Cryptography Requirements

Crypto Basics

- All crypto be done in a FIPS 140 validated cryptographic module.
  - Standardized, secure cryptography
  - Mature testing program
    - 13 commercial CMVP labs do testing worldwide
- Minimum of “112-bit strength”
  - What we’re requiring for Fed Gov. by 2010
  - TDES, AES 128, 2048 RSA/DSA, 224/256 ECDSA, SHA 224/256
    - NIST SP 800-57 Part 1
  - Should be good for a couple of decades

Crypto Module

- Separate program or device for cryptography
- FIPS 140-2: a crypto module test standard
  - 4 security levels (next version will have 5 levels)
- NIST has a Cryptographic Module Validation Program with 13 commercial CMVP test labs
- *Software* and *hardware* modules
  - Software modules are just programs
  - Hardware modules are often just little microcomputers dedicated to cryptography
    - Separate little fairly easily tested sandbox for crypto

Public Key Cryptography

- Two related keys:
  - Public key can be made public
    - Encrypt or verify digital signature
    - Usually presented in a public key certificate
  - Private key must be kept secret
    - Decrypt or sign digital signature
  - Public key cryptography is relatively slow
    - Use with symmetric key mechanisms for better performance

Digital Signature: Signing

- First we hash the message we're going to sign to generate a short (e.g. 256-bit) message digest of the message
- Then we apply the private key to the message digest to generate the signature.
- Often include the PK certificate of the signing key with the signed message to authenticate the public key

Digital Signature: Verification

- Verifier hashes the signed message and applies the public key to the message digest to verify the signature
- Verifier then knows that the corresponding private key was used to sign the message, and that it has not been altered in any way since.
  - Authenticates message and largely eliminates chain of custody issues

Public Key Certificate

- A digitally signed message
  - Often signed by a “Certification Authority”
  - May also be “self-signed”
- Binds a public key to
  - The name of the issuer (issuer name)
  - The name of the key holder (subject name)
  - Any other attributes desired (e.g. issue date)
- Widely used standard format is “X.509”

Signature Module

- Hardware Crypto Module
  - A separate chip, not just a program
    - Permanently attached to the motherboard
      - If the module dies, the voting device dies
    - Typically a small microcomputer, with the programming burned into ROM (permanent memory)
  - Generates it's own signature keys
    - Private key components never leave module
  - Generates its own public key certificates
  - Protects private key from compromised system software

Signature Module

- Requires capability to
  - Generate public-private key pairs
    - Implies a random number generator
  - Store two private keys securely
  - Store and output Device Public Key Certificate
  - Perform the private key (signature operation)
  - Generate complete signatures and public key certificates
    - Implies capability to hash messages
- All other crypto can be done in on the voting device in a software crypto module.

Signature Key Management

- Philosophy: make it as automatic as possible
  - Long term “Device Signature Key” comes with the device from the factory, lasts the life of the device
  - Short term “Election Signature Key” created automatically in election setup process
    - Used to sign audit records for a single election
  - Election private key destroyed in election closeout process.
    - After private ESK is destroyed, no way to create new audit record for this voting device

Device Signature Key (DSK)

- A public/private key pair
- Generated in Signature Module at the factory
  - Private key never leaves the SM
- Device Public Key Certificate
  - Binds Device Pub. Key to voting device unique ID
    - Typically manufacturer, model and serial number
    - Placard on outside of voting device
  - Stored in module, but can be exported
  - Created by device manufacturer
  - Can be self-signed or signed by an appropriate CA

Election Signature Key (ESK)

- Key pair generated by Signature Module as a part of election setup.
- Election Public Key Certificate created as a part of election setup
  - Subject name is election identification information
    - No standard given for format of election identification
  - Issuer name is the Device Unique ID from the Device Public Key Certificate
- Count kept of number of times each election private key is used

Election Closeout

- Output a signed summary telling how many times the EAS was used.
  - Should be able to account for every use of the ESK
- The ESK is erased.

Summary

- Hardware signature module
  - Protects keys from corrupted software
  - Used to sign audit records
- Permanent Device Signature Key
- New Election Signature Key for each election
- Simple, automatic key management by the Signature Module