

Voting Over the Internet (VOI) Technical Overview

**16th Annual Computer
Security Application
Conference (ACSAC)**

December 2000



BOOZ·ALLEN & HAMILTON



**Federal Voting
Assistance
Program (FVAP)**

Overview

- **Provide Background on VOI Pilot Effort**
- **Provide High Level Technical Overview**
- **Security Services**



Background of VOI

- **Post-election Surveys Show That the Single Biggest Barrier to Military and Overseas Citizen Absentee Voting Is Mail Transit Time**
- **Use of Fax Transmission During Desert Shield/desert Storm Was a Great Success**
- **46 States Now Allow Electronic Transmission of Absentee Voting Materials**
- **Can the Internet Be Used As an Alternative Absentee Voting Method?**
 - Must Preserve Integrity, Secrecy and Ability to Audit Electoral Process



Program Goals

“To examine the feasibility of using the Internet as an alternative method for absentee registration and voting for UOCAVA* citizens through a small scale pilot system”

- **Multiple Layers of Security to Achieve Acceptable Risk Reduction**
- **Use the Internet As a Communications Backbone**
- **Maximize the Use of Commercial Off-the-shelf Technologies)**
- **Use the DoD Public Key Infrastructure**

* “Uniformed and Overseas Citizens Absentee Voting Act”

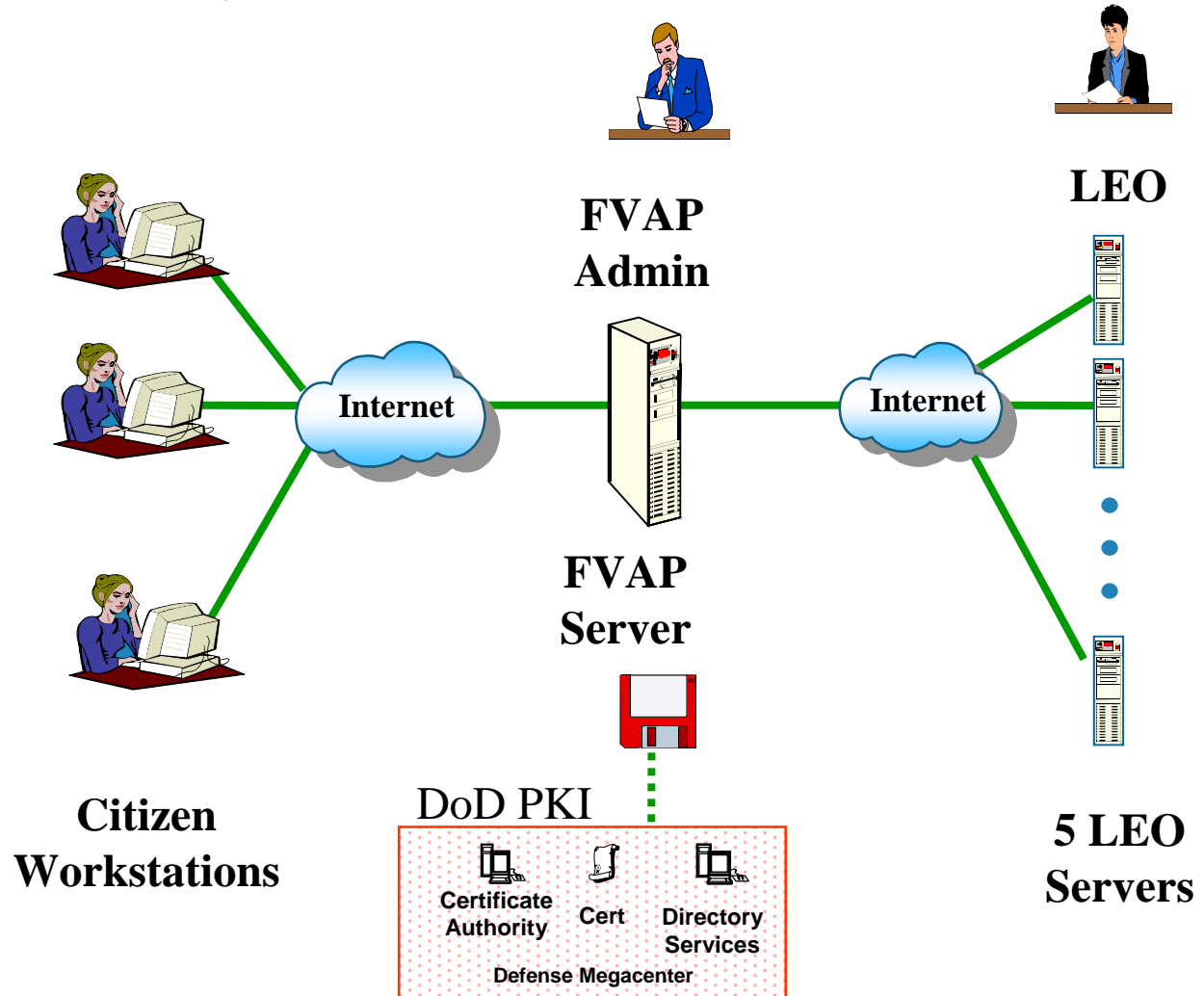


Scope of VOI

- **Feasibility Assessment: Technology & Process**
- **Small Scale, Federal/State/Local Pilot Program**
- **Participating Jurisdictions**
 - State of South Carolina
 - Okaloosa & Orange Counties, Florida
 - Dallas County, Texas
 - Weber County, Utah
- **Provided Absentee Registration and Voting for 2000 General Election**



VOI System Architecture



Voting Over the Internet



VOI Technical Features

- **Commercial off-the-shelf HW & SW**
 - RSA toolkits
 - Microsoft IIS and SQL Server
 - Netscape Browser
- **Open standards**
- **Custom software applications**
 - Registration
 - Ballot generation tool
 - Voting
- **Internet communications backbone**



Citizen Workstation

- **Citizen with a DoD Certification (P12 file) on a floppy disk**
- **PC with Internet Connectivity**
 - Netscape Browser with strong encryption
 - Custom VOI plug-in installed



FVAP Server Segment

- **Provides PKI Services to all Backend LEO Server Segments**
- **Acts As a Trusted “post office”**
 - Appends a date time stamp on objects from the Citizen
 - Signs the new object
 - Distributes the object to correct LEO
- **Transaction Monitor**
 - Records system transactions



FVAP Server Segment

- **PKI Services**
 - Signature Check
 - CRL Check
 - CRL Loaded Manually
 - Certificate Chain Validation
 - CA-1 or CA-2 and DoD Root
 - Date Expiration Check



LEO Server Segment

- **Receives All Completed Registration Forms and Voted E-Ballots**
- **Support LEO Workflow**
- **Support E-Ballot Processing**
 - Reconciliation
 - Stripping Citizen info from E-Ballot Object
 - E-Ballot Decryption
 - E-Ballot Printing



VOI Security Features

- **Multiple layers of security to achieve acceptable risk reduction**
 - Object security
 - Transmission security
 - Operational security
 - Physical security
 - Personnel security



VOI Security Solutions

- **Public Key Cryptography**
 - Integrity
 - Identification & Authentication
 - Non-repudiation
 - Confidentiality
- **Secure Sockets Layer**
 - Transmission security
- **Intrusion Detection System**
 - Unauthorized probing and access



Personnel Access Control

- **Certificate-based access control for citizens**
 - Portable Security - *“Floppy is the Token”*
 - Access limited to VOI Pilot participants
 - Access control based on Citizen’s Common Name
- **SSL3 Certificate-based access control for FVAP and LEO admin staff**
 - Admin staff authenticated using standard COTS SSL3 mechanisms
 - Access limited to small list of authorized personnel
 - Access control based on Admin’s Common Name



Transmission Security

- SSL3 without required client certificates between Citizens and the FVAP Server
 - Citizen is NOT required to load certificate into the browser prior to accessing the system
- SSL3 with client authentication for LEO and FVAP admin staff
 - Certificates must be installed into the browser prior to accessing the system
- SSL3 without required client certificates between FVAP and LEO servers
 - COTS web products do not support certificate exchange for mutual authentication!



Transmission Security

- **Router based security**
 - Access control filters
 - Access restricted based on source and destination IP addresses
 - Access restricted based on network service type (TCP, ICMP)
 - Access restricted based on TCP application service ports



Cryptographic Security Services

- **Digital Signatures**

- 1024 bit keys
- Widely used for various security services
 - Authentication
 - Data integrity
 - Non-repudiation

- **Encryption**

- E-Ballot Triple DES encryption (112 bit keys) modeled after S/MIME secure messaging model for confidentiality (secret ballot)
- E-Ballots encrypted using LEO privacy certificate
- Only authorized LEO staff can ever decrypt E-Ballots



Summary Points

- **COTS Alone Inadequate to Meet Security and Operational Requirements**
 - Custom plug-in
 - Voting application required modifications to existing protocols
- **Third Party Review of Security Architecture and Design Required to Build Confidence**



Summary Points (Cont.)

- **This Is About As Important As Any Application There Is**
 - Need to Move Carefully and Diligently
 - Security is Recognized as the Key Component



Presenter POC Info

Edward Rodriguez
Booz, Allen & Hamilton, Inc.
rodriguez_ed@bah.com

