GAO Sanctioning Process and PKI System Issues

PKI Steering Committee

August 27, 2001

Overview

- Background
- GAO sanctioning process
- PKI integration issues
- Future GAO work
- How highly automated systems change the audit process
- Questions

Background

- GAO support for electronic records
  - 1984 - GAO reviewed Treasury's wire transfer system
    - Better method needed to authenticate high dollar value transactions
    - GAO provided conceptual example of how electronic signatures could improve controls

Background

- 1984 - Treasury decided to convert its payment processing system for agency payments from paper to electronic
  - Treasury adopted and improved the model suggested by GAO and developed the Treasury Electronic Certification System
  - GAO sanctioned the production system in November 1988
- GAO formally recognized that something other than a handwritten signature, or similar technique (stamp, autopen, etc.), was a symbol of the intent to be bound

Background

- 1991 - Comptroller General Decision issued regarding Electronic Data Interchange
  - No statutory prohibitions exist that prevent agencies from forming and maintaining government contracts when adequate data integrity is maintained

Background

- Provided criteria that we use to evaluate electronic signature systems
  - Unique to the signer
  - Under the signer's sole control
  - Capable of being verified
  - Linked to the data in such a manner that if the data are changed, the signature is invalidated during the signature validation process

➢ Criteria is the same as handwritten signature process used in paper based processes

- Signature is used to show an individual's intent to be bound

Background

- 1996 - GAO sanctioned a full scale implementation of standardized electronic signature system used in the Corps of Engineers Financial Management System
  - Design allows Corps to move to a “paperless” financial management system
  - Over 30,000 users world wide and tens of millions of electronic signatures generated

GAO Sanctioning Process

- System adopted by Department of State for one application
  - Reduced development risks
  - Saved about $750,000
  - Reduced deployment time by 30 months

GAO Sanctioning Process

- GAO has sanctioned 3 systems and is in the process of reviewing several others
  - GAO has also been asked by three agencies -- FDIC, DOD (Defense Joint Accounting System and Wide Area Workflow), and Corps of Engineers to consider sanctioning PKI based electronic signature systems that are under development

GAO Sanctioning Process

- GAO's involvement in sanctioning an electronic signature system is constructive engagement rather than the traditional audit role
  - Informal comments are provided on critical documents and processes
  - Agency is free to disregard GAO's informal comments, however, GAO makes it clear on what impact, if any, this could have on GAO's ability to sanction a system
  - GAO does not use the work performed in the sanctioning process to generate traditional GAO reports

GAO Sanctioning Process

- The only formal document that GAO produces is a sanctioning letter
- GAO may later review the system using another audit team

GAO Sanctioning Process

- Basic steps
  - Agency contacts GAO and requests their involvement in the development process with the ultimate goal of sanctioning the system
  - GAO decides whether to participate in the project
  - Critical documents are reviewed
    - Concept of operations
    - Policies and procedures
    - Test evaluation reports
  - Sanction letters

GAO Sanctioning Process

- System is evaluated against the 4 criteria for evaluating electronic signature systems
  - How are keys generated
  - How are certificates linked to a given individual
    - Physical identification
    - Limitations on acceptance of certificates issued by third parties

GAO Sanctioning Process

- How are split knowledge and dual control concepts utilized
  - One individual authenticates the certificate holder
  - Another individual authenticates that certificate holder should have a given certificate
- Are FIPS 140 compliant cryptographic modules used
  - Level 1 modules for general users
  - Split knowledge and dual control hardware modules for Certificate Authorities (generally Level 3 or 4)

GAO Sanctioning Process

- Have the critical policies and procedures been documented
- Are adequate audit trails maintained
- Has the system in operation been adequately implemented

PKI Integration Issues

- Integrating an effective PKI into an application is not hard, it just requires disciplined development processes
  - Disciplined development processes
  - Application integration

PKI Integration Issues
Disciplined Development Processes

- Disciplined development processes
  - Disciplined software development and acquisition processes are needed to maximize the likelihood of achieving the intended results (performance), within the established resources (costs), on schedule
  - Although disciplined processes have been shown to reduce development time and boost productivity without harming quality, cost, performance, or maintainability, they are not used by the majority of developers in the public and private sectors
    - Disciplined processes come over time and require a combination of tools and methods that take time to effectively implement

PKI Integration Issues
Disciplined Development Processes

- Discussion of what constitutes disciplined processes is beyond the scope of this presentation
- Examples of products produced and processes used by disciplined organizations in electronic signature applications include
  - Concept of operations document
  - Standard interface between electronic signature system and user applications

PKI Integration Issues
Disciplined Development Processes

- Concept of operations
  - Describes system characteristics from a user's point of view
  - User organizations, missions, and organizational objectives are explained from an integrated systems point of view
  - Used by disciplined organizations to reduce requirements related defects
    - User acceptance test cases are drafted to help identify requirements related defects
    - Provides the foundation for identifying functional requirements

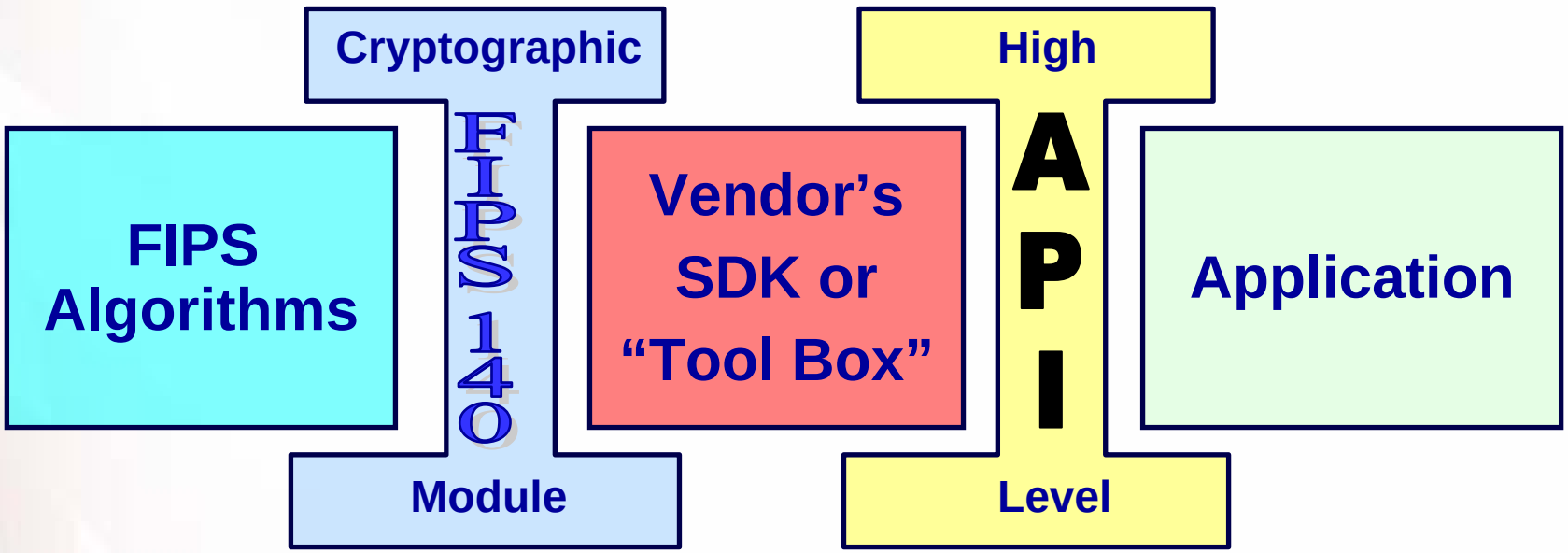
PKI Integration Issues
Application Integration

- Standard interface between electronic signature system and applications needing electronic signature services -- high level calls or high level API
  - Experience on Treasury, Corps, and State efforts have demonstrated benefits of high level calls
    - According to State, they saved about 30 months and $750,000 in development by utilizing a standardized electronic signature system that was developed by the Corps of Engineers
    - Corps of Engineers found that its developers would “rather fight than switch” to low level calls

PKI Integration Issues
Application Integration

- Makes the critical security functions a “black box”
  - Interface must be standard and stable
  - Applications can “trust” the electronic signature system
    - Security review of electronic signature system is not required each time a new application is “electronic signature” enabled
    - Question is whether application developer made the standard call, not whether the application developer properly coded the electronic signature functionality
  - Security boundary conditions are well defined which facilitates evaluation and risk management

PKI Integration Issues
Application Integration



PKI Integration Issues
Application Integration

- August 1996 - Energy developed a PKI specifications document for electronic signature services
  - Defined the high level calls for the signature services that would be used in a travel system
    - Log in and log out
    - Sign data and verify signature
    - Generate certificate, renew certificate, revoke certificate, get certificate by name or number, get CRL
    - Remove private key
  - COTS vendor did not implement the calls as promised

PKI Integration Issues
Application Integration

- FDIC is leading a project that includes several agencies (e.g., Energy and Treasury) to update the high level calls and provide additional functionality
  - Using high level calls developed by NIST for Energy's PKI project
  - Includes calls for encrypting and decrypting data
  - Unlike the Energy document, it does not define how to "interact" with CA, e.g., generate certificate, since FDIC plans on using the vendor's existing process for handling this functionality

PKI Integration Issues
Application Integration

- Although current approach facilitates vendor independence, a couple of items remain
  - Revisit Energy document to determine changes needed because of a better understanding of the “problem” and to support additional functionality
    - Are changes needed high level calls associated with certificate authority operations need
      * Generate certificate, renew certificate, revoke certificate, get certificate by name or number, get CRL
    - Additional functionality - encryption key management

PKI Integration Issues
Application Integration

- Vendor independence
  - Allows best solution for a given requirement
    - Certificate Authority functionality
    - Registration Authority functionality
    - Various types of user devices, e.g., smart card, software, other tokens
  - Demonstrated in Corps of Engineers system
  - Reduces development risks for COTS vendors
    - Answers questions on which PKI product(s) should be supported

PKI Integration Issues
Application Integration

- Utility programs are needed for audit purposes
  - Independent validation of electronically signed data using an input file specified by the user
  - Supports analysis of the critical data characteristics associated with a given signature transaction
  - Supports verification that critical files associated with the electronic signature system or other systems have not been altered after they are approved for production
  - FDIC effort is defining the requirements for such programs

Future GAO Initiatives

- GAO has been asked by agencies how electronic signature technology should be implemented and are willing to discuss the internal controls that must be present for a given risk level
- Several different “architectures” may need to be addressed
  - Traditional client/server
  - Web based
  - Legacy and COTS applications

Future GAO Initiatives

- Traditional client/server
  - Basic approach used in previous systems sanctioned by GAO
    - Generally associated with custom development since other methods generally do not yet provide this ability
  - Signing takes place on client
  - Transaction level data integrity
  - Internal control issues associated with this process are “well understood”

Future GAO Initiatives

- Web based applications
  - ➢ May not support traditional client based signature techniques
    - Development of browser “plug in” may be costly and users may not want to install new software
      - Internet Explorer 6.0 does not support plug ins
    - Risk associated with application may not justify development of an electronic signature system that that signifies an individual’s intent to be bound and provides the traditional transaction level data integrity

Future GAO Initiatives

- We have been asked by DOD to review a web based system that only uses User IDs and Passwords
  - Desire to use system as an interim solution until DOD PKI is rolled out
  - Have discussed the conceptual approach and, assuming DOD complies with the agreed upon internal controls, we expect to use this as an example of how data for low risk web based applications can use User IDs and Passwords to generate electronic signatures that signify an individual's intent to be bound
    - Controls that will be used and approach are outside the scope of this presentation

Future GAO Initiatives

- Legacy and COTS applications
  - ➢ Most legacy and COTS applications do not support electronic signatures that signify an individual's intent to be bound
    - May use PKI to perform secure sign on functions, however, data is "signed" by linking the user ID or equivalent to the data
      - Data is still exposed to the risks associated with inadequate general and application controls
    - Inadequate implementation of PKI techniques
      - Failure to properly implement FIPS algorithms
      - Inadequate certificates

Future GAO Initiatives

- At least three conceptual approaches to implementing effective electronic signature techniques in legacy and COTS applications
  - Transaction level
    - Will require a great deal of application rework
    - Will probably be a long transition period
    - Standard interface should help expedite this process

Future GAO Initiatives

- System signing
  - Electronic signature generated by an electronic signature server on data received through network
  - Does not generally provide a strong bond between individual and data since network is trusted for at least a short period of time
    * Does provide assurance that data has not been altered after it was signed which limits the time that weaknesses in general and application controls can impact data integrity
    * Requires good configuration management in order to “recreate” and validate the transaction in questioned
    * Requires development of utility programs that can be used to check the integrity of data base

Future GAO Initiatives

- Periodic backups
  - Periodic data base backups (at least daily) are performed and then signed
  - Does not provide a strong bond between individual and data
  - Exposes data to general and application control weaknesses for longer period of time which reduces confidence in data integrity
  - Requires very good configuration management and data recovery techniques
  - Utility programs required to periodically validate data integrity

How Effective Electronic Signature Systems Change the Audit Process

- Data integrity is a key question that auditors must address
  - Level of effort is directly related to the quality of the data that is used
  - Effective electronic signature systems can help provide the necessary data integrity to reduce the audit effort
    - Adequacy of electronic signature system's implementation must be assessed
    - Auditors must understand how to use the electronic signature system to validate that key controls, e.g., separation of duties, have been effectively implemented

How Effective Electronic Signature Systems Change the Audit Process

- Examples
  - Electronic signature system used by the Corps allows the automated determination of whether an adequate separation of duties had been implemented and the extent of any weaknesses
    - In most systems without effective electronic signature systems, it is very difficult to assess the quantitative effects of weaknesses identified

How Effective Electronic Signature Systems Change the Audit Process

- General and application control weaknesses lead to questions on the reliability of the data, however, by checking the electronic signatures, a quantitative measure is available to assess the impact of the weaknesses identified
  - Although weaknesses still need to be corrected, at least a measure is available to determine the impact

Summary

- GAO supports electronic records when data integrity is maintained
- GAO has sanctioned 3 systems and several systems are currently being reviewed
- The sanctioning process is a constructive engagement between the agency and GAO
- PKI implementation issues can only be addressed through disciplined processes because of the institutional will associated with disciplined processes

Summary

- Standard interface facilitates a risk based evaluation of an electronic signature implementation and reduces the risks associated with integrating an electronic signature solution
- Effective electronic signature techniques can significantly change to way that a system is audited

Questions

martinj@gao.gov

202-512-9481