The Bell™

Privacy, Security and Technology in Internet Voting

JULY 2000 | Published Online Monthly | Vol. 1 No. 3

www.thebell.net | ISSN 1530-048X

Mission bells were used in colonial California for telling time, announcing events, and for passing on news from one city to another. Our symbol is the classic outline of a mission bell because THE BELL newsletter serves similar purposes.

Coming Issues

- Marketing: Private Internet Voting
- Internet Paradigms
- Cryptography: Why and What?
- Internet Voting FAQ

Call for Papers

Join the dialogue and submit your paper to THE BELL. See page 2. All papers are peer–reviewed.

Free Subscription

THE BELL is FREE of charge for Internet distribution in PDF format, and is also available in hard copy. For information, see the back cover.

Contents

The Private Sector Won't Wait

Internet voting applications are vigorously growing in the private sector. In twenty-five U.S. states, Internet voting is already legal. It is also allowed by the U.S. Securities and Exchange Commission (SEC). Why? Increasing voter participation, reducing costs and providing faster results are some of the reasons. **(continued on p. 5)**

Would You Sacrifice Your Privacy to Gain Security?

Many people are not aware that digital certificates work by breaking your privacy.

This overview of digital certification systems is an updated version of a standard online reference that has been downloaded more than 250,000 times on the Internet. It discusses privacy and security restrictions that CANNOT be overlooked when applying digital certificates to Internet voting, where protecting voter anonymity is a basic requirement. **(continued on p. 3)**

"Why vote by Internet?"

"What *NEED* is met by Internet voting?"– Bill Kimberling of the Federal Election Commission (FEC) last week offered Maryland election officials a series of questions about Internet voting that he suggested should be answered before voting online can become a reality. **(continued on p. 13)**

THE BELL™ Newsletter

Editor: Eva Waskell
ewaskell@safevote.com

Website: www.thebell.net

Address: 1001 D Street, Suite 202, San Rafael, CA 94901-2800

Phone: (415) 482-9300

Fax: (415) 482-9400

Subscriptions: See back cover.

Back issues: Free of charge for PDF, consult sales@safevote.com for hard copy.

Privacy: We will not forward to third parties any personal, address or credit information supplied to us by you. Any other information we may receive is treated as public and non-confidential.

Submissions: Contributions are welcome. All material is to be submitted to the editor as an e-mail attachment in WordPerfect, MSWord or ASCII text. Submissions will be subject to peer review but authors will have the final decision on editing. There are no deadlines for submission. Material that is timely may be published immediately. The editor reserves the right of discretion on what and when to publish.

From the Editor

Dear Reader:

While the stock market slump has somewhat curbed the dot.com fever, the Internet itself continues to expand at breathtaking speed. In an effort to facilitate this expansion and make it easier to transact business over the Internet, the U.S. Congress recently passed S.761, the Millennium Digital Commerce Act. Policy-makers claim that an electronic signature is more secure and more difficult to forge than a paper and ink signature. Such statements need to be looked at very closely. One also needs to ask: Is this legislation based on a comprehensive and scientific understanding of how digital signatures work? Are there any roadblocks around the corner?

If this legislation were based on "bad" science, it would mean that the public would eventually develop misgivings about the integrity of online transactions. In such a case, ignorance is not bliss because ill-conceived policies regarding digital signatures can lead to a false sense of security among end users, erode trust and leave the underlying problems unsolved – problems that inevitably surface once flawed legislation is put into practice.

This July issue contains an overview of digital certification systems that will provide background information for those who want not only to understand more about what these systems are and how they work, but for those who want to know what questions to ask in order to evaluate the risks involved, including the risks to privacy in Internet voting. This issue also finalizes the marketing study for public Internet voting in the U.S. and introduces the subject of private Internet voting. Coming issues will deal with the technology and market for private Internet voting, different paradigms for understanding and using the Internet, cryptography basics and much more.

THE BELL is now catalogued at the Library of Congress. We are open to suggestions you may have regarding libraries, universities or other locations where a printed version might be archived for the benefit of the public. Your ideas are welcome.

Eva Waskell, Editor
Communications Director
Safevote, Inc.

THE BELL'S MISSION STATEMENT

Our mission is to contribute to the public dialogue on Internet voting as well as to lead discussions on collaborative decision-making in general. THE BELL intends to provide high-quality, non-partisan, timely and useful information regarding privacy, security, technology, voting, their markets and relevant policy issues.

Overview of Certification Systems: X.509, PKIX, CA, PGP & SKIP

Do you understand digital certificates? Do you know what they warrant?

by Ed Gerck, Ph.D.[*]

Cryptography and certification are necessary Internet features and must be used together – for example, in e-commerce and Internet voting. This work deals with digital certification issues and reviews the three most common digital certification methods in use today, which are based on X.509/PKIX Certificates and Certification Authorities (CAs), PGP and SKIP.

The certification methods are respectively classified as directory, referral and collaborative based. For two parties in a dialogue the three methods are further classified as extrinsic, because they depend on references which are outside the scope of the dialogue. A series of conceptual, legal and implementation flaws – including lack of suitability of purpose – are catalogued for each case, emphasizing X.509 and CAs, which directly helps users as safety guidelines when relying on digital certificates. Governmental initiatives introducing Internet regulations on certification, such as by TTP, are also discussed with their pros and cons regarding security and privacy. Throughout, the paper stresses the basic paradox of security versus privacy when dealing with extrinsic certification systems – which is very important in voting systems.

This paper has benefitted from the feedback of the Internet community and its online versions received over 250,000 Internet visitors from more than 80,000 unique Internet sites in 1997/2000. The paper was also presented by invitation at the Black Hat Conference, Las Vegas '99. THE BELL is publishing the first part of the paper. The footnotes, references and the full PDF version as well as the original (larger) HTML version are available at www.thebell.net/papers/

Introduction

The Internet is an open system, where the identity [1] of the communicating partners is not easy to define. Furthermore, the communication path is non-physical, non-deterministic, and may include any number of eavesdropping and active interference possibilities. Thus, Internet communication is much like anonymous postcards that are anonymously routed and answered . However, these postcards, open for anyone to read, write, change, or discard, must carry messages between specific endpoints in a secure and private way.

The solution is to use encryption (to assure privacy) and certification (to assure that communication is happening between the desired endpoints and that it is tamperproof) [MOV97]. This paper deals extensively with certification, the paradox of privacy versus security, as well as closely related matters of encryption and Internet protocols.

The question is whether we should be willing to sacrifice privacy in order to have security [Ger00]. In e-commerce the answer has been a resounding "Yes." And this approach has been quite successful. E-commerce Internet security is based on breaking privacy, from digital certificates as discussed here, to credit-card transactions, to registering a dot-com domain name [Ger00].

In elections, however, we need a "privacy wall" between the voter and the ballot – if I get the vote I cannot know who the voter is, if I get the voter I cannot know what the vote is. Some security technology provided by digital certificates as discussed here and used in e-commerce cannot preserve the anonymity of the vote [Ger00], a right protected by law and considered essential to democracy.

The problems that may be caused by false certification or no certification mechanisms can range from a "man-in-the-middle" attack in order to gain knowledge over controlled data, to a completely open situation to gain access to data and resources. Such problems do not disappear with encryption or even with a secure protocol such as SSL [Fel97]. If the user is led to connect to a site which appears to be the desired one, as in a spoofing attack [Fel97], the user may end up with a secure connection to a fraudster.

This paper reviews the three most common certification methods in use today, which are based on X.509/PKIX Certificates and Certification Authorities, PGP and, SKIP.

These methods are studied from a systemic point of view. The main motivations for this paper are: (i) Conduct a comparative review of the three methods, (ii) Unify a set of references to the most important issues in certification and encryption, as they are related to Internet needs and recent governmental policies, (iii) Provide a basis for the evaluation of other certification solutions available or to be developed, (iv) Identify room for improvements on the current security level of certification, that could be dealt with by other methods, (v) Provide users with safety guidelines to be used when resolving certification issues, and (vi) Access the impact on Internet transaction security due to the security control policy needs of Governments currently actively promoting such policy solutions. The original expanded version of this paper is online [Ger97a].

It is important to note that IETF's PKIX [PKIX] is a direct derivation of X.509. The reader will find essentially the same conceptual features and problems in PKIX as in X.509.

1. Certification Methods

Public-key cryptography may give the impression that security can be simply achieved. It seems that one only has to distribute the public-key at will, with no need to control it, and anyone can receive secure messages. The same procedure being applied to each side, sender and receiver, both could immediately engage in secure communication.

However, who is at the other side? Is that key really from the sender? Is the key still valid? Questions soon appear and it becomes clear that public-key cryptography has indeed solved the problem of public-key security but not the problems of public-key acquisition, recognition, revocation, distribution, re-distribution, validation and, most importantly, key-binding to an identifier and/or key-attribution to a real-world entity. Communications can be verified neither for origin authentication nor for data-integrity– communications can be private but not secure.

Of course, a private communication with a fraudster is not secure just because it is private. Clearly, without binding the key to an identifier such as a person's common name, the key is just a byte string and can be yours as well as anyone else's. But common names or identifiers are oftentimes not enough– where legal capacities must be defined, one needs to have some assurances that the key can be attributed to one well-defined real-world entity such as a person or company.

Certificates provide a strong binding between the public-key and some attribute (usually the entity's name and/or the entity's real-world identity). Certificates still entail all the previous questions, such as certificate acquisition, recognition, revocation, distribution, re-distribution, validation and, most importantly, what is the intended meaning for key-binding to an identifier and/or for key-attribution to a real-world entity. And they insert a new one, namely the privacy concerns for that identifier and real-world entity (e.g. an Internet voter). However, certificates introduce tamperproof attributes which can be used as convenient references to differentiate one certificate from another, one key from another and, possibly, one entity from another.

Absolute certification methods are a logical impossibility, because a certificate cannot certify itself. Three main methods have been proposed to deal with this situation, as this paper classified them for the first time:

- Directory methods: X.509 and CA [X509a], [X509b]

- Referral methods: PGP [PGP]

- Collaborative methods: SKIP [SKIP]

Each of the above paradigms deals with the basic certification question in a different way, as analyzed in the following sections. However, for two parties in a dialogue, they share a common ground in that they depend on references which are external to the dialogue between the parties. Hence, they are called extrinsic and share common characteristics, as will be comparatively discussed here. Further discussion on the general characteristics of extrinsic certification as well as the existence proof of two other certification modes, called intrinsic and combined, is presented in [Ger97b].

2. X.509 and CAs

The ITU-T Recommendation X.509 (which has been implemented as a de facto standard) [X509b], describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed by using cryptographic techniques. It is this second level that interests us here. It defines a framework for the provision of authentication services, under a central control paradigm represented by a "Directory".

The "Directory" is implemented by Certification Authorities (CA), which are governed by Certification Practice Statements (CPS). The CPS is internally defined by each CA within broad limits and lie outside the scope of X.509, even though X.509 refers several subjects to be defined in the CPS, as discussed in the exposition. There are three main entities which can be outwardly recognized in X.509 certification procedures:

CA: a general designation for any entity that controls the authentication services and the management of certificates.

(continued on p. 7)

The Private Sector Won't Wait

Edited by Jim Hurd [*]

As the Private sector vigorously embraces Internet voting, the Public sector is taking a close look at how to utilize this tool. Understanding Internet voting in these two sectors is critical to everyone involved.

Introduction

Twenty-five U.S. states have ratified Internet voting for Private sector companies. These companies use the Internet to decide matters which are no less important than those facing public election participants today.

The following states and one territory have ratified Internet voting for the Private sector: Arizona, California, Delaware, Georgia, Illinois, Indiana, Louisiana, Maryland, Michigan, Minnesota, Mississippi, Missouri, Nevada, New York, North Carolina, North Dakota, Oklahoma, Ohio, Pennsylvania, Puerto Rico, Rhode Island, Tennessee, Virginia, Wisconsin and Wyoming.

The Federal agency that is the primary overseer and regulator of the U.S. securities markets, the U.S. Securities and Exchange Commission (SEC), also allows shareholders of publicly-held corporations to use the Internet to vote.

The Private sector won't wait and Internet voting is here to stay. It is already part of daily life.

Safevote, Inc. is conducting a comprehensive study in order to learn more about the dynamics in Private sector voting. The study includes the SEC regulations on Internet voting, as well as a close look at the New York State and Delaware regulations on Internet voting –the two most important states in this area. The study also looks at service providers of Internet voting in the Private sector and at Internet voting in selected publicly held corporations and in private associations. This article, derived from this study, is an introduction to Private sector voting. Future issues will contain additional material.

1. Proxy Voting Comes in Two Flavors: Transfer Proxy Voting and Delegation Proxy Voting

One important point to address in our discussion of **Private** vs. **Public** Internet voting is the difference in terminology between the two sectors, where the same words may be used to mean quite different things.

Consider, for example, the very words *"proxy voting"*. These words are used in both sectors in different ways to denote who has the final authority in casting the vote.

We need different names. For reasons soon to be made clear, we will denote the type of proxy voting used in the **Private** sector as **"transfer proxy voting"**. We will denote the type of proxy voting used in the **Public** sector as **"delegation proxy voting."** Both types complement each other – in transfer proxy voting there is no delegation, and vice versa.

In **Private** sector voting, when the term "the shareholder votes by proxy" is used, **it means that the shareholder personally made the voting choices and that those choices are transmitted via a transfer agent** to the company as given by the shareholder in his proxy. It does not mean that the shareholder is authorizing someone else to make the voting choices. The proxy is a **document** and *proxy voting* means voting by a proxy "document" or electronic media such as mail, telephone, or the Internet. Private sector proxy voting by telephone, mail or Internet is desirable because it has the potential to increase voter participation, reduce costs, and provide faster results.

In **Public** sector voting, however, ***proxy voting denotes a quite different process that is undesirable because it may easily compromise election integrity.*** **The term "proxy voting" means a delegation to a person to vote on behalf of another.** For example, the Administration and Cost of Elections (ACE) Project states: "Proxy voting is a method that is at odds with the usual notions of integrity of voting practice and a throwback to earlier notions of voting accessibility. It allows registered voters to appoint another person to vote in their name. Unlike assisted voting in voting stations (see Language /literacy assistance and physically/visually impaired voters), there can be no controls to ensure that the registered voter's instructions on how to vote are followed by the appointed proxy, and, therefore, it may very easily be subject to abuse. It can be of particular concern where systems allow a proxy to cast a vote for more than one registered voter, and especially where a single person may cast proxy votes for any number of relatives." [ACE]

In addition, we note that each sector also uses the word *proxy* in a different way. In the **Private** sector, a ***proxy*** is a

document, a phone call or an Internet message that is entrusted by a voter to an agent, which collects such proxies as tasked by a company and transfers them to the company – whereas in the **Public** sector, a ***proxy*** is a person who will actually vote in the voter's name, by delegation.

Proxy voting in the Private sector is based on transfer. In the Public sector, proxy voting is based on delegation.

We also note that there may be wording in proxy statements to the effect that if the shareholder does not indicate how his shares should be voted on the proxy, then those shares are voted as the Board of Directors recommends. This is **not** delegation proxy voting because the Board's recommendations are known and thus accepted by the voter before the vote is cast. The voter is still the one making the choice. However, if additional items come up for a vote at the meeting, that were not in the proxy document, then the proxy document **may** authorize management to use its best judgment to vote on those issues –which corresponds to delegation proxy voting.

Private sector proxy voting involves other considerations as well, especially privacy and security, which will be dealt with elsewhere. The reader is referred to the Glossary at the end of this article for further terminology specific to the Private sector.

2. Transfer Proxy Voting and Public Elections are Similar Processes

In the Public sector, a public election is a process where poll officials (the "agents") receive ballots ("documents") and transfer them to the election officials (the "company").

The above paragraph identifies a process where "agents", "documents" and "company" play the same role both in transfer proxy voting as well as in public elections. This means that **transfer proxy voting and public elections are similar**. However, as shown before, there is **no** similarity between transfer proxy voting and delegation proxy voting.

These two observations are critical pieces of the puzzle if we want to understand the lessons of Private sector Internet voting and apply them to Public sector Internet voting because **private proxy voting and public elections are similar processes.**

These two processes are also regulated in a similar fashion, at least in the U.S. The U.S. Federal government, e.g. through the SEC (Securities and Exchange Commission) for private proxy voting or the FEC (Federal Election Commission) for public elections, acts in either case by *rulemaking* – the process by which federal agencies implement legislation passed by Congress and signed into law by the President. Rulemaking can involve several steps: concept release, rule proposal, and rule adoption. However, as exemplified by the SEC, a corporation is only permitted to use the Internet to conduct proxy voting to the extent that it is permitted by the state in which the corporation is incorporated. **In other words, state law is the starting point for determining if a corporation or a county may legally use the Internet to conduct private proxy voting or public elections.** Such laws may, of course, vary from state to state.

Thus, by observing the parallels between private proxy voting and public elections, as well as the vigorous expansion of Internet voting in the Private sector state-by-state, one would expect that **those states which already allow Internet private proxy voting for corporations would be closer to adopting Internet voting in public elections.**

Conclusion: Critical Pieces of the Puzzle

This article shows:

1. *Proxy voting* in the Private sector is not waiting for tomorrow. Twenty-five U.S. states already allow Internet voting in the Private sector. The SEC also supports Internet voting for publicly-held corporations.

2. *Proxy voting* in the Private sector is defined by **transfer**, whereas *proxy voting* in the Public sector is defined by **delegation**. **The latter can easily compromise election integrity in Public sector proxy voting but plays no role in Private sector proxy voting.**

3. *Proxy voting* in the Private sector is similar to public elections. This allows parallels to be drawn between developments in both sectors, Public and Private.

As we grow in our understanding of the power and possibilities inherent in Internet voting, it is very important to understand the actual mechanisms involved. When we understand the critical functions clearly, we can move forward swiftly without FUD (Fear, Uncertainty and Doubt).

Understanding both the difference between Transfer Proxy Voting and Delegation Proxy Voting as well as the different ways they function in Private vs. Public elections are absolutely critical pieces of the puzzle we are all putting together.

Acknowledgements: Dr. Ed Gerck and Maurer Marketing Associates contributed material to this article; Eva Waskell collaborated in editing.

REFERENCES

[ACE] http://www.aceproject.org/main/english/po/poa02e/default.htm

GLOSSARY – FOR PRIVATE SECTOR

Proxy - a written authorization given to a transfer agent by a shareholder, for someone else (usually the company's management)

to cast his/her vote at a shareholder meeting or at another time. A proxy can be sent by phone, by mail or by the Internet.

Transfer agent - an agent for proxy voting and registrar for a publicly held company, that keeps a record of every outstanding stock certificate and the name of the person to whom it is registered. When stock changes hands, the transfer agent transfers the ownership of the stock from the seller's name to the buyer's name. The registrar provides a daily reconciliation of all transfer records to verify that the number of shares debited is equal to the number of shares credited. The transfer agent also uses the shareholder records to pay dividends and issue proxies to shareholders. Transfer agents know who the registered shareholders are and the number of shares each is authorized to vote. Transfer agents usually assign a PIN to authenticate shareholders voting by telephone or Internet. Transfer agents, functioning as Inspector of Elections, attest to the accuracy of the vote tabulation.

Proxy solicitor - agents that contact shareholders to secure the necessary vote with as much participation as possible. Ownership analyses and vote projections are created to assess a clients' vulnerability to shareholder activism or takeover bids and to predict the likely success of company initiatives.

Proxy research and advisory company - an agent that provides proxy research, vote recommendations and voting agent services for institutional investors. A proxy research and advisory company analyzes proxy issues and recommends votes for shareholder meetings. Voting agent service provides investment managers, pension funds, banks and other institutional investors with a solution to proxy voting compliance. A proxy research and advisory may also offer specialized research tailored specifically to the needs of Socially Responsible and Taft-Hartley investors.

Jim Hurd is the Marketing Director of Safevote, Inc. He graduated from George Washington University, 1981, B.F.A., Graphic Design. He won National Awards in Design in U.S. Corporate Identity 5 and 8. He has been a speaker at numerous conferences, including: IQPC (7/98 - Washington, DC), IWD (6/98 & 11/99 - Des Moines, IA), ICDC (11/95, 97, 98 & 99 - Sacramento, Los Angeles, Reno & San Diego), IEEE (3/98 - San Francisco). He has been focusing his work on creative business development for a variety of technology companies in the Silicon Valley since 1997.

Overview of Certification Systems

(continued from p. 4)

The CA is also called the issuer. A CA can be public (a bank that issues certificates to allow its clients to access their bank account), commercial (a service provider that sells certificates to other parties, such as Verisign), private (a company that issues certificates to allow its employees to perform job duties), or personal (you, me). CAs are in general independent, even in the same country.

Subscriber: an entity that supplies to the CA the information that is to be included in the entity's own certificate, signed by the CA. Usually, as defined in CA's CPSs, the information supplied by the subscriber is "endorsed" by the issuer, where "endorsed" means "copied as received". This corresponds to "end orsement without recourse". For example, in English law one can endorse "without recourse" (or, as it used to be expressed, "sans recours"), which passes on the benefit of a bill of exchange without adding any guarantee. In other words, the CA copies the subscriber's information to the certificate, but neither denotes nor confirms it –i.e., there is no warranty.

User: any entity which relies upon a certificate issued by a CA in order to obtain information on the subscriber. Also called the verifier. Users may use any CA or any number of CAs, depending on their location and ease of access. The user should be central to the decision process in all steps, since the user is the party that is relying on the information and is thus at risk.

A further entity is the Naming Authority (NA), which is usually not outwardly perceived but which is the actual entity that defines the naming scheme used by a CA. The CA can double as a NA, but they provide two different functions. Semantically, the CA certificate refers to a name; however, it does not denote it –the NA denotes it.

The authentication services provided by CAs are especially relevant in regard to three central questions:

What is a X.509 certificate?

Even though section 3.3.3 of X.509v3 defines a certificate as: *"user certificate; public key certificate; certificate: The public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it."*, there are several open questions regarding the contents of certificates and their issuance conditions which need to be discussed (see next), as well as the issue of certificate revocation (see next).

What is the naming scheme used in X.509 such that a certificate can be associated with a user?

Section 11.2 of X.509v3, "Management of certificates", states that the certificate allows an association between a name called "unique distinguished name" or DN for the user and the user's public-key: *"A certificate associates the public key and unique distinguished name of the user it describes."*, while Section 7 explains that such DNs are essential to the security design of X.509: *"Authentication relies on each user possessing a unique distinguished name."* But, how are DNs assigned? Where are they unique? The DN is denoted by a

NA and accepted by a CA as unique within the CA's domain, where the CA can double as a NA. It is interesting to note that the same user can have different DNs in

different CAs, or can use the same DN in different CAs even if it is not the first one to use it in a CA – so, different DNs for different CAs do not necessarily mean different users and vice-versa. Furthermore, a DN may not contain the user's real-world name or location.

What are the validation procedures for the certified data that is included in a certificate?

X.509 is moot on validation procedures for data included in a certificate such as the user's name, with the exception of validation procedures for the user's public-key which are suggested (not mandated) in Section 10 of X.509v3. For example, regarding validation procedures for the user's identity, Section 11.2.a states that: *"a certification authority shall be satisfied of the identity of a user before creating a certificate for it"*, which means that identity validation procedures are to be satisfied in the CA's frame of reference by following the CA's own self-defined rules (the CPS), which can be entirely different for different CAs. Further, in general, commercial CA's CPSs accept indirect references when issuing certificates, such as using an ID as identity proof, which can be easily subject to fraud and lead to public risks.

Thus, X.509 focuses on defining a mechanism by which information can be made available in a secure way to a third-party – the certificate itself. However, X.509 (and PKIX) does not intend to address the level of effort which is needed to validate the information in a certificate neither define a global meaning to that information outside the CA's own management acts.

The main purpose of a CA is to bind a public key to the name contained in the certificate and thus assure third parties that some measure of care was taken to ensure that this binding is valid for both – i.e., name and key. However, the issue whether a user's DN actually corresponds to identity credentials that are linked to a person or simply to an e-mail address – and how such association was verified – is outside the scope of X.509 and depends on each CA's self-defined CPS and on each NA.

Regarding the all-important DN specification denoted by the NA and accepted by the CA, the X.509 DN scheme is based on ITU-T X.500 Recommendation [X500a], [X500b] – but X.500 is not completely defined and, apparently never will be. There is no Internet workgroup, not even ITU-T as its proponent, that currently works on X.500 final naming definitions. This is due to several factors, such as the lack of a centralized world body that would be acceptable to all parties and needs and, most importantly, the perception that global indexes involve strong privacy concerns.

Thus, there was ample room for many different readings of the proposed X.509 Recommendation, as different implementations had to ad hoc define how DNs would be used in X.509. Also the X.509 Recommendation depends on many others ISO, ANSI, ITU, and IETF standards, amendments, meeting notes, draft standards, committee drafts, working drafts, and other work-in-progress documents, besides the convoluted language used in some of these specifications, which makes their use difficult by itself, as pointed out by Peter Gutmann [Gut98].

A characteristic of X.509 is that almost all issues that involve semantics or trust are delegated to a CA's CPS – the Certification Practice Statement – which is declared out of scope in relationship to X.509. The CA's CPS is the governing law that the CA presents to potential clients and represents a top-down framework. While some consider the CPS mechanism to be a good way to introduce flexibility in X.509 because each CA can have their own rules for different needs, such mechanism can be considered as X.509's ***black-hole*** and cannot be directly harmonized for different CAs.

Thus, while this ***black-hole*** mechanism affords a "solution" to the undefined semantic and trust features in X.509 (as they are declared out of scope and delegated to the CPS), this *laissez faire* attitude leaves ample room for strong differences between CAs and for a biased "take-it-or-leave it" attitude regarding what a CA subscriber can expect.

These problems have caused independent interpretations of X.509 in actual implementations, e.g. as shown in products from Netscape, Microsoft, RSA, etc., and by CAs.

For example, lack of CPS harmonization does not allow X.509 to directly scale to a planetary Internet, when different CAs would need to allow for cross-certification (i.e., when subscribers of different CAs are users to one another). Even though cross-certification could work in a parochial Internet where everyone knows what to expect and share a common law and trust system, it is doubtful that it could be successfully applied between competing businesses or different states in a country – much less between different countries, since there is no common world law. There are also subjective and intersubjective aspects of certification and trust [Ger97c]which are needed, but which cannot find a unified global expression – as it would be required for X.509 cross-certification.

Besides, X.509 certificates are not human readable and the user cannot easily see what is being accepted. In fact, he has to take it for granted that it is correct – e.g., when a browser presents a readable conversion. However, even experts disagree on basic X.509 issues, as explained above, and there is usually ample room for doubt about what exactly a X.509 certificate is, why it is acceptable or why it is not acceptable. In other words, ***X.509 certificates have a twilight zone exactly on the most important issue with certification: what has been certified***.

(continued at THE BELL website: http://www.thebell.net/papers/certover.pdf)

Internet Voting: U.S. Market Intelligence Study, Conclusion

Safevote, Inc.[*]

This issue presents the conclusion of our marketing study overview of current voting systems in the U.S. Parts I and II were presented in former issues of THE BELL. This issue highlights findings from counties in New York and Texas regarding election costs, current voting system status, Internet voting perspectives and other related topics. The entire market intelligence study focusing on the 2000 U.S. public elections contains over 200 pages and will soon be available in a limited printed edition.

Highlights of State and County Findings

State of New York

Certified Systems - Voting systems are approved specifically for election day voting or absentee voting. Only mechanical lever and DRE machines are certified for election day voting. Punch cards, mark-sense and paper are certified for absentee voting. All systems must provide a full ballot display on a single surface. Voting system options are very limited because few vendors are able to meet this requirement.

Voting System Replacement Trends - Only three counties have purchased DRE machines. All three are also using mechanical lever machines. Only three counties have purchased punch card systems and three have purchased mark-sense systems for absentee voting.

Early Voting - Absentee mail-in voting is increasing.

Current Voting Systems -

Current Voting Systems in New York For Election Day Voting

	#	%
Punch Card Ballots	59	95
Mark-sense Ballots	3	5
Total	62	100

Internet Voting - The requirement for a full ballot display on a single surface is a barrier to the approval of an Internet voting system. The full ballot must be viewed without scrolling the computer screen. Another barrier is a requirement that absentee ballot counting systems enable hand as well as machine counting.

New York Counties

New York City Board of Elections

Election Official - Commissioner

Current System Status - Shoup Manual mechanical lever machine for election day voting. Current ballot requirements exceed the 8 columns 40 row capacity of the Shoup Manual. Plans to replace the Shoup Manual system with a Sequoia Pacific system were sidelined when a subcontractor to Sequoia Pacific failed to provide an acceptable system and a law suit was filed by the Board of Elections against the subcontractor.

The Sequoia Pacific mark-sense system will be implemented for absentee voting. Sequoia Pacific is the only New York State certified vendor of a full face mark-sense ballot.

Barriers to System Change - Replacement of the Shoup Manual system is on hold pending the outcome of the lawsuit against the Sequoia Pacific subcontractor. Mayor is "termed out" and is unlikely to expend large amount of money on a new voting system. The DRE system was priced at $60 million when the contract was signed.

Criteria for New System - Full face ballot design, ability to accommodate multiple languages, key punch for write-in candidates, adequate capacity to meet ballot length requirements.

Election Costs -

Average cost per election: $6 million
Average cost per registered voter: $1.76

Replacement System - In the interim the county is purchasing used mechanical lever machines from Calhoun, FL.

Internet Voting - Concerns about security, voter education, and legislator reluctance to change voting systems. Use of

voting system computers by schools presents problems of wear and tear and breakage of machines that must be in working order on election day.

Nassau County

Election Official - Commissioner

Current System Status - AVM Manual mechanical lever machine. Machines are reliable, but tallying of votes is slow and subject to human error as poll workers make errors when taking readings from the machine counters.

Barriers to System Change - Cost, voter education. Current system has very low operating costs.

Election Costs -

Average cost per election: N/A
Average cost per registered voter: N/A

Replacement System - No plans for replacing the AVM Manual. Hope to obtain a scanable form from Sequoia Pacific to automate data entry of election results. Poll workers would enter machine readings on a form that could be scanned into the county's mainframe.

Internet Voting - Concerns include voter education, verifying that voters receive the correct ballot, secrecy of the ballot if voting done in a classroom setting, potential problems in data transmission, and tampering of votes during data transmission. Advantages include faster election results.

State of Texas

Certified Systems - Punch card, mark-sense, traditional DRE and touch screen systems. Recertification of all current voting systems and certification of new voting systems is on hold pending details on the recent ADA requirements on disabled persons access to a secret ballot.

Voting System Replacement Trends - Several counties are purchasing touch screen systems for early voting. Mark-sense voting systems are the primary replacement to punch card systems.

Early Voting - Early voting has grown in popularity since it was introduced in 1987. Currently up to 35% of ballots cast are through early voting (mail-in or in-office). Election officials are seeking systems that will increase the efficiency and reduce the cost of providing and tabulating multiple ballot styles at early voting locations.

Current Voting Systems -

Current Voting Systems in Texas For Election Day Voting

	#	%
Punch Card Ballots	16	6
Mark-sense Ballots	144	57
Mechanical Voting Machines	3	1
DRE	1	<1
Paper Ballots	90	35
Total	254	100

Internet Voting - There are no current standards for an Internet voting system; the vendor must submit the system for certification and it will be reviewed to determine whether it meets the voting system requirements of the Texas Election Code. It may be possible for a vendor to present a system that utilizes the Internet to transfer results from a polling place terminal to a central counting station.

Texas Counties

Bexar County

Election Official - County Clerk

Current System Status - ES&S mark-sense voting system with central count tabulation for election day and early voting. System is inadequate to handle the volume of a large jurisdiction. Transporting the ballots to the central tabulation center and reading the ballots is time consuming. Inefficient for providing multiple ballot styles at early voting sites.

Barriers to System Change - Unable to select new system until details on meeting the ADA requirements are available and voting systems are recertified in Texas.

Criteria for New System - Efficient for early voting, meets new ADA requirements, ease of use for election judges who are senior citizens, easier, speedier tabulation, ease of consolidating results from election day and early voting systems if different voting methods are used.

Election Costs -

Average cost per election: $325,000 to $350,000
Average cost per registered voter: $.40 to $.43

Replacement System - Favors touch screen systems, wireless systems are advantageous for the seniors who serve as election judges. New system will be phased in starting with the touch screens for early voting. County is generally wary of unproven systems given historical voting system problems.

Internet Voting - Concerns regarding difficulty of explaining Internet voting, location of the point of encryption, adaptability of older voters, security and privacy. If an Internet voting system were certified in time for the replacement system decision, it would be given serious consideration. Otherwise, the estimated timetable for Internet voting is 5 to 10 years.

Dallas County

Election Official - Elections Administrator

Current System Status - ES&S mark-sense voting system with in-precinct counters for election day voting and ES&S touch screen system for early voting implemented in 1998.

Criteria for New System - Single vendor accountability for mark-sense, touch screen voting systems and voter registration system. High speed in-precinct counters. Ability to make ballot changes from a supervisory terminal vs. changing individual voting devices. Very easy to use for election judges - avoidance of complicated procedures and wire connections. Vendor support.

Selection of New System - Disappointed with few types of voting systems on the market. Many systems are based on old technology in new packages. Touch screen cost-prohibitive for election day voting.

Satisfaction with New System - High voter acceptance of touch screen system. Voters over 55 like it the most. Touch screen easier to use than punch cards. Saved $100,000 on paper costs for early voting. Reduction in voter error as touch screen alerts voters of errors. Excellent vendor support from ES&S. With opportunities to rent out the system, and savings in paper and overtime costs, the system will pay for itself in 5 years.

Election Costs -

Average cost per election: $750,000
Average cost per registered voter: $.40 to $.43

Internet Voting - Participating in the Federal Voting Assistance pilot project in Internet voting for the military. Convenience is a key advantage. Popularity of early voting demonstrates importance of convenience. Must overcome equal access issue. Security is first in importance. Pilot projects must be problem free to build confidence. Voters like excitement of computer voting. Internet voting will start slow and rapidly expand. Concerns about using computers in schools for voting include: computer durability with student usage, security, elections disrupting school curriculum, overlap with other efforts to computerize schools. Estimated timetable for Internet voting is a minimum of 5 years. Internet voting will occur in phases starting with the military in hazardous locations, then anyone in the military, then voters who are out of state on election day.

Other - Dallas is one of the top 5 counties in the country in numbers of elections. On average the county has voting 1 out of every 3 days.

Tarrant County

Election Official - Elections Administrator

Current System Status - ES&S Optech IIIT mark-sense system for election day and early voting. Paper costs are rising, cost of unused ballots for early voting is $45,000. System is very adaptable for providing outsourced elections.

Criteria for New System - Ideal voting system is touch screen, allows the blind to vote by audio, eliminates unused ballot waste for early voting, offers ease of consolidating results from election day and early voting systems if different voting methods are used.

Systems for the Disabled - Active interest in voting systems for the disabled. Favors ES&S system that accommodates a variety of disabilities. However, at $15,000 per unit the system is very expensive. Anticipates that 30% of the equipment on the market will be eliminated with new ADA requirements - providing a substantial opportunity for vendors to fill this need.

Election Costs -

Average cost per election: $700,000
Average cost per registered voter: $.88

Replacement System - Decision to purchase voting system units for the disabled on hold until it is determined that the new system is certified as meeting the new ADA requirements.

Early Adopter - Willing to test new systems, provide opportunity for publicity to new vendor. Professional staff willing to work with vendor on system testing.

Internet Voting - Authored fall-1999 newspaper article stating that Internet voting is the wave of the future. Early voting has demonstrated the importance of the convenience factor. Consumer acceptance of online banking will facilitate acceptance of Internet voting. Envisions introduction of Internet voting on a phased basis. Sees Internet voting as an important solution to accommodating the needs of physically disabled voters. Recommends placing voting system computers for the disabled in places where they are needed, such as in the Lighthouses for the Blind. Suggests placing voting system computers in grocery stores, libraries, and other sites to satisfy the needs of voters who do not have computers. Envisions Internet voting occurring much before 2010.

This finalizes the 2000 U.S. market overview presentation.

Interactive Glossary

coordinated by Ed Gerck, Ph.D.

> *This is an interactive glossary project with the readers. Definitions are discussed before they are entered into the glossary. The underlined sentences represent proposed definitions for discussion. Comments are welcome.*

In the last issue we discussed the definitions of *identification* and identity in terms which could be useful to Internet protocols in general and to Internet voting protocols in particular. The definitions need to be affirmative and avoid circular references (e.g., to identify is to ask for an identity; an identity is that which identifies). These are the results obtained so far, open to public discussion:

to identify	to look for connections
coherence	a natural or logical connection
identification	a measure of coherence

Let us discuss them with some examples from [Bohm97].

No doubt every human being is ***born*** with some unique and unalterable characteristics, such as DNA sequences and fingerprints. Each person also ***acquires*** other rather unique characteristics, such as a name, a handwriting style and a signature. But these characteristics are not useful for identifying people ***in Internet protocols***. Even in those countries where the law requires that every person should have an official name, two people may easily have the same name – even in a small city. And there are many countries, such as the United Kingdom, where people can change their names without formality or official records, and can use several names for different purposes, none of which are more truly theirs than any other. Authors and entertainers commonly use several names.

Without wishing to be philosophical about this, a person is the aggregate of his past. He is the person who was born at some place and time (known to him only by the assertions of others), was educated at this and that school and university, has held this and that employment, published these papers, become known to this bank or mortgage lender, those neighbors and these friends, owns these assets and has those debts, has that appearance and this signature (at the moment), committed that crime, left these fingerprints at the scene, etc., etc.

To identify someone is thus to assemble a collection of facts which are true of that person and no other – i.e., these facts constitute connections, and these connections identify. To identify is to look for connections –as defined above.

However, how many facts are necessary to ***identify***? Is ***identification*** also a matter of connection quality and not just quantity? These questions will help us discuss and understand the definition of ***coherence*** in coming issues.

[Bohm97] Bohm, N. "Authenticating identities". MCG 1997, http://www.mcg.org.br/identity.txt

Internet Voting Technology Alliance

The IVTA Discusses its Articles of Incorporation

The Internet Voting Technology Alliance (IVTA) is currently discussing online its Articles of Incorporation in its ADM Workgroup. Discussions are open to all. To subscribe, visit http://www.ivta.org/adm/charter.txt

According to the draft in discussion, the IVTA will be a non-profit corporation without capital stock, operated exclusively for educational, literary and scientific purposes. Such purposes shall include, among others:

A. To facilitate and support the technical evolution of Internet voting, and to stimulate the involvement of the industry, government and others in the evolution of Internet voting by the discussion and issuance of voluntary technical standards, as well as their application in the certification of Internet voting products and services;

B. To provide information to the industry, government, and the public at large concerning the technology, use and application of Internet voting;

C. To promote educational applications of Internet voting technology for the benefit of government, colleges and universities, industry, and the public at large;

D. To provide a forum for exploration of new Internet voting applications, and to stimulate collaboration among organizations in their operational use of the Internet for Internet voting.

Media Watch & Links

1. "Why vote by Internet?"

Kimberling Offers Maryland Officials Questions to Answer about Internet Voting

Bill Kimberling of the Federal Election Commission (FEC) last week offered Maryland election officials a series of questions about Internet voting that he suggested should be answered before voting online can become a reality. Kimberling, Deputy Director of the FEC's Office of Election Administration presented his questions to the Maryland Association of Election Officials at the organization's annual meeting June 4-6 in Cumberland, MD.

Kimberling began by simply asking *"Why vote by Internet?"* Previous innovations in election technology, Kimberling observed, came about because of some need, such as the prevention of fraud, or substantial cost savings. *What NEED, he asked, is met by Internet voting?*

Kimberling said Internet voting advocates argue that it will increase voter turnout but he suggested there is good reason to believe that it won't. Those with Internet access are wealthier and better educated, groups with high turnout already, whereas those without Internet access are disproportionately poor and members of racial minorities, groups with relatively low turnout. Kimberling pointed out making voting more convenient is no guarantee of increasing turnout either, citing examples when hours for voting, or days of voting have been extended. Nor would the percentage of younger voters necessarily increase. Evidence indicates although young people may use the Internet, their online focus is rarely on government and politics.

Kimberling speculated that if the cost of Internet voting was relatively inexpensive, the election vendor that conducted the Arizona's Democratic Party primary would not have refused to release cost figures. Internet voting would be an *added* cost because it is being projected a s a supplementary voting option. There are no current plans anywhere to make it a substitute for systems currently in effect.

After asking *"How do we ensure the identity of the voter,"* Kimberling wondered, *"If this requires sending a pin number to every voter, then why not send them an absentee ballot instead?"*

Other questions to be answered: *How do we ensure that the voter gets the right ballot? How do we ensure the privacy and integrity of the vote? How do we guard against hackers (foreign and domestic)? What about viruses, Trojan horses, and such? What procedures would be used for contested elections and recounts that would retain the confidence of those challenging the results?*

Even if all the technical questions are answered satisfactorily, Kimberling reminded the election officials, the questions of purpose, fairness, and cost-benefit remain.

This article appeared on page 5 of the June 12, 2000 issue of Election Administration Reports, a newsletter for election officials, and is reprinted here with the permission of the Editor. The italics are ours.

2. Microsoft Alters Outlook E-Mail to Block Viruses

Microsoft is altering its popular Outlook e-mail software to prevent users from running any executable program attachments -- like the infamous Love Bug virus. But as a tradeoff for the added security, users will find that Outlook will also block some attachments that are harmless or possibly even beneficial.

http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2000/05/15/national2008EDT0809.DTL&type=tech_article

3. New, Nastier E-Mail Virus On the Attack

A far more potent and diabolical e-mail virus than the "I Love You" bug began to spread yesterday, two weeks after the original attack ravaged computers around the world and caused billions of dollars in damage.

http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/05/19/MN87695.DTL&type=tech_article

4. The Dark Side of Cookies

Find out how you are traced while surfing on the Web.

http://www.cookiecentral.com/dsm.htm

5. Junkbusters: How Web Servers' Cookies Threaten Your Privacy

How to disable cookies, check your browser and further protect yourself.

http://www.junkbusters.com/ht/en/cookies.html

6. Surfer Beware III: Privacy Policies without Privacy Protection

In a December 1999 survey, the Electronic Privacy Information Center (EPIC) reviewed the privacy practices of the 100 most popular shopping websites on the Internet and found that the privacy policies available at many websites are typically confusing, incomplete, and inconsistent.

http://www.epic.org/reports/surfer-beware3.html

7. "Digital Storm" Brews at the FBI

In response to growing concerns about terrorism, hackers and other high-tech criminals, the Federal Bureau of Investigation is planning a series of sophisticated computer systems that would sharply increase agents' ability to gather and analyze information. The FBI is seeking more than $75 million in budget appropriations to continue a massive information technology expansion, which includes a system dubbed "Digital Storm" that eases the court-sanctioned collection and electronic sifting of traffic on telephones and cellular phones.

http://www.washingtonpost.com/wp-dyn/articles/A20426-2000Apr5.html

8. F.T.C. Chairman Will Accept Gradual Moves on Net Privacy

The head of the Federal Trade Commission, which is seeking new authority to regulate the privacy practices of Internet businesses, told Congress on Thursday that he would support a scaled-back version of the commission's proposal if it would help start the process of setting basic consumer protections online.

http://www.nytimes.com/library/tech/00/05/cyber/articles/26privacy.html

9. Privacy Proposal Rankles Internet Industry

Internet industry groups lashed out yesterday at the Federal Trade Commission's recommendation that Congress make laws establishing basic online privacy standards. Two industry groups, the Information Technology Association of America and the Online Privacy Alliance, called the legislation unnecessary, and said the Internet industry is already doing a good job protecting consumers' privacy.

http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/05/23/BU100464.DTL&type=tech_article

10. Privacy Statement from the Transatlantic Consumer Dialogue

The Transatlantic Consumer Dialogue (TACD) is a forum of U.S. and EU consumer organizations which develops and agrees upon joint consumer policy recommendations to the U.S. government and European Union to promote the consumer interest in EU and U.S. policy making. In the area of data privacy, the TACD welcomed substantial improvements made to the "Safe Harbor" proposal negotiated by the two governments. Nonetheless, the TACD still feels many of its earlier criticisms of the agreement still apply.

http://www.tacd.org/statsum2000.html

11. Group Calls Privacy Protection Measures Ineffective

Web surfers who believe they have taken adequate precautions to protect their personal data online may be in for a rude awakening, according to new privacy reports showing that preferences for high security frequently revert to low security without notice.

http://news.cnet.com/news/0-1005-200-1891902.html

12. Web Also Revolutionizing ID Fakery

For a small fee, or often for free, Internet users can download programs or buy software that will print driver's licenses, birth certificates, immigration cards, job certificates and school transcripts.

http://www.washingtonpost.com/wp-dyn/articles/A29724-2000May18.html

13. After Attack by Hackers, AOL Tightens Data Access

America Online said yesterday that it would take steps to fix flaws in its network that allowed hackers to get access to personal information about some members last week.

http://www.nytimes.com/library/tech/00/06/biztech/articles/19hack.html

14. Political Websites Lack Constituents

In the parlance of populist politics, the people soon might "throw the bums out." The bums in question are some of the myriad websites devoted to politics.

http://www.zdnet.com/intweek/stories/news/0,4164,2574545,00.html

BOOK REVIEW - The Unwanted Gaze: The Destruction of Privacy in America

by Jeffrey Rosen (Random House 2000, $24.05)

As thinking, writing, and gossip increasingly take place in cyberspace, the part of our life that can be monitored and searched has vastly expanded. E-mail, even after it is deleted, becomes a permanent record that can be resurrected by employers or prosecutors at any point in the future. On the Internet, every website we visit, every store we browse in, every magazine we skim –and the amount of time we skim it –create electronic footprints that can be traced back to us, revealing detailed patterns about our tastes, preferences, and intimate thoughts. In this pathbreaking book, Jeffrey Rosen explores the legal, technological, and cultural changes that have undermined our ability to control how much personal information about ourselves is communicated to others, and he proposes ways of reconstructing some of the zones of privacy that law and technology have been allowed to invade.

http://www.epic.org/bookstore/

Links

Junkbusters - http://www.junkbusters.com

National Association of Secretaries of State
http://www.nass.org

National Conference of State Legislatures
http://www.ncsl.org

The Privacy Page
http://www.privacy.org

Privacy Rights Clearinghouse
http://www.privacyrights.org

Privacy Times
http://www.privacytimes.com

From Our Readers

From Kathleen Williams, Assistant Clerk Recorder Registrar of Voters, Plumas County, CA:

I think it's great...very informative. My staff and I got information in the newsletter we have no other way of getting.

From Betty Carter, retired election supervisor, Orange County, FL:

In regard to THE BELL's June headline"Would You Vote Naked?", I commented some time ago that if you can use the Internet to vote in the privacy of your own home, then you could indeed vote naked.

From Paul Terwilliger, Product Development Manager, Sequoia Pacific:

In the June 2000 issue of THE BELL, Roy G. Saltman, in his article 'Voting Systems, Conclusion', writes: "Typically, DRE machines are not designed to retain individual voter-choice sets."

This is not true!

Virtually all DRE systems on the U.S. market have been certified to the FEC's Voting Systems Standards. (For a complete list of certified systems, see www.electioncenter.org/about/nased.html) These standards are quite specific about the storage of individual voter ballot images. For example, section 2.3.2 of the Standards, "Accuracy and Integrity", states in part:

To attain a measure of integrity over the process, the DRE systems must also maintain an image of each ballot that is cast, such that records of individual ballots are maintained by a subsystem independent and distinct from the main vote detection, interpretation, processing and reporting path.

The electronic images of each ballot must protect the integrity of the data and the anonymity of each voter, for example, by means of storage location scrambling. The ballot image records may be either machine-readable or manually transcribed (or both), at the discretion of the vendor.

The Voting Systems Standards have been in existence since 1990; it is surprising that Mr. Saltman was unaware of this requirement.

Response to Paul Terwilliger from Roy Saltman:

THE BELL was not clear in identifying the year in which my chapter in Advances in Computers was first published. Volume 32 of Advances in Computers was published in 1991, which means that my chapter was completed in 1990. Of course, since then, DRE machines have been designed to record voter-choice sets. I was one of the originators of the requirement that they should be so designed.

Please see page 6 of my report Accuracy, Integrity, Security in Computerized Vote-Tallying, NBS Special Publication 500-158, published in 1988. To quote: "Each voter-choice set (i.e., the machine's record of all choices of a voter) should be retained in the machine on a removable non-volatile medium (e.g., magnetic disk). Storage locations of the voter-choice sets would have to be randomized to prevent association of a particular set with a particular voter. The retention of the voter-choice sets makes possible a verification (on an independent machine) of the DRE machine's summation of the voters' choices that it recorded....."

Thank you for the opportunity to clarify this point.

We thank our readers for their comments and regret not being able to include them all.

THE BELL™ Newsletter on Internet Voting

THE BELL c/o Safevote, Inc.
1001 D Street, Suite 202
San Rafael, CA 94901-2800

FIRST-CLASS MAIL
U.S. POSTAGE PAID
SAN RAFAEL, CA
PERMIT NO. 896

DATED MATERIAL
Please Expedite

The Private Sector Won't Wait See p. 5

To enter your FREE monthly subscription, visit the website www.thebell.net or use the form below.

cut here MAIL ORDER FORM cut here

Enter your one year monthly subscription to THE BELL: visit the website www.thebell.net or fill out the form below

Privacy Notice: We will not forward to third parties any personal, address or credit information supplied to us by you.

NAME/TITLE_____

COMPANY_____

ADDRESS_____

E-MAIL_____

[ ] FREE – in PDF format sent to the above e-mail address and/or

[ ] $30.00 SUBJECT TO AVAILABILITY – in printed format sent to the above mail address.

[ ] PAY BY CHECK OR MONEY ORDER Make check or money order payable to Safevote, Inc.

[ ] PAY BY CREDIT CARD Complete the information below.

[ ] Visa [ ] MasterCard [ ] Am Express [ ] Dinners [ ] Discover [ ] MasterCharge

Card Number_____ **Expiration Date**_____

Signature_____ **Print cardholder's name**_____

INSTRUCTIONS: Mail completed order form to the address below. Allow two weeks for processing.

THE BELL c/o Safevote, Inc.
1001 D Street, Suite 202
San Rafael, CA 94901-2800