

Voting Over the Internet Using Public Key Infrastructure

Author: Wayne J. Schepens

Purpose:

To develop a pilot project providing a secure electronic alternative to absentee voting in efforts to enhance the efficiency and security of the absentee voting process. Demonstrate acceptance among the local governments participating while encouraging others to pursue the convenient and safe service this program provides. Explore the security services authentication, availability, confidentiality, integrity, and non-repudiation provided for the transmission and delivery of objects related to the voting process, from request of registration through ballot submission.

Method:

Follow the Systems Engineering Design process to develop the concept, design a solution, and execute a pilot project with the participation of five jurisdictions within the four states endorsing the project. An iterative approach of analysis, synthesis, and evaluation was applied to ensure requirements meet customer expectations and the system performs the functions at least equivalent to the existing paper absentee voting process. The pilot project, including a subset of the population served by *the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)* will test to validate security acceptance, feasibility, and usability.

Results:

After performing initial interviews and data gathering sessions with the advocate organization we spent several months prioritizing the system requirements and developing an initial concept. We were then provided the opportunity to present our concept during the January 1999 Alliance Conference in Rosslyn, Virginia. Those in attendance included the Senior Service Voting Representatives, state and local jurisdiction representatives, and technical staff from the participating States. This audience was extremely receptive and stated the concept was a 90% solution. This was impressive since we had yet to have the opportunity to meet with the participating States themselves. To this point all was worked through the advocate organization. The States accepted our request to perform a site survey to gather site specific information and requirements.

The site visits were performed in April of 1999 and subsequent to this effort the requirements were frozen for development of the pilot project. The pilot was developed through the summer and fall of 1999 and delivered for installation and training in December 1999. The January 2000 deadline for registration was met. Registration is currently on-going and results for the system's performance will be analyzed during an evaluation period planned after the November 2000 General Election.

New or breakthrough aspect of work:

This work describes an application of the Department of Defense (DoD) Medium Assurance Public Key Infrastructure (PKI) to harness the security services of authentication, availability, confidentiality, integrity, and non-repudiation. This asymmetric form of cryptography provides the capability to digitally sign and encrypt the objects transmitted through the system. To operate within the system all major system components were required to obtain DoD PKI certificates. These components include the following: citizen (end user), advocate server, and local jurisdiction server. For ease of implementation, the advocate organization was designated a Certification Authority to distribute certificates to all involved.

Conclusions:

It was demonstrated that a solution for a "secure" electronic alternative to absentee voting was achievable with the use of PKI. Vulnerability studies were performed and the results, including that of Third Party testers, were collected and analyzed. The risk associated with voting over the internet proved to be within the bounds of acceptance for the States and advocate organization. It is yet to be seen whether that will be the case with the remainder of society.