Federal Technology Service

ACES and PKI

The Business Case for e-authentication

What Is ACES?

ACES (Access Certificates for Electronic Services) – GSA's digital signature certificate program was developed to allow the public and government business partners, vendors and government agencies a secure way to conduct business with the Federal government over the Internet.

Legislative Mandates

Paperwork Reduction Act required agencies to justify the creation of new systems requiring the collection of paperwork.

FPKI Steering Committee Access with Trust … Published in September 1998 to provide insight to government managers on fostering safe, secure electronic interactions, internally and externally, through the use of public key technology. ACES is a key initiative of the Access with Trust document.

Government Paperwork Elimination Act requires all agencies to make forms applicable to at least 50,000 individuals available electronically via the web. The Deadline for Agency compliance is October 2003.

Electronic Signatures in Global & National Commerce Act – signed into law, June 2000. Eliminates the legal barriers to electronic commerce while preserving protections for consumers.

Health Insurance Portability & Accountability Act (HIPAA)…Adopted in 1996, ensures the privacy and security of health care information.

Benefits of ACES

- A complete IT web-base security solution
- Provides authentication, non-repudiation, data integrity and identification
- Eliminates Agency costs for establishing own Certificate Authority (CA) saving an estimated $500,000
- Compatibility – Common access across government
- Meets current and emerging regulatory requirements
- Provides a Government-wide Public Key Infrastructure
- Reduces overall costs by aggregating Government requirements

Benefits of ACES (con't.)

- Allows individual agencies to leverage off each other's requirements
- User friendly – Clients can have one certificate to do business with multiple agencies

Business Case for ACES

Normally when making security decisions, we look at the cost of the security provided compared to the value of what we are protecting. Federal agencies today must make those decisions in light of the legislative mandates we just discussed. Value of the data being protected is not the only consideration here.

Why do a business case?

- Provides decision makers with data and documentation on various proposed e-authentication/PKI programs to enable them to determine if the cost of PKI is justified.
- Ensures that the ratio of benefits to risk is sufficient.
- Compares cost of present information processing versus cost of processing it electronically.
- Evaluates the enhancement of agency's mission-critical goals if PKI/e-authentication is implemented.
- Compares the risks of implementing e-authentication to the rewards.
- Compares other ways to protect information such as pin-password. bar coded cards, Smart Cards, and Bio-metrics (alone and in combination with other technologies.

Compare Alternatives

- Prepare business case analysis, evaluating and comparing various life cycle costs, and estimates of benefits.
- Use resulting information to assists in developing the financial analysis needed for budget and funding proposals.
- Weigh this information against possible risks.

Business Case Factors

- Costs of Implementation
- Strengths of PKI
- Benefits Comparison
- Risk Evaluation

Cost of Implementation

- Equipment purchases
- Training of personnel
- Software upgrades
- Management of the program
- Number of staff members dedicated to the program, including Help-Desk Support
- Proposed number of Registration Authorities, comparison of various Certificate Authorities, their price per certificate issued, and comparison of transaction based and flat-rate certificate options

Strengths of PKI/ACES

- **Authentication** – allows agencies to verify identity of users remotely, giving both the agency and the user confidence in the system.
- **Technical non-repudiation** – Because certificates are validated by the Certificate Authority when presented to the agencies, users cannot deny the transaction, providing recourse to the agency.
- **Data Integrity** – Documents are protected from modification during the transaction.
- **Confidentiality** – Both user and agency know that transaction is protected.
- **Interoperability** – One ACES certificate can be used across multiple agency applications and across government.

Benefit Comparison

- What are the monetary benefits to implementation (Return on Investment)?
  - ACES takes a fundamentally different approach from other programs in the industry. To provide sound ROI information, GSA is issuing a task order for a cost benefit analysis to be done, comparing ACES to other programs and giving decision makers the tools needed to select the best PKI product for their situation.
- Value of other benefits such as improved morale, increased productivity, reduced errors in data and time lost to locating and correcting errors.
- Other areas to consider that are less-easily defined are increased public awareness, increased user confidence improved security.
- Customer service benefits include capability for self service on a 24-7 basis.

Risk Evaluation

- Certificate Authorities – Compare them to ensure their reliability, their track record with other agencies, their depth of knowledge and ability to respond to problems
- Interoperability of your PKI solution
- Industry standards
- Organizations formed to enhance the effectiveness of PKI/e-authentication
- Consistency of your program with that of the Industry
- Will the money invested satisfy the legislative mandates
- Determine “Best Practices” data and apply to decision making process

Summary

A business case provides decision makers with the necessary information to make a major business decision. By comparing costs,benefits and risks, the decision makers have at their fingertips critically analyzed information, helping to ensure that the resulting decision to use PKI/e-authentication is the correct one.

Examples of Federal PKI Implementations

- National Institutes of Standards and Technology (NIST)

- Social Security Administration (SSA)

National Institute of Standards and Technology (NIST)

- ACES Task Order for the electronic submission of proposals for the Advanced Technology Program (ATP)
- Task order was for $900,000
- Uses digitally signed documents to send proprietary information over the Internet, digitally signs and encrypts forms, captures data and populates ATP database
- Uses a web server for downloads/submission of forms and documents, then pulls them behind NIST and ATP firewall
- Piloted from 8/22/01-9/26/01 with 15 users (70 users expressed interest in participating)
- Goal of receiving 10 proposal submissions, actually received 12
- Will go “live” when ATP’s next competition opens

Social Security Administration (SSA)

- Using ACES Digital Signature Certificates for on-line annual wage reporting
- Following pilot, SSA had a 90 percent approval by the 100 businesses participating for tax year 1999
- Automating W-2 submissions critical to agency where nearly 6.5 million employers submit over 240 million W-2 forms for their employees
- Continuing to expand pilot capabilities and implementing digitally signed forms

Conclusion: ACES Benefits

With ACES, you can achieve assurance of identity in your electronic transactions with the public – at the same or higher level of confidence that you have doing business with paper, for a modest initial outlay and very minimal recurring costs

- Control access to private or business-sensitive data
  - Trusted, logged, auditable access
- Receive digitally signed documents
  - Trusted, auditable signatures that are authenticated and stand up in court; are achievable…
- Using a government-certified, GISRA-compliant, OMB-approved system that cuts across Government stove-pipes
- Citizen gets one face to government

ACES
Access Certificates for Electronic Services