned company or who favor a hands-off regulatory approach to that company's industry.

The situation is no different here with the Smart Initiatives Initiative. Either the companies that stand to reap a considerable benefit from its passage support it, or else it will not succeed. I've identified three classes of company that I think will most benefit from the Smart Initiatives plan:

1. PKI suppliers
2. smart card companies
3. electronic services companies (insurance, HMOs, banks)

PKI vendors will benefit in several ways from the passage of Smart Initiatives. First, Smart Initiative states would need to buy expertise, software, hardware, training, and so on from PKI and related vendors. Second, the deployment of such large numbers of certificates would mean an overnight leap to almost ubiquitous distribution in Smart Initiative states, and, through the principle of network externalities, thus making

everyone's digital cert now even more useful, since so many others would have them, too. This would allow secure authentication to become a commonplace aspect of online transactions and both facilitate and enhance the centrality of PKI in e-commerce and related areas. Third, by upgrading the PKI and the political process in the states which are early adopters of Smart Initiatives, these jurisdictions will become models for others, thereby spurring further deployment in areas that fear being left behind, in some cases even by administrative order or legislative action.

That's if the Smart Initiatives Initiative qualifies for the ballot, in one or more states. But even if it only qualifies for the ballot, and we go ahead with a campaign to pass it, the earned news coverage that such a measure would generate would, it seems to me, be worth much more than could ever be gained by the expenditure of a comparable amount of money in any public relations or advertising campaign.

Digital certificates and PKI are not on most Americans' radar screens. They might not be on most of their screens even after a hearty campaign about them. But many more opinion leaders, company presidents, government agencies, news organizations, and members of the general public would know what a digital certificate is and maybe even how it works, and especially what it's good for, after a campaign to pass a Smart Initiatives Initiative came to their state.

So I think that if Smart Initiatives passed, they would be tremendous boon for the PKI community. If they failed to pass, but managed to educate and inform people about the value of PKI, they would still have earned their keep and done a lot to further the effort to make such tools ubiquitous.

I've been thinking about the relationship between technology and politics for almost a quarter century, since I was a special correspondent covering science and politics stories at **The Stanford Daily**. I would report stories involving the intersection of various technologies and the political process, mostly controversial subjects like swine flu inoculations, nuclear power, and recombinant DNA. I noticed that, with the exception of Dr Edward Teller on the subject of nuclear weapons, neither the political actors nor the technologists seemed to understand the others' fields. And yet the core of the controversy usually involved how to make an informed political decision involving some bit of scientific procedure or data, which was itself often being contentiously argued over. So the situations could get complex.

Around that time I decided that I could do myself and everyone else some good by trying to bridge the gap between technology and politics, by combining a journalist's respect for the truth and skills at ferreting it out and publicizing it, with a teacher's vocation of educating people about facts, demolishing myths, and helping anyone who cared to to gain the knowledge necessary to make the most informed decisions possible.

I did that by running for Congress in 1980 on a platform of "Compute, Don't Commute." From what I understand traffic is like now on the Central Expressway, this

may have been one of my most perceptive suggestions. I did it when, in the mid-80s, I co-founded the Cable Communications Cooperative of Palo Alto, Inc., an eventually abortive attempt to put a community in charge of its own telecommunications system. I did it when I wrote the Virtual Voting Rights Initiative in 1996 and the California Internet Voting Initiative in 1999, the first of which mandated the same Smart Initiative system I'm advocating today.

And I'm doing it now by proposing and working to pass the Smart Initiatives Initiative, because I believe it will empower all of us to use technology in a directly political way, and give us as citizens the same effectiveness that we have as Napster users. In the case of Smart Initiatives, that means to have the power to choose our laws as easily (but perhaps with more in-depth consideration) as we choose our tunes.

The difference that technology is making in our daily lives and the changes it is bringing to the world are enormous. Its potential to facilitate our liberation or our enslavement is equally huge. Unless we want to be mere consumers, engulfed and devoured by an all-powerful, all encompassing entertainment/telecommunications monolith, that sees us as commodities, as "eyeballs" to be mesmerized and wallets to be plundered, then we need to do something serious now to increase the power of individuals and groups to exert some control over our own destinies.

Fortunately, we have all the tools we need to do that. We have a Constitution and over 200 years experience using it, making us the market leader in continuous years of democratic self-rule. And we have the technological tools we need to maintain and expand the practice of our democratic rights.

What we still lack, however, is a commitment to putting our high tech tools to work in the service of our highly valued democratic principles, a commitment to applying them in a way that counts, and is not merely an advisory poll. If the states adopt the Smart Initiative idea, they will, in the medium and long run, save themselves money, enable themselves to deliver e-government services on an unprecedented scale, spur e-commerce, and, not incidentally, create the infrastructure for a digital democracy that can and will synergize the complementary strengths of democratic safeguards and network-based computing. Put another way, Smart Initiatives stands for "political reform through Internet power." Properly and adequately financed, it seems to me a powerful, even unbeatable, combination.

Victor Hugo famously wrote that "nothing in the world is as powerful as an idea whose time has come." The idea of Smart Initiatives meshes multiple themes in networked computing and our political practice. It enhances the political space, the computing space, and the commercial space. Its adoption everywhere will be good for PKI community. Perhaps Smart Initiatives is an idea whose time has come.

Thank you.

In November, 2000, the e-government bulletin (UK) ran an article I wrote to introduce British readers to the idea of Smart Initiatives.

The Teledemocracy Revolution that Never Was

(November, 2000)

Read the original at:

http://headstar.com/egb/issues/November2000.txt

```
E-GOVERNMENT BULLETIN
The Email Newsletter On Electronic Government,
UK And Worldwide.

ISSUE 93, NOVEMBER 2000

IN THIS ISSUE:

Section Three: US Election Special
- Digital Petitions

SECTION THREE: US ELECTION SPECIAL
- DIGITAL PETITIONS

THE TELEDEMOCRACY REVOLUTION THAT NEVER WAS

The two most common criticisms of fully-fledged, remote Internet voting
are that it's not safe and that it's not fair.

The safety argument says that securing Internet voting against
cybervandals and perpetrators of electronic election fraud simply can't
be done, given existing technologies. The argument against Internet
voting as unfair revolves around the so-called 'digital divide', the
uneven distribution of access to the Internet within society.

There is something to be said for each of these objections. However, a
more powerful complaint about Internet voting, which comes from a
purely political viewpoint, is simply that it won't actually have much
effect on the operation of the political process or the distribution of
power in advanced societies.

The widespread implementation of remote Internet voting will be
important to the companies that hope to make money by providing out-
sourced election services to political jurisdictions. It will make
voting easier and more convenient for those voters who already vote.
Beyond that, there will be little to distinguish the political
landscape of a jurisdiction using remote Internet voting from one using
any of the legacy systems now in place.

If the current election campaign has shown anything, it's that a
political system organised around and dominated by money, packaged
candidates, and show-biz production values is, at best, able only to
generate the same kind of interest created by a mediocre television
series and a resoundingly negative reaction, ranging from apathy to
disgust, on the part of a majority of those who are supposed to be
deciding how they are governed. After months of this, letting people
```

vote for their favourite candidate on the Net instead of at the traditional polling place just doesn't make any difference.

This isn't to say that the Internet is not capable of mediating the political process in ways that would give citizens more choices, that would significantly reduce the influence of money in the process, and that would give them more control over the outcome of disputes over issues.

But what's required to bring about these genuine reforms is the legal recognition of citizens' right to have an impact online and the practical means to accomplish this. And 'having an impact' in this context does not merely mean the right to be heard, it means the right the to actually participate in the making of decisions.

More and more, 'Internet democracy' is being forced into various definitions that don't actually give people any power, merely the appearance of it. Elected representatives, for years reluctant even to give out their e-mail addresses (if they had them), now want to 'listen' to their constituents online. Their staffers in charge of listening build websites for this purpose and log the incoming email the way they used to (and still) log the paper mail.

Sometimes the tabulated results even figure into decisions made by the representatives. But often they don't, and often they are quietly repressed by the whispered 'suggestions' of major campaign contributors that may run counter to the expressed desires of the listened-to but ignored mass of citizens.

Listening to the concerns of citizens over the Net is good. Posting campaign contributions in a timely manner on easily-accessed and easily-understood web pages is good. Letting people pay their taxes, apply for licenses, or find out about government services online is very good, since it saves government money and makes the lives of citizens easier. But any of these, or all of these, is not electronic democracy, it is not using the Net as it could be used to make government better, not 'more responsive,' but 'more democratic.'

Making government more democratic by means of the Internet means changing the laws and institutional arrangements we have now to include the active, daily participation of regular citizens in the formulation, discussion, and enactment of the laws by which society is governed. It means letting us govern ourselves with the best tools available, including especially the Internet.

So, is there an existing political process or structure that could be cyberized and then serve as a lever by which the actual will of real citizens can play a substantial role in the formulation and creation of laws and, through these laws, public policy.

It so happens that in the United States – or in about half the US states, at any rate - there is. It's called the initiative process, and allows citizens unhappy with the inaction of their elected representatives on a certain issue to formulate their own proposed law addressing that issue.

Proponents of such an initiative are required to collect a certain number of signatures of their fellow citizens on petitions. If they collect the requisite number of valid signatures, the proposed measure goes on the next election ballot. Voters can then pass or defeat the initiative at the polls.

In practice, the most significant element in getting an initiative on the ballot is the need to raise the necessary money to pay professional signature-gatherers. In California, where initiative proponents need to collect 419,260 valid signatures, the going rate for these services is approaching one million dollars.

So what's the best course of action for a group or individual with a complaint or proposal they'd like everyone to vote on, but without a million dollars? Right now, there is nothing they can do. But if signatures could be collected over the Internet, it would be a different story.

That story could be about to unfold, thanks to a reusable, 'open source' online petitioning initiative called the Smart Initiatives Initiative. In the next issue of E-Government Bulletin we will set out how this works, and how it could shift the balance of democratic power towards the citizen in a new 'open source democracy' in the US.

* Article by Marc Strassman, Author of the Smart Initiatives Initiative and Founder and Executive Director of the Smart Initiatives Project. See: http://www.smartinitiatives.org

On November 18, 2000, I sent an open e-mail to Kevin Shelley, the Democratic Majority Leader in the California Assembly. Mr. Shelley had authored a bill to begin testing Internet voting around the state. The bill passed the Legislature, but was vetoed by Democratic Governor Grey Davis. I couldn't help noticing the similarity between the language and approach in Governor Davis' veto message and the language and approach in Governor Pete Wilson's message vetoing AB44 in 1997, so I wrote the Majority Leader to suggest that we work together to upgrade and reform California's electoral technology. I have since been in discussions with his office about doing so.

An Open E-mail Letter to the Majority Leader

(November 18, 2000)

On October 13, 1997, when Pete Wilson vetoed AB44, a bill ordering the Secretary of State to study Internet voting in California, he (or a staff member) wrote:

To the Members of the California Assembly:

I am returning Assembly Bill No. 44 without my signature.

This bill would require the Secretary of State to assign a task force to study the creation of a digital electoral system and to report the results to the legislature.

I am supportive of reasonable approaches to campaign and election reform. As such, I have recently signed Senate Bill 49 (Karnette, Ch. 866) which will establish an electronic filing disclosure system. The provisions of that bill will allow technology to be introduced into the campaign finance system in a reasonable and thoughtful manner yet provide adequate safeguards against misuse.

Unfortunately, I cannot say the same for AB 44. This bill calls for a task force to study establishing a digital electoral system that would, among other things, allow individuals to register to vote, sign an initiative petition and cast their vote through the use of digital technology. The use of such a system will compromise voter confidentiality and generate significant opportunities for fraud. Since the digital system would be available only to those with access to computer terminals, it would not replace the current system. Accordingly, the use of two systems would complicate voter verification procedures, further compromising the electoral process.

Although current encryption technology is making advances in providing a more secure environment to prevent tampering by third parties, no one can yet guarantee a completely safe, tamper-proof system. Without such a guarantee, a study is premature.

Cordially,

PETE WILSON

Three years later, on September 28, 2000, his successor, Grey Davis, vetoed AB 2519 with this message:

To the Members of the Assembly:

I am returning Assembly Bill 2519 without my signature. This bill would establish an Internet Voting Pilot Program in three counties to test the viability of a system allowing voters to cast their ballots via the Internet in general elections to be held before July 1, 2003.

While I am a strong supporter of increasing both the number of registered voters and voter participation in the state's elections, this bill is premature for several reasons.

Before Internet voting can be successfully implemented, security measures to protect against fraud and abuse must be more fully developed. Other states are experimenting with online voting with varying degrees of success. I am not convinced the necessary safeguards are in place to begin this experiment in California.

Accordingly, I am returning AB 2519 without my signature.

Sincerely,

GRAY DAVIS

I read yesterday in the Business Journal of San Jose that you are going to try again to get authorization for a limited form of Internet voting in the California. I wish you every success.

I've been trying to achieve the same goal since 1996. My first effort was the Virtual Voting Rights Initiative, a copy of which is attached. The VVRI provided for voter registration, initiative petition signing, and regular voting over the Internet, with voter identification and authentication to be provided by digital certificate.

The VVRI never qualified for the ballot. Instead, it was submitted by Assemblymember Kevin Murray on December 2, 1996 as AB44. After being amended into a study bill and not an implementation bill by Assemblymember Murray at the recommendation of Secretary of State Bill Jones, it eventually passed both houses, only to be vetoed by Pete Wilson, as referred to above.

In 1999, I drafted a second effort to bring Internet voting to California, the California Internet Voting Initiative. The CIVI would have authorized Internet voting only on systems that met certain listed specifications, the details of these specifications to be determined by the Secretary of State. The CIVI never made it to the ballot, but you can read it and see a website designed to qualify it under existing, legacy, regulations, at: http://www.civix.org.

This year, I wrote and am now circulating the Smart Initiatives Initiative, which would require the State to establish a California State Certificate Authority to issue digital certificates (and smart cards) to every adult Californian, and allow all of us to use these certificates to digitally sign initiative and other official petitions online.

The Smart Initiatives Initiative is completely silent on the subject of Internet voting, but does allow citizens to conduct e-government transactions with the State using their certificates, in situations where the state chooses to allow this. You can read the SII, and download a valid petition form for it, at: http://www.smartinitiatives.org.

Smart Initiatives implicitly relate to Internet voting in at least two ways. Qualifying, passing, and implementing Smart Initiatives would result in the distribution of approximately 20 million digital certificates and smart cards within the State, and it would give us a chance to use them on a regular basis for political purposes, as well as for commercial ones. This would let individual citizens and the State itself gain valuable experience in the use of the Internet for authenticated political transactions. This experience could provide valuable information for determining the best ways to implement other authenticated political transactions (such as Internet voting).

Secondly, putting Smart Initiatives in place would mean that it wouldn't cost a million dollars to qualify an initiative to implement Internet voting, but a lot less. Such a California Internet Voting Initiative could be qualified and passed even if Governor Davis, as he has promised, continues to oppose such a reform.

All this background now comes to its point. I support your efforts to bring Internet voting to California, but the Governor, who must sign any legislation you bring to him to do this, does not. You can keep passing bills to move us forward, but he can keep vetoing them.

But he can't veto an initiative.

So I'm suggesting that we work together now to pass Smart Initiatives and, if you're interested, to pass, before or after Smart Initiatives is implemented, an Internet voting bill of the type you favor, by means of the initiative process.

No one has more experience than I do in writing and advocating Internet voting initiatives in California. No one has more experience than you do in trying to legislate Internet voting into existence through the Legislature. Between what each of us knows and can do, I expect we could succeed, regardless of the Governor's attitude on this issue.

I hope we can talk soon about moving forward together on this.

Sincerely,

Marc Strassman
Executive Director
Smart Initiatives Project

While the debacle in Florida's November, 2000, election was still going on, I published an article in the Sacramento Bee's "Forum" section about that old standby, Internet voting, and called for "making Internet voting software Open Source" as a way of preventing the kinds of failures that characterized the recent voting in Florida.

Electronic voting not just point & click

(November 26, 2000)

Many people are saying that the voting mess in Florida demonstrates the need for Internet voting now. The situation in Florida is the combined result of using antiquated technology within an outmoded administrative model in an election so close that the overall dilapidation of the entire system could no longer be hidden.

But converting a system based on IBM 360 technology from the mid-60s to a remote Internet voting system, and expecting voters who were baffled by stylus-and-punch-card technology to instantly grasp drag-and-click systems, may be overly optimistic.

I voted this election in Los Angeles on a touch-screen system from Global Election Systems. It was fast, fun and, I assume, accurate. I was validated to the system with a smart card that was personally programmed for me by an election worker, who "charged" it with the right to vote once in my district after I signed and gave her the back cover of my voter pamphlet, which had been mailed to me.

This was at least as secure as the standard procedure here, which prohibits election workers from asking for any ID from prospective voters. If I, and all other voters, had already had a smart card that contained my name and address, we all could have used that card to vote on these touch-screen machines, without any additional intervention from on-the-scene election workers, who could then have concerned themselves principally with helping people figure out how to insert the cards in the machine and how to select by touch the candidates and initiative and referendum options of their choice.

But this approach is not remote Internet voting. And I believe that at this point in time, it is a better way to ascertain the will of the people.

Remote Internet voting has yet to overcome some important technical and administrative problems. The most interesting one, in my view, is what I call the problem of "anonymous authentication." Electronic voting, under our democratic system, needs to be anonymous. That is, the authorities need to be unable to determine who has cast any particular ballot. On the other hand, each voter needs to be authenticated, one way or another, to a greater or lesser degree of certainty.

With paper ballots of any kind, the authentication occurs when the election worker checks the voter in and thereby checks his or her name off the list of people who are entitled to vote. Remote Internet voting systems can do this by identifying a person wanting to vote by means of a PIN, a password, or, more rigorously, a digital certificate.

Paper ballots are anonymized by tossing them into the ballot box, where the uniformity of every ballot (apart from their content) effectively makes it impossible to know which person cast which ballot. Thus are voters able to be both anonymous and authenticated, using paper ballots.

While it may be theoretically doable, no one has yet explained to me intelligibly and persuasively exactly how it's possible to simultaneously authenticate and anonymize a ballot in cyberspace, where there is no way to create the virtual equivalent of a ballot box in which to effectively shuffle the electronic ballots so no one can tell who voted how. Any system that attempts to anonymize the ballot of a person already authenticated to vote is going to leave an electronic trail of the process by which it has attempted to perform the anonymization. Working backward along that trail will eventually reveal whose ballot it was that was "anonymized," which is, of course, no anonymity at all.

One can argue that, by making it illegal to "de-anonymize" electronic ballots, the practice can be prohibited. When has making something illegal ever succeeded in keeping it from happening? There are other technical problems with Internet voting. The California Task Force on Internet Voting has highlighted most of them, including the use of viruses and Trojan horse programs to block, change or modify remotely-voted electronic ballots, and the use of denial-of-service attacks to effectively shut down election servers during the crucial and limited hours of an election.

There is also the infamous "digital divide," much discussed already, which is regularly invoked, not as an argument for providing every citizen with the means and the training to effectively use the Internet for civic activities, such as voting, but as a reason for denying everyone the opportunity to so use it.

Here is a final note on the lessons of Florida as they apply to remote Internet voting. If and when these technical and social obstacles to the use of the Internet for remote voting are overcome, we should decide now that the software used for such a system be Open Source. Open Source software means software where the computer code that runs a program is in the public domain. It is freely available on the Net. It can be examined and inspected by anyone who wants to.

Making Internet voting software Open Source will eliminate the undesirable situation where counties use propriety Internet voting software programs that are closed to the public, which makes the public jurisdictions using them dependent on private, for-profit companies for the maintenance and possible upgrade of the code that they, and their citizens, depend on to give them free and fair elections.

As we know very clearly from the current imbroglio in Florida, confidence in the system is damaged by fouled-up election procedures, putting the continued viability of that system into question. When the current obstacles to Internet voting are eventually overcome, let's be sure the software will not further undermine public confidence in the election system, even before it is used.

Marc Strassman is founder and executive director of the Smart Initiatives Project (www.smartinitiatives.org)

The Open Source software paradigm can provide a model, as well as actual tools, for building a transparent, secure, and effective form of self-government. I expanded this idea of "Open Source Democracy" in an article I wrote for the e-Government Bulletin (UK), which ran it in their December, 2000, edition.

Towards an Open Source Democracy

(December, 2000)

Read it in place at:

http://headstar.com/egb/issues/December2000.txt

```
E-GOVERNMENT BULLETIN
The Email Newsletter On Electronic Government,
UK And Worldwide.

ISSUE 94, DECEMBER 2000
Section Four: US Case Study
- Digital Petitions

SECTION FOUR: US CASE STUDY
- DIGITAL PETITIONS

TOWARDS AN OPEN SOURCE DEMOCRACY

In our last issue, we looked at how US citizens can initiate
legislative measures in some states through the 'initiative process',
under which they are required to collect a certain number of signatures
on petitions. If they collect the requisite number of valid signatures,
the proposed measure goes onto the next public election ballot, and
voters can then pass or defeat the initiative at the polls.

The nearest one can come at the moment to collecting signatures over
the Internet for these purposes is to create a 'PDF' graphical file
version of the initiative petition, post it on the web or email it to
those requesting it, and let them print it out, sign it, and post it
in.

This is an inelegant and often difficult way of proceeding, given the
need to print the forms out on two sides of the paper, compress the
text to fit in limited space and so on.

The obvious way to have people sign initiative petitions over the
Internet is to let them sign them using digital certificates. As of 1
October 1 2000, the US federal E-Sign bill is in effect, authorising
the use of these online credentials to sign contracts online. It's only
logical to say that if digital certificates are now good enough to sign
multi-million dollar contracts, they ought to be good enough to
indicate your desire to see a particular legislative proposal voted on
in your state.

The 'Smart Initiatives Initiative' currently being circulated in
California was created to implement this idea in practice. Its primary
aim is to allow people to vote on a measure requiring the state to
provide all citizens with a digital identity certificate. The project
```

has until March 12, 2001 to collect 419,260 valid signatures of California voters who want to see it on the primary ballot in 2002.

With Smart Initiative petitions, as with any petition, verifying the identity of the signer is key. Still, while the identity of the signer must be knowable by the authorities that check the signatures, it need not be made available to the general public. In fact, under the provisions of the proposed Smart Initiatives Initiative, it is protected by the same restrictions on disclosure as are legacy pen-on-paper signatures.

Moving the initiative-signing process online benefits all parties involved. For proponents, it reduces the cost of circulating their petitions by several orders of magnitude. For citizen-signers, it makes it much easier to study a proposed initiative and then, if they want, to sign it from home, office, or other location.

For the election officials who currently need to spend months checking a mere random fraction of the submitted signatures before extrapolating according to arcane formulas to determine the 'official' number of valid signatures, the power and convenience of a digital system to rapidly and comprehensively tabulate the results would be a much-welcomed improvement.

Because the first major provision of the Smart Initiatives Initiative is the distribution by the state of a high-level digital certificate to each citizen, citizens-as-consumers and citizens-as-commercial entities will benefit as well. They will be able to use these certificates not just to sign initiative petitions but to buy insurance, order groceries, tele-commute, check their children's homework assignments, and do anything possible now or in the future that requires them to establish their identity online.

At a minimum cost of ten dollars each, however, providing 20 million Californians with a digital certificate will not come cheap. Hence another proposal that could lower this cost and pay other dividends as well, a proposal to develop Open Source Public Key Infrastructure (PKI) software.

Open Source software is computer programming code that is not secret. The instructions that make it run are available openly to everyone. It makes sense to consider the creation of an Open Source PKI Foundation to facilitate the creation of Open Source PKI code, not only to save the State of California a lot of money, but also to set the stage for using open source software to eventually provide Internet voting services.

In addition to the cost savings for the government, building a PKI and using Internet voting software where the internal code is open would mean that it could be properly understood by the people who use it. It would provide a technological analogue of the political openness and participation that is central to this entire vision of what could be termed 'Open Source Democracy.'

Nor would it be inappropriate, eventually, to move many other existing and future e-government applications to an Open Source model. In such an environment, we could avail ourselves of a seamless web of

information, decision-making, and functionality. As the reach and power of the web steadily evolve, these principles of openness and self-determination would be a concrete realisation of the long-sought ideal of 'government of the people, by the people, and for the people.'

* Article by Marc Strassman, Author of the Smart Initiatives Initiative and Founder and Executive Director of the Smart Initiatives Project. See: http://www.smartinitiatives.org

During the first week of December, 2000, I sent an e-mail to California Secretary of State Bill Jones, pointing out what I saw as similarities between legislation he was supporting and the Smart Initiatives Initiative. I asked for his support for my efforts. Of course, there was no answer from him or his office.

Open E-mail Letter to California Secretary of State Bill Jones Asking for Support for Smart Initiatives Initiative

(December 6, 2000)

Dear Secretary Jones:

I was examining your "California eGovernment Plan" when I read about the "California Digital Identification Act," which would "require the Department of Motor Vehicles (DMV) to work with Certification Authorities to provide one and only one digital signature key pair to any Californian who requests one and provides proof of identification to the DMV."

The Smart Initiatives Initiative, now circulating, says, in pertinent part:

11790. (a) The Department of Motor Vehicles, the Secretary of State, the Department of Information Technology, and the county registrars of voters, shall collaborate to establish the Digital ID Issuing Authority of the State of California, whose mission shall be to efficiently and cost-effectively provide California residents with a high-level digital certificate in an easy-to-use form.

What can I do to help you realize your plan to provide Californians with secure digital identification?

Your plan for eGovernment goes on to say:

Upon passage of this legislation, DMV-issued digital identification will be deemed sufficient proof of identification for all electronic transactions with public entities that would otherwise require proof of identification.

The Smart Initiatives Initiative goes on to say:

11791. (a) A digital certificate issued by the Digital ID Issuing Authority pursuant to Section 11790 shall be accepted by any state entity that offers secure transactions over the Internet, as complete and adequate proof of an individual's identity...

Since your plans for eGovernment and the content of the Smart Initiatives Initiative on these points are so close, almost word for word identical, I hope you will consider supporting my efforts to implement your goals by supporting my efforts to qualify and pass the Smart Initiatives Initiative, or to incorporate its major elements into the recommendations of the Speaker's Commission on the California Initiative Process, or

include it in whatever legislation eventually authorizes and funds the Department of Motor Vehicles' purchase and distribution of digital certificates and smart cards as driver's licenses and state ID cards.

I also hope you will support my efforts to ensure that "all electronic transactions" as referenced in your plan will be construed to include the digital online signing of initiative and all other official government petitions, including referenda, recall, in lieu, and nomination petitions at all levels of government within the state.

You might also want to read "Jump-Starting the Digital Economy (with Department of Motor Vehicles-Issued Digital Certificates), a briefing paper published June 1, 1999, by the Progressive Policy Institute, which addresses the justification, implementation, and implications of the policy we both support of assuring that California go from worst to first by equipping its citizens with digital certificates. You can access this paper at:

http://www.ppionline.org/ppi_ci.cfm?contentid=1369&knlgAreaID=107&subsecid=126

Please feel free to contact me to discuss any of this at your convenience.

Sincerely,

Marc Strassman
Executive Director
Smart Initiatives Project

A week later, I wrote an article that addressed the finances of Smart Initiatives.

Fuzzy Math for Smart Initiatives

December 14, 2000

Over the last few weeks, I've been checking with knowledgeable sources to put some real numbers on the elements involved in implementing Smart Initiatives in California.

Here are the basic numbers:

Smart Initiatives in California means issuing smart cards and digital certificates to approximately 25 million people, the number of adults 18 and older now living in the state.

A very large smart card company, an industry leader, told me it would cost $5.98 each to provide the state with 25 million smart cards. Let's round that up to six dollars each. This means it would cost $150 million to provide a smart card for each adult Californian. This price does not include "personalization," or the insertion on the card of the digital certificate and the placement on the card's surface of a picture ID, a holographic image to prevent counterfeiting, or any other additional information, like name, address, height and weight, and so on. That's one hundred and fifty million dollars for the blank smart cards.

I got pricing on the digital certificates, the computer code that will allow for the actual "digital signing" of online initiative petitions, contracts, or other transaction forms, from two large and leading digital certificate companies. One of them quoted me a price of fifty cents each for 25 million certs. The other quoted me a price of one dollar each at that quantity.

Let's do the math. At $150 million for the cards, an additional $12.5 or $25 million for the certs and a certain amount to get the certs onto the cards and also onto the desktops, laptops, PDAs, and cel phones of the end users, we can pretty safely say that the whole project could be accomplished for something less than but close to $200 million dollars.

Now, let's consider what it costs to validate the pen-and-ink signatures of citizens on paper petition forms, which is what Smart Initiatives is designed to supplement.

One source, an election official in the East (San Francisco) Bay, told me that it costs their department between eighty cents and one dollar to process a single signature submitted to them on an initiative petition. This official went on to say that a highly-skilled elections worker could check 200 of these signatures in seven hours, adding that the less-skilled temporary workers who are often required to check signatures is more likely to authenticate around 150 signatures in the same seven hour period. This official

also expressed a great deal of unofficial enthusiasm for automating this laborious process by means of the Smart Initiative system.

A second source, employed in a similar capacity in the Registrar of Voters office in a South Bay county, corroborated these figures, telling me that it was hard to pin down a definite estimate, since all kinds of variables (like messy signatures) were often involved in the validation process. Nevertheless, this official told me that the cost in that office to verify a single signature was between sixty cents and a dollar.

So, to make the argument for Smart Initiatives as compelling as possible and the math as simple as possible, let's assume that it costs one dollar to verify one signature.

Initiative petitions must be submitted to the Registrar of Voters offices in the county in which they were signed. Now, since some initiatives garner greater support in some parts of the state than others, petitions containing varying numbers of signatures to be certified will be received by the Registrar's Offices in different counties, and this distribution will vary from initiative to initiative. It's therefore not possible to say with any certainty what the cost to each county will be for a given initiative.

Let's assume that the figures from the two Bay Area counties are reasonably approximate indicators of what the costs for doing the checking are throughout the state.

To qualify an initiative for the ballot in California requires 419,260 valid signatures (if the initiative is a statutory one, meaning that it calls for changing or making a new state law) or 670,816 signatures (if the initiative is constitutional, calling for a change in the State Constitution). Many invalid signatures are commonly submitted.

There are two methods of checking the signatures. The Random Sample method checks a certain random sample of submitted signatures and uses complicated formulas to project the likely number of valid signatures in the entire mass of submitted signatures. There is also the Total Count method that, just like it sounds, involves checking every signature. Determining which method is to be used depends on other complicated formulas.

For simplicity's sake, and to make the case for Smart Initiatives as compelling as possible, let's say that 500,000 signatures need to be authenticated in order to qualify a single statutory initiative petition, more if it's a constitutional initiative. At our agreed-upon figure of one dollar per validated signature, that's half-a-million dollars to qualify each initiative.

How much this costs overall every year is, of course, a function of how many initiatives are submitted for certification, whether they're checked with the Random Sample method or the Total Count method, and whether they are statutory or constitutional initiatives. Two out of the five counties I asked to supply data have so far been able and/or willing to do so. My request to the Secretary of State's Office for statewide figures has as of yet not been answered.

One would, of course, hope that the methods of using ink, paper, cardboard, and many sets of hands and eyes to compare written signatures on the petition forms with the signatures on the registration cards stored in the Registrars of Voters offices are more precise, uniform, and reliable than the methods recently employed in Florida with limited success, but one can hardly know, or say for sure, that they are without more scrutiny of data not yet available to press or public.

What we can know for sure is that digital versions of initiative petitions, using the latest technology for secure online transaction processing, can process 200 petitions in seconds, rather than hours, and do so uniformly, according to established and recognized criteria. Like all digital processes, checking a digital signature for authenticity yields clearly-defined results. The signature is either completely valid, proven to have come from the person claiming to have made it and not modified in transit, or it is completely invalid, either not coming from the claimed sender or modified since the signing, or both.

There are no dimpled, pregnant, or hanging digital signatures.

Let's say that 20 statewide initiative petitions are submitted for verification every year in California. (Once the Secretary of State's Office provides real data, we can substitute it for our assumptions.) At half-a-million dollars each, that's 10 million dollars in signature-checking costs per year. Letting county election officials save that much, or close to that much, each year would give them at least part of the money they need to begin purchasing the DRE, or touchscreen, voting terminals that many seems to agree are an appropriate way to upgrade existing voting technologies, or to otherwise upgrade often antiquated Chad-o-Matic™ punchcard systems.

Obviously, taken in isolation, spending $200 million to save $10 million dollars is not a good investment. But distributing 25 million smart cards and digital certificates to every adult California is not something that will only impact the initiative petition signing process. There are at least two other areas where it will have a big effect.

The first is in the area of e-government, the direct delivery of information-intensive services to citizens over the Internet. Paying taxes and fees, applying for licenses, accessing secure data, submitting official documents, including especially legal briefs and other forms, and many other functions will become securely doable by 25 million Californians by means of the same digital certificates they will be using, if they so choose, to sign initiative petitions online, and which Smart Initiatives would put into their hands even if they never signed an initiative petition online or off.

It now costs one million dollars for a citizen or organization to qualify an initiative, and it costs the State half-a-million dollars to check the signatures on it. With Smart Initiatives technology (smart cards and digital certificates) in place, it might cost the circulators ten thousand dollars to qualify their initiative and the State five thousand dollars to validate the signatures on it. This is a cost reduction for both citizen and state of one hundred times.

Imagine what a similar reduction in costs would mean for taxpayers when the transition to e-government brings about a comparable reduction in State costs for administering its transactional processes.

The convenience, speed, accuracy, and trustworthiness of e-government transactions will benefit citizens. The power, synergy, reach, speed and lower cost of e-government transactions will benefit the State. The money saved by the State through e-government could go to enhance state services, be returned to citizens through lower taxes and fees, or some combination of the two. Proposals for the disposal of these savings could be made, fittingly, by citizens themselves through a Smart Initiative.

On top of these savings and increases in efficiency and convenience, there is also the massive economic effect of equipping 25 million consumers for participation in a wide range of existing and emerging commercial transactions, such as online shopping, now including even the purchase of big-ticket items such as cars and houses. It is already legal under the Federal E-Sign Bill to sign such contracts, but its provisions are rarely used, in large part because few people have digital certificates, experience using them, or even basic information about what they are, all limitations that will disappear with their universal distribution under the provisions of Smart Initiatives.

One should also note that the State Department of Vehicles is already considering providing every holder of a driver's license or a state ID card with a smart card and digital certificate as part of their driver's license or state ID card. If this happens, then the cost of instituting a system of Smart Initiatives will be trivial, even though the political benefits to citizens and the financial benefits to counties and the State will be substantial. And, as long as the digital certificates issued through the DMV are made valid for e-government and e-commerce transactions, the benefits listed above will also be realized.

The bottom line of all this fuzzy math is that digital logic, in the form of Smart Initiatives, can deliver a big gift to the State of California and all its citizens, if we have the imagination and will to let it.

During the same week when I testified before the "Speaker's Commission on the California Initiative Process," Sacramento's alternative newsweekly, Sacramento News & Review, ran a "Guest Comment" column I'd written for them, in which I said, in part, that "The stated purpose of the Commission is to reform the initiative process. Some believe its real purpose is to weaken the initiative process, which has never been very popular among legislators whose power and prerogatives it can seriously diminish."

Guest Comment

Small "e" democracy

By Marc Strassman

Recently, two highly-respected journalists, David Broder of the Washington Post and Peter Schrag of the Sacramento Bee, have written books blasting the initiative process as, respectively, the enemy of representative democracy and the nemesis of justice and equality in California.

I, on the other hand, believe that the biggest problem with California's initiative process is that it costs a million dollars to qualify one for the ballot. Accordingly, I wrote the Smart Initiatives Initiative, now circulating, which requires the state of California to issue every qualified person in the state a digital certificate that he or she could use to sign initiative petitions online using the Internet. This would mean that people and organizations could qualify their initiative through SignSite.org™ for a hundred times less than it costs to pay professional circulators to do the same work.

Perhaps because of these two books, or perhaps because of the perceived threat of the Smart Initiatives Initiative, California State Assembly Speaker Robert Hertzberg has established the Speaker's Commission on the California Initiative Process. I'll be testifying about Smart Initiatives at the Commission's hearings in Sacramento on Jan. 22.

www.smartinitiatives.org

The stated purpose of the Commission is to reform the initiative process. Some believe its real purpose is to weaken the initiative process, which has never been very popular among legislators whose power and prerogatives it can seriously diminish. I believe that the Commission needs to give serious consideration to the Smart Initiatives concept if it is to further the goals of the progressives who created the initiative process almost a century ago as a means of curbing the power of that era's special interests.

Other government entities ought to be involved in the implementation of Smart Initiatives. I believe that it would be most appropriate, both technically and politically, to designate the Department of Motor Vehicles as the so-called Certification Authority, the Office of the Secretary of State as the Validation Authority, and the Department of Information Technology as the Directory Services Authority to be the core elements in a California Digital Identification Authority (CDIA).

Supplying all Californians with advanced digital credentials under this system would enable not only Smart Initiatives, but smart government generally. E-government implementations would increase efficiency, save money, put state and local agency services at people's fingertips from anywhere and help restore the popular confidence in government that is evidently so lacking almost everywhere today.