

November 15, 2004

ROBERT KNAPP:
Chair, Berkeley Division of the Academic Senate

From: [Senate Committee on Computing and Communications](#)

Subj: **Conducting Senate Business Electronically**

In your letter dated September 16, 2004, you asked some specific questions about the technology of conducting Senate business electronically.

Conclusion

We believe that yes, it is not only technically feasible, but also advisable and desirable to allow and encourage the use of electronic means to conduct discussions and votes, as a supplement to face-to-face meetings, in the conduct of Senate business. Given the realities of time pressures and scheduling difficulties, this could increase participation in both discussion and votes. I am sure you recognize that electronic discussions are distinctly different from face-to-face interaction, and should be viewed as a supplement rather than substitute.

We also believe that discussion and voting can be done in a fashion that does *not* require the purchase of special equipment or software by individual Senate members, nor anything beyond a bare minimum of new skills or training. It *does* presume faculty access to standard desktop computers with Web browsing capability and network access, and it does presume that the campus and/or Senate acquire or construct some special centralized software.

Security

You ask if Senate discussions and voting can be conducted ‘securely’. 100% absolute security is not possible, and approaching this ideal would be quite invasive on users and quite expensive, so our answer is necessarily more nuanced. The appropriate question is whether ‘adequate’ security can be achieved within the constraints of available equipment and skillsets and budgets. Online business is already conducted on campus in contexts that we believe are at least as sensitive as Senate business, including e-commerce (selling various items and collecting gifts and tuition) and grade submission. The level of security for those purposes (and indeed many of the detailed security mechanisms) can be replicated for Senate business. We believe the resulting level of security is more than adequate.

To delve more deeply, what is meant by ‘security’? This is context dependent; in the context of Senate business, we believe the primary security issues are:

- *Confidentiality*. The nature of discussions is that they are conducted in a open atmosphere *within* committees. Are discussions disclosed *outside* the committee?

- *Privacy*¹. The nature of an open exchange within a committee is that it is divulged to other committee members, but is it possible for other committee members to divulge other member's comments outside the committee?
- *Secrecy*. There may be instances where 'secret' ballots are conducted. There are different flavors of secrecy: Is each member's vote transparent within the committee, but only the overall tally or result is disclosed outside the committee? Is the ballot intended to be secret from other Senate members (as in Division-wide elections)?
- *Accuracy*. Is it possible for non-member outsiders to participate in discussions or votes, fraudulently impersonating members? Is it possible for committee members to vote more than once?
- *Attribution*. Are discussions or votes ever conducted anonymously, or alternatively must a comment or vote be attributable to a particular member? If the latter, who has access to the identity of the contributor?
- *Non-repudiation*. Is it possible for a committee member to withdraw or change a vote, after it has been placed?
- *Archiving and destruction*. Are communications and documents preserved indefinitely, or are they destroyed?

We must also assess any security scheme in light of the seriousness with which we view threats and accept consequences. The dimensions of this include:

- *Adversaries*. Who are the adversaries? Is their objective to disrupt Senate business, or to control outcomes, or achieve monetary gain? What is their skill level?
- *Means*. By what means do we envision an adversary attacking the Senate business? Do we envision an adversary who is willing to break and enter a computer facility (which can always be effective), or merely one who attempts to fraudulently participate in Senate processes over the public network?
- *Consequences*. Should attacks be successful, what is the nature and seriousness of the impact on the Senate and its members? How does this balance the perceived benefits of conducting business online?
- *Visibility*. If attacks are attempted or successful, will they be visible, so that corrective action can be taken, or is it possible for them to go undetected?

Senate business is quite diverse with respect to these requirements. For simplicity we believe any technological solution should be judged in relation to the *most stringent* requirements that arise in the context of Senate business.

Senate requirements

We now relate the foregoing general discussion Senate business specifically. First some general comments:

¹ The subtle difference between confidentiality and privacy is whether outsiders are able to gain access to discussions without the assistance of committee members (confidentiality) or with that assistance (privacy).

- Generally Senate business is conducted in a collegial and trusting atmosphere. However, some committees require confidentiality to be effective.
- At the discretion of Senate leadership, electronic discussions or votes can be consciously bypassed for any specific item of business in the face of discomfort or unfamiliarity. E-business should always be considered an option.
- We advocate that full participation by non-electronic means be facilitated for any individual Senate member who is uncomfortable or unfamiliar with it.

We assert the following specific requirements (for the most stringent, rather than typical, Senate uses). There are some important caveats about what level of security can be achieved, which we italicize below for emphasis.

- *Confidentiality.* All discussions and documents should be freely available to committee members, but (if desired) closed to non-committee-members (whether Senate members or not).
- *Privacy.* In either face-to-face meetings or electronically, there is no feasible way to prevent members of a committee from disclosing to outsiders the comments or votes of other committee members. Our primary defense against this is collegiality, or in extreme cases sanctions and penalties after the fact. *However, such unauthorized disseminations are both easier and often more widespread and damaging in an electronic context².*
- *Secrecy.* An individual's vote should (if desired, in a 'secret ballot') not be disclosed to other Senate members or outsiders. Both the votes of individuals and the identities of the voters should be captured by the application. There would be two approaches, which different levels of safeguards: (1) As in political elections, the databases of votes and voter identities could be maintained separately, making it impossible later to associate a specific vote with a specific individual. This would limit the visibility into some forms of fraud³. (2) A (confidential) electronic record binding the identity of the voter to each vote could be kept. This would provide greater visibility into fraud problems, and enable more complete post-election auditing⁴. We recommend the second approach, as the confidentiality of this information can be preserved with a high degree of confidence.
- *Accuracy.* Only legitimate committee or Senate members should be allowed to vote, and they should be allowed to vote at most once.

² For example, written comments can easily be taken out of context, and cut and pasted into an email message sent to a widespread mailing list, even anonymously. There is no feasible technological means to prevent this—it is an inevitable consequence of internal disclosure—and once it occurs no way to reverse it.

³ Each voter could be informed by email that they voted and it can be insured that each individual identity is associated with only a single vote (providing visibility into fraudulent votes). The total number of votes as compared to the total number of voters is easily audited. However, if there is any question about changes to votes (say by a malevolent system administrator), there would be no way to audit this.

⁴ All the safeguards of the first approach would be preserved. In addition, voters can confidentially verify that their votes were accurately recorded, or a post-election audit can contact voters to verify that their votes were accurately recorded. On the other hand, this would make it possible for the votes of individuals to be revealed (say by a malevolent system administrator).

- *Attribution.* Participation should never be anonymous—a comment or vote should always be recorded (including identity of the source) and available for later auditing or tabulation, but only by those authorized to do so.
- *Non-repudiation.* Members should be allowed to vote at most once, and not allowed to change a vote once it is cast. If changes are allowed, we expect they would be outside the confines of the e-voting system.
- *Archiving and destruction.* Document drafts and communications should be preserved and available for the duration of a decision-making process. In some instances, preservation indefinitely can be problematic, as for example their unintended availability for lawsuits. In contrast, face-to-face verbal communication is preserved only through the (imperfect) memories of the participants. Document drafts and discussion in electronic media are always systematically preserved through automated backup, and in addition participants may preserve their personal copies. *Absent extreme (an impractical) measures, it is unlikely that electronic records can be fully and reliably destroyed in all their instances.* Thus, it should be assumed that electronic forms of documents and communications are available for the indefinite future in their original form, although various effective measures can be taken to restrict access to them.
- *Third-party access.* All computer systems have one or more system administrators, security managers, or developers who must possess unrestricted access in the course of fulfilling their legitimate roles. It must be recognized that *such administrators, managers, and developers will have access to otherwise confidential or secret information, and if they choose may modify I or reveal it to others, and confidence must be placed in them to not betray that trust.* Fortunately, in almost all cases there would be visibility into these malevolent actions⁵.

The following is our evaluation of the level and nature of threats in the Senate e-business context:

- *Adversaries and threats and consequences.* Various other campus business (like grade submission and e-commerce) is conducted electronically. The security architecture we propose later conforms to measures used for those applications. We believe that the security requirements of those applications are at least as sensitive as Senate business (and in many cases involve the possibility of monetary loss by individuals or institution).
- *Visibility.* Senate business is generally conducted transparently within committees, in full view of its members. In the unlikely event of a security breach, the viewing of outcomes (including tabulations of votes by individual committee members) provides immediate visibility. A notable exception is the secret ballot, where keeping records of voter identity attached to votes (proposed earlier) provides complete visibility (at least for post-election auditing).

⁵ The notable exception is the secret-ballot election if a confidential record linking voter and vote is not preserved.

Aside from these functional requirements, the Senate context imposes other practical requirements:

- Senate and committee members have a widely varying level of expertise and access to computing facilities. Thus, any solution should work transparently across as many computing environments as possible.
- Because Senate members (and student members of committees as well) will access Senate e-business through a variety of platforms (Windows, Mac, UNIX, Linux, etc) and in many cases from personal computers that are not professionally managed (including in residences), relying on the deployment to computers owned by all Senate and committee members of *any* hardware or software specific to the conduct of Senate business is impractical and should be avoided. For the same reason, any approach that relies on storage of information on these personal computers is inherently insecure⁶.
- We assume that all Senate and student members have access to computers with web browsers and an Internet connection, and that those web browsers have specific security features (Secure Socket Layers, or SSL) already widely used for applications on and off campus.
- Many Senate e-business functions (and especially voting) require authentication (verification of identity) of Senate or committee members participating in Senate e-business. Fortunately there is an existing authentication infrastructure on campus, CalNet, which is appropriate for this purpose, and we advise that it be used exclusively⁷. This will not require any Senate-specific capabilities (such as the distribution of secret encryption keys or passwords).

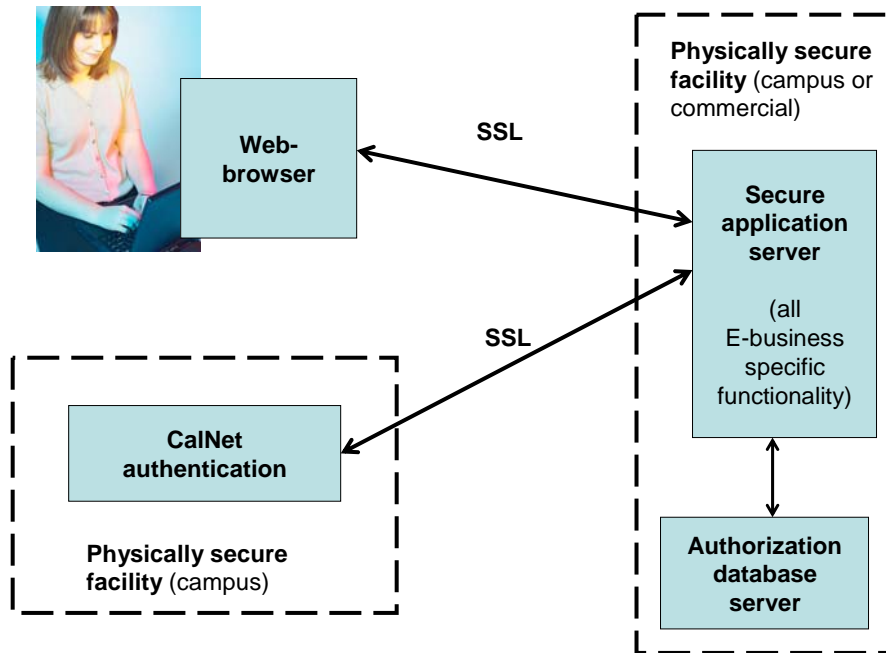
A security architecture

A security framework which we judge to meet all the foregoing requirements is shown below. This is a 'strawman' proposal and deserves additional study before proceeding to an implementation phase⁸, especially as to the specific applications supported.

⁶ Even if we presumed strong security measures like encryption (which we believe is impractical in any case), most of these machines will be in non-physically-secure locations, and thus vulnerable to being compromised.

⁷ This authentication depends solely on the knowledge of a secret 'passphrase' by the individual, and is thus vulnerable to an individual revealing his or her passphrase to others. Fortunately individuals are generally motivated to preserve this secret, since this can bring harm to the individual as well as institution. Stronger forms of authentication do exist, such as biometrics (fingerprint or retinal scan), but require the distribution of special equipment.

⁸ Also, the members of COMP are faculty from a variety of disciplines with a common interest in the use of computing on campus. While we do have a couple members who possess considerable computer and network expertise, none of us is considered a computer security expert.



There are four notable and essential elements of this security framework:

- The *client* is typically a desktop computer used for access by a Senate or committee member to access all features of the e-business application suite. It is presumed that this client has installed any of several widely available web browsers with built-in SSL (Microsoft and Netscape/Mozilla/Firefox, for example). SSL is already presumed for a number of campus applications, including grade submission. Thus, the full capabilities of Senate e-business should be available to those using Windows, Apple, UNIX, and Linux machines⁹.
- All e-business applications execute on a secure *server* located in a physically secure data center¹⁰. Communication between server and browser is secured¹¹ using SSL.
- Authentication of the Senate or committee member is accomplished using the existing [CalNet authentication](#) infrastructure. Most Senate members and students already have a CalNet ID and passphrase¹², which is also useful for downloading campus-licensed software, accessing electronic library materials, submitting

⁹ In rare instances it may be necessary to upgrade the web browsing capability to more recent versions.

¹⁰ The campus operates a newly constructed data center with strong physical security measures.

¹¹ Without depending on the distribution or storage of a secret key to the client, SSL provides three important capabilities: (1) It *authenticates* the server, so that the user will not be fooled by bogus servers. (2) It encrypts all two-way communication using a random one-time 'session' key, maintaining *confidentiality*. (3) The encryption also insures the *integrity* of communication, so that information cannot be changed in transit by an adversary. SSL does *not* authenticate the user or client, but that is the purpose of CalNet.

¹² A few faculty may have to obtain a CalNet ID using well-established campus procedures, but will find that ID useful for various other purposes on campus (such as grade submission). It will be more common for students wishing to participate in Senate committees to have to obtain a CalNet ID.

grades, and various other campus applications. CalNet ID can not only authenticate the identity of the user¹³, but also authenticates the *role* of the individual (at the granularity of faculty member, staff, or student).

- An *authorization database* associates with an individual's identify the authorization to participate in a specific activity. For example, a committee discussion and voting would be authorized for participation of committee members only, and the authorization database would supply the identity of those committee members to the application¹⁴. The authorization database would be maintained by the Senate staff or the committee chair.

Any application software within this framework must be designed or modified to accommodate two capabilities: (1) User authentication by CalNet. (2) Access control at the level of individual votes or discussions based on the CalNet identity in association with the authentication database. This implies that existing software cannot be used off-the-shelf, but must be modified.

Also notable is what this security framework does *not* support, which is application-specific client-based functionality. For example, we do not recommend that client-based email be used for conducting discussions; rather, discussions would be conducted by server-based discussion forums. Using email for this purpose is convenient and familiar, but has several disadvantages:

- Absent other measures, email is not systematically archived and organized. Participants can do this for themselves, but any such effort is duplicative.
- Email can be made confidential by using encryption during transit, and its origin can be authenticated. Software such as [PGP](#) exist for this purpose, but this would violate our principle of avoiding special software and secret key generation or distribution¹⁵. Absent this, it is quite insecure.
- Discussion forums are specifically designed to support group discussions, while email is not. For example, a discussion forum automatically preserves and organizes contribution by topical threads, includes search tools, and so forth.
- Email delivery is not reliable—the biggest problem is removal by spam filters.

¹³ This depends on the user not divulging their 'passphrase' to others. If they do, they can be impersonated. A passphrase cannot be stolen as it crosses the network due to SSL encryption. However, there exist 'trojan horse' worms and viruses and spyware which can capture and transmit keystrokes (including typed passwords) to third parties. The new campus [minimum standards for networked devices](#) are intended to prevent campus-attached (but not residential) clients from being infected.

¹⁴ Ideally the authorization database is maintained completely separately from the Senate e-business applications. However, today it is generally more practical for each application to maintain its own internal authorization database, since the campus has not yet identified a general solution to authorization. This has the disadvantage that separate databases must maintained and updated for each application, and this in turn places a premium on minimizing the number of separate applications.

¹⁵ Email encryption is also somewhat ineffective, as it does not control what happens to the email once it reaches the client and is decrypted, and is vulnerable to any attacker with physical access to the client.

Email is effective as a tool for notifying and reminding committee members of activity on the discussion forums and soliciting their participation. Of course, email can be used for other purposes as long as its non-secure nature is recognized.

Broader campus needs

The Senate needs for secure discussion, voting, and elections are not unique. If the campus had this capability, it could be used for a number of other purposes:

- Sensitive discussions on internal policy and faculty hiring within academic departments
- Search committees for high-level administrative and academic appointments (Chancellor, Vice Chancellors, Provosts, Deans, etc.)
- Review of applications for admission
- Review of proposals
- Staff performance appraisals
- Etc.

Thus, any solution should take into account the broader needs of the campus, not simply exclusively Senate needs. This should also provide additional impetus and resources for implementation and operations.

The application(s)

The Senate e-business application needs three basic capabilities:

- Post documents for access by Senate and committee members.
- Discussion forum to manage postings of comments and replies.
- Survey and voting, with tallying and selective disclosure of individual votes and results. Actually, for most committee purposes the discussion forum can be used for voting; a specific voting capability (capture and tabulation) is required for conducting Senate-wide votes and elections.

All three of these capabilities require *access control*¹⁶ based on committee membership, which in turn requires authentication of users and a role-based *authorization database*¹⁷.

We recommend that off-the-shelf software applications be chosen if at all possible. These functions are reasonably standard, and it should therefore not be necessary to develop them from scratch¹⁸. It is unlikely that one software application will provide best-of-breed capabilities in all these areas. However, it is relatively simple to build a Web-based front end that integrates the interfaces to several applications (especially with the new Web services technologies).

¹⁶ By access control, we mean limiting the ability to view information to those who's identity has been authenticated and who are authorized to view and modify this information.

¹⁷ An authorization database maintains, for each piece of information, identities of all those with permission to view or modify this information.

¹⁸ It may be necessary to add to or modify existing applications to link them to CalNet authentication and to an authorization database.

There are two ways to access software applications: (1) Software can be *licensed* and installed on a secure server on campus, in which case the campus becomes responsible for its operation. (2) The application can be accessed as a *subscription service* over the network, in which case a third party handles the operations. Both approaches are consistent with CalNet authentication—there are a number of existing examples. For example, [CalMatrix](#) (already available to the campus community) is a discussion forum based on the subscription service [WebCrossing](#), where the vendor has specifically added CalNet authentication. (Thus, if you are a member of the campus community, you can login and try out this discussion forum today.)

Advantages can be cited for both approaches:

Licensed or free software installed and operated on campus	Application accessed over the network by subscription
Free (open source) software has no licensing cost	Trial before purchase
Internal control of features and addition of features in the future	Minimal draw on campus staff resources
Data security under total control of campus	Data security subject to contractual terms and penalties
Easier to provide connectivity to other campus applications (like CalNet)	

COMP has not attempted to identify a specific application suite or approach to development and deployment. We believe that this must be subject to additional discussion and study, and ultimately is tied into budget and staffing considerations that are beyond our knowledge or control.

Existing UC Senate e-Business applications

The Berkeley Division may be able to simply adopt an existing application created elsewhere in the UC system.

The UC Office of the President has created the Systemwide [Academic Senate Committee Forums](#) based on [PHP Billboard](#), an open source package for creating community bulletin boards¹⁹. It currently uses a forum-specific password which is sent to each new registrant by email, and of course the registrant can subsequently change this password. This is relatively insecure and inconvenient, although adequate as an interim solution.

In a separate project, the UC Office of the President is creating a "[Federated Identity Management](#)" capability utilizing the Internet2 [Shibboth](#) open source software. This capability will allow UC employees and students to access systemwide applications using

¹⁹ This application does not yet provide voting capabilities, but is oriented around discussions and the posting of documents. As noted above, a forum application should be adequate for committee voting, but it does lack the anonymity and tabulation capabilities that would be important for Division-level voting.

the authentication infrastructure on their own campus²⁰. Specifically, it should be possible to add this capability to the Academic Senate Committee Forums, and UC Berkeley Senate members and staff and students would then be authenticated utilizing CalNet as recommended above.

The UC Santa Barbara Academic Senate has deployed an e-business application called [MySenate](#), which is built using [ColdFusion](#). Although we have not been able to try out the two applications, MySenate is reputed to be considerably more elaborate than the Committee Forums.

Moving forward

The Senate can draw upon the following resources in moving forward:

- Academic senates at other universities should be queried to see if there is relevant experience or role models, and even available software.
- The campus computing staff is experienced and familiar with the acquisition and installation of commercial applications for the campus community, including attendant security issues. As illustrated by CalMatrix, it has already provisioned similar applications for the campus.
- [E-Berkeley](#) is the campus initiative dedicated to the dissemination of e-business technologies on campus, and would be a natural home for initiating and managing this project.
- The [School of Information Management and Systems](#) has a great deal of expertise in this type of application, especially organizational and usability issues.
- We have internationally renowned computer security expertise on the faculty (such as Professors [Tygar](#) and [Wagner](#) of Computer Science), and they should be asked to review any plan prior to implementation.
- COMP would be pleased to review any project plan.

It would be appropriate for the Senate to make a request of the [E-Berkeley Steering Committee](#) to initiate a project. A task force could then be formed to study the details (approach, choice of software applications, etc.), develop a project plan, and estimate budget needs. Various options, including adopting existing commercial applications or the solutions already provided by the UC Office of the President or UC Santa Barbara should be considered. Appropriate task force members would include representatives of E-Berkeley, the Academic Senate, at least one faculty technical expert, and students (especially SIMS students). A second committee consisting of Academic Senate members and SIMS students could be enlisted to study the user and organizational interfaces and make recommendations. Once budget and staff resources were identified, the project could proceed as an E-Berkeley managed project.

²⁰ The Federated Identity Management is in a demonstration phase. This capability is currently planned to be added to UC for Yourself, Your Benefits Online, and the California Digital Library for employees and students at UC San Diego, Irvine, and Los Angeles. Subsequently it can be extended to other applications and all campuses.

Appendix: Candidate applications

Survey and voting

There are dozens of sites supporting online surveys, which can also be used for voting. [SurveyMonkey](#) is a typical site (and see their [pricing page](#) for links to dozens of other similar sites). Another tool that has been successfully used on campus is [Zoomerang](#). None today offer CalNet authentication or a suitable authorization database.

There are two halves to a survey: authoring the survey, and taking it (or voting). The latter should be simple for anyone accustomed to using a web browser and not require training. The former is a little more complex, and this is where the training issue comes in. We believe the way to handle this is to train a staff member in the Senate Office to author these surveys. Committee chairs can simply convey the voting issue to the Office, which can manage the authoring and informing of committee members.

Posting and discussion

Shared document repository, collaborative authoring, and shared discussions is one of the most common category of web-based software solutions. It is so common that choosing a suitable solution from among voluminous choices will be difficult. Many of the available solutions are much more elaborate than what the Senate needs, which makes them unnecessarily difficult to use and expensive. This plus compatibility with the chosen security model should allow the choices to be narrowed quickly. As an example, see the services [WebEx](#) and [Microsoft Sharepoint](#) and for more options the white paper (a little dated) [Choosing Web Conferencing Software](#) by David Woolley. [WebCrossing](#) is a viable choice, is already CalNet enabled, and this vendor has developed a multi-faceted relationship with the campus.

One interesting option is the [Sakai project](#) software. This is an multiple-university open source project (in which UC Berkeley is participating) to create the e-learning software of the future. Sakai will include discussion and collaboration components, and has the advantage that many faculty and students will already be users. (However, it is not today mature enough for this purpose.)

Acknowledgement

The [E-Berkeley Implementation Task Force](#) reviewed this document and we appreciate their valuable guidance and suggestions.

Revision history

Nov. 4, 2004: First committee-approved version posted, and Chair Knapp notified.

Nov. 15, 2004: Revised version posted after Systemwide ITTP Committee meeting, with addition of a section on what other UC Senate organizations are doing.