"Managing Your Return on Investment (ROI) for Public Key Infrastructure (PKI) Security in the Digital Future"

Peter J. Butziger

Booz Allen & Hamilton
410-684-6698 (W)
410-850-4592 (F)
butziger_peter@bah.com

The digital future holds unprecedented convenience and efficiency of data access. However security remains one of the most limiting growth factors across all industries. These security concerns include: confidentiality of connectivity (internet and beyond), application of digital signatures in paperless environments, single sign-on authentication, and evolving court cases of hacker damage and corporate liability. What are IT professional expected to do when the demands are to do more with less money, time, and resources? The evolving answer to all of these security concerns is an investment in a security foundation called Public Key Infrastructure (PKI). Many people have been playing with this technology within the internet and email worlds for years and new vendors are showing up by the dozens to get a share of this explosive and promising security market. However, it still seems to be missing the mark for corporate Information Technology decision-makers. Where is the Return on Investment (ROI).

PKI for Confidentiality: Customer security profiles historically focus on exposure of assets to determine how much to spend on security. This continues to be a solid approach for traditional confidentiality security markets (e.g. intelligence communities, national & trade secrets). Confidentiality of data during storage often requires the cost of a trusted third party for key recovery of the privacy key in PKI. Transmission confidentiality vendors primarily utilize PKI asymmetric keys to swap traditional runtime symmetric encryption keys (faster cryptography) to achieve secure pipes. The rapid growth of the Internet has provided a new avenue for many markets to potentially achieve substantial savings in reduction of distribution and commission costs (varies based on market). However, this changes the traditional exposure of assets paradigm with the customer's assets at risk (i.e. credit cards for EC/EDI) as opposed to the traditional security investor (corporation or service offerer). Most markets could afford to invest in PKI Secure

Sockets Layer (SSL) browser based security with the potential for even greater savings. The predictability of customers to trust in the fundamental uses of PKI is the multi-billion dollar question. Will a sufficient percentage of customers change their buying habits to achieve a timely PKI ROI for corporations or service offerings? To date the Internet security PKI confidentiality approach has failed to generate sufficient confidence in the customers who would put their own assets at risk. This is somewhat ironic given the willingness of customers to give a waiter (total stranger) their credit card or toss receipts bearing such information in the trash. The U.S. Government currently limits a customer's liability to $50 in the case of credit card fraud although no similar liability basis has been set for the issuance and use of PKI X.509 certificates.

PKI for Identification and Authentication: The historical I&A market also uses the exposure of assets measurement paradigm like confidentiality. The market is seeing new promising expansions beyond the intelligence comminutes partially due to the popularity of single sign-on. Passwords have proven to be somewhat ineffective as something we know is often limited to something written down on a sticky attached to the monitor screen. With the increased threat of a single sign-on to multiple applications, many corporations are searching for a combination of something you possess and something you know. The standards communities are still fighting over defacto single sign-on standards and the vendors are aggressively turning out products with limited interoperability. This use of PKI does not require third party key recovery. The I&A PKI user base can be substantial but not as big as digital signatures. The primary factors of I&A PKI ROI surround the frequency of PKI certificate reissuance and the strategy for access control. The reissuance options vary from run your own certification authority (and cost effectively protect it) to outsource the issuance and reissuance of certificates. The Local Registration Authorities (LRAs) have made outsourcing increasingly appealing by leveraging existing corporate resources. The alternative access control strategies range from leveraging X.509 certificate extensions to indicate classification (great for data that is already classified) to access control lists maintained either centrally or decentralized by application. The PKI ROI for I&A is increasingly based on revocation of authorized privileges along with prevention of access. The desire to revoke privileges instantaneously (due to hackers) has led some to prefer centralized access control lists.

PKI for Digital Signature: The automation and reengineering of systems is increasingly dependent on the elimination of paper and the associated written signature. PKI provides for a digital signature and combined with a secure hashing algorithm provides for integrity (questionable in today’s paper world) to supplement the digital future. The concept of non-repudiation, “not being able to dispute having digitally signed an electronic document and its associated integrity”, is the foundation of evolving court cases in the digital future. The levels of PKI security policy enforcement and PKI components selected will go a long way in deciding legal liability for those issuing certificates and using them. This risk is perceived unacceptable to many corporations with to potential for huge liability suits until the acceptable PKI conventions settle out or the Government steps in to limit liability (i.e. credit cards). The ROI in the Digital Signature arena is largely based on the potential for cost reduction in the elimination of paper and the conveniences to customers of automated processing and business process reengineering. Like the I&A market the initial issuance and reissuance of the certificates represents the primary cost. No key recovery is needed or encouraged for digital signatures.

PKI Distribution and Component Selection: This tutorial will attempt to provide sample customer profiles that make the selection of individual PKI components appropriate to achieve the targeted ROI for each customer. These profiles will be representative of real customers that Booz Allen & Hamilton has assisted in the struggle for achieving PKI ROI. The pursuit of maximum PKI ROI involves evaluating all areas of potential PKI use across confidentiality, I&A, and digital signature applications. PKI component factors will include certification authorities (Verisign, GTE Cybertrust, Netscape, Microsoft, Motorola CAW, Cylink, etc.), directories (X.500, LDAP), tokens (smartcards, PC/MCIA, diskettes), certificate extensions, key recovery (IBM Keyworks, Motorola CAW, Recoverkey), and standards bodies. Lessons learned in ROI are taken from Booz Allen & Hamilton intellectual capital gained from: Information Research & Engineering Network (IREN), DoD, Federal Government Agencies, commercial banks, etc.) Examples will include: confidentiality (data storage & internet transmission), I&A (X.509 extensions, decentralized & centralized access control), digital signatures (email, paperless, legal).

Managing Your ROI for PKI Security in the Digital Future

22nd NISSC Conference
October 18-21, 1999

Peter Butziger

Booz • Allen & Hamilton

410-684-6698 butziger_peter@bah.com

Solicit Management Buy-In

“**Strategic Planning Assumptions:**

”Within two years of deployment, 20 % to 30% of PKI deployments will fail because they do not demonstrate value (.09 probability)”

Source: GartnerGroup: “Justifying PKI as Protection and Opportunity,” (July 1998) - Reprinted with permission, July 1999.

Do Your Value Homework

- *Identify Potential PKI Value Candidates*
- *Evaluate Applicable Industry PKI Impacts*
- *Map Candidates to Applicable PKI Enabled Products & Services*
- *Select Required PKI Components That Provide Incremental and Strategic Alternatives*
- *Identify Adaptable, Cost Effective Value*
- *Keep Management Informed of Value*

Identify Potential PKI Value Candidates

- ***Target Valued Asset Protection & Liability Exposure***
  - Intellectual Capital (Pending Patents / Secrets)
  - Paperless Automation Requiring Digital Signatures
  - Remote Access (Intranet / Internet, Classified)
  - New Business Ventures (Electronic Commerce Market Penetration, Goodwill Exposure, BPR)
  - Regulatory Pressure for Protection of Personal Information and Intellectual Property ("due diligence")

Evaluate Applicable Industry PKI Impacts

Banking Industry Profile

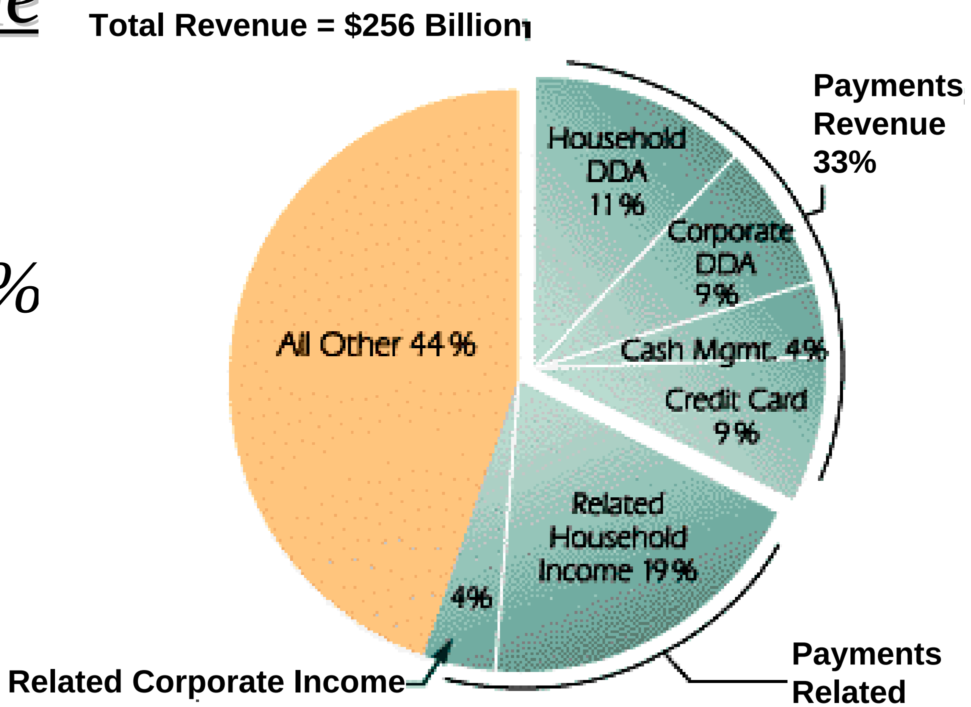
- *Security* is acknowledged by banks and customers as the biggest obstacle to Internet banking

Evaluate Applicable Industry PKI Impacts

Banking Industry Profile

- *At Risk: Bank's* payment processing *(direct & related) accounts for > 50% of revenue*
- *At Risk:* Customer ownership *and valuable* buying habits

Payments as a Percentage of Total Banking Revenue



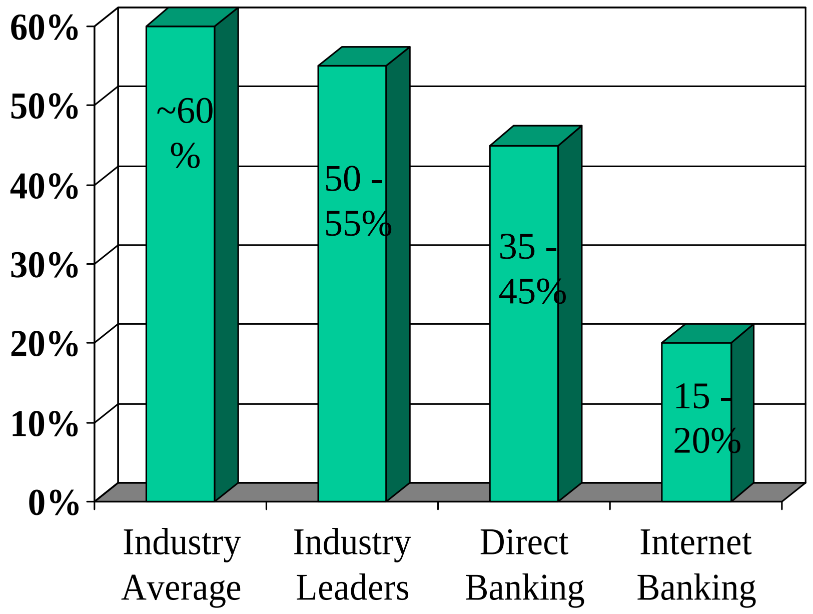
Note: Revenue includes net interest and non-Interest Income
Source: FDIC, Faulkner & Gray, BAH Analysis

Evaluate Applicable Industry PKI Impacts

Banking Industry Profile

- *Threat:* Reduction in operational cost as % of revenue from paper checks to debit cards and Internet banking

Potential For Improved Productivity Ratios
(Revenue / Operational Cost)



Source: Company Financial Reports: Industry Interviews

Evaluate Applicable Industry PKI Impacts

- ***PKI Banking Industry Value Proposition:***
  - – Pursue the piloting of PKI enabled services for candidate value areas
  - – Evaluate PKI related impacts on present corporate market offerings
  - – Utilize PKI related services to assist in future strategies and alliances to retain and grow market share

Evaluate Applicable Industry PKI Impacts

Sample Banking PKI Early Adopters

- ***Scotia Bank***
  - Using Entrust CA to issue personal banking industry certificates
  - Targeting Canada
- ***Digital Signature Trust***
  (Subsidiary of Zions First National Bank)
  - Using CertCo CA to provide outsourcing of certificates to Utah
  - Targeting U.S., Teamed with ABA for EC & web site authentication
- ***Identrus LLC***

  (Consortium of:Bank of America, Chase Manhattan, Citigroup, Deutsche Bank,Sanwa Bank, & 5 other international banks)
  - Pilot program testing cross certification between CA vendors
  - Targeting identification of parties involved in electronic transactions

Map PKI Value Candidates to PKI Enabled Products & Services

- *Data Storage Confidentiality: Data Encryption & Key Recovery*
- *Transmission Privacy: Secure Sockets Layer, Virtual Private Networks*
- *Correspondence Integrity & Non Repudiation: Digital Signature (E-Mail, Code, Contracts)*
- *Identification & Authentication: Access Control, Single Sign-On, Mutual Authentication*

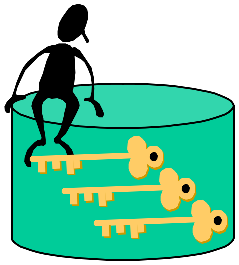
Data Storage Confidentiality

Sender

Encrypt Symmetric Key

Receiver

Decrypt Symmetric Key



- *Confidentiality* (Encryption of Data on Systems)
  - – Symmetric keys are usually used for encryption for performance while the asymmetric public key is used to encrypt the symmetric key for the recipient.
  - – Traditional confidentiality products include desktop or laptop encryption products
  - – Key Recovery (Third party or CA provided)
    - Prevent accidental or malicious data destruction
    - U.S. export limitations

Transmission Privacy

- ***Transmission Privacy:*** (Protection of information in transit using encryption)
  - Encryption is used like confidentiality which passes a symmetric key for performance of privacy.
  - Key escrow is not required for transmission privacy since the data is decrypted upon receipt. An unsuccessful attempt will result in retransmission.
  - Secure Sockets Layer (SSL) is a predominant approach to web enabled browsers and provides a one time symmetric session key which is wrapped in the intended recipients public key
  - Virtual Private Networks are a popular way to leverage the Internet or Intranet for privacy using encryption.

Sender

Encrypt
Symmetric
Key

Receiver

Decrypt
Symmetric
Key

Correspondence Integrity

Sender

#%& Securely Hash Data

Digitally Sign

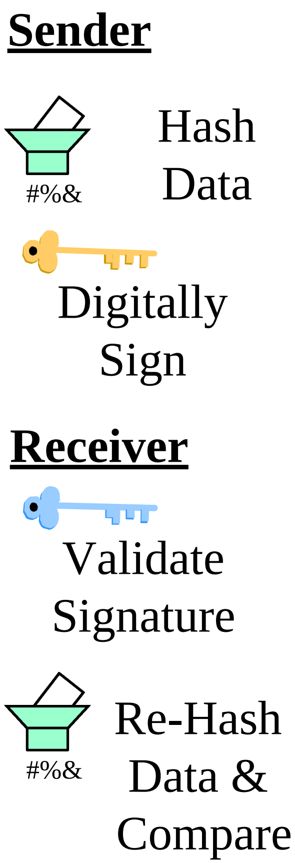
Receiver

Validate Signature

#%& Re-Hash Data & Compare

- *Correspondence Integrity* (Confidence that data digitally signed by an initiator has not changed since its last signing.)
  - To validate the signature: check certificate validity date, chain, certificate revocation list, and provide human to validate trust of common name
  - Secure E-Mail provides PKI Enabled Products and requires human decision for trust to occur
  - Signing of code has become popular with vendors in an effort to reduce liabilities for malicious code and instill customer trust (i.e. Microsoft using VeriSign to sign code)
  - Legal State and National laws are being defined and accepted to allow for Digital Signatures to support contractual agreements

Identification & Authentication



Sender

#%& Hash Data

Digitally Sign

Receiver

Validate Signature

#%& Re-Hash Data & Compare

- *I&A* (Digital Signature replacement of traditional IDs: Driver’s License, SS Card, Passport, Green Card, Password, Written Signature)
  - Like Correspondence Integrity, the individual must digitally sign something that the other party can validate
  - Single Sign-On extends access control to many applications without re-validating identity
  - Provides Mutual Authentication by each party digitally signing something that each party can validate. Either previous validated access list or human party validation is required.

Identification & Authentication

User

Digitally Sign

System

Validate Signature

Compare to List or Use Label

Archive Protection

- ***I&A Access Control*** (Based on PKI Certificate Identity and Either Control List or Certificate Extension)
  - Can Utilize Digital Signature and Validation for Identity and an Access List for Access Confirmation
  - Can Utilize Label Based Access Control to Confirm Access to Multiple Data Sources
  - Can Utilize Centralized Directory of Authorities
- ***Non Repudiation*** (Undeniable Proof of Originating Sender Digitally Signing Data / Document and Demonstrated Protection of Signing Private Key. Legal Judgments on PKI Liability are still Pending.)

Select Required PKI Components

- ***Provide Incremental & Strategic Alternatives***
  - Product Development, Application Integration or Selection of Enabled Products (Vendor / Consumer)
  - Certificate Acquisition:
    - Outsourcing Versus Self Issuance
    - Timeframe Versus Volume
  - Standards Compliance & Interoperability:
    - Commercial, Government, International
    - Certificates, Algorithms, Tokens, Internet, Applications
  - Vendor Alliances and Market Share

CA Binding

Certificate Authority Component

- ***A Certificate Authority*** provides trusted binding of an identity to an individual by securely signing an X.509 certificate with a protected CA private signing key.
- ***Vendor discriminating characteristics include:***
  - Outsourcing Versus Self Operated
  - Protection of the CA Signing Keys
  - Cryptographic Algorithm Support
  - Human Involvement in Issuance (LRA)
  - Generation and Storage of Privacy Keys (Tokens)
  - Internal Versus Third Party Key Recovery
  - Audit and Archive Capabilities

CA Marketplace

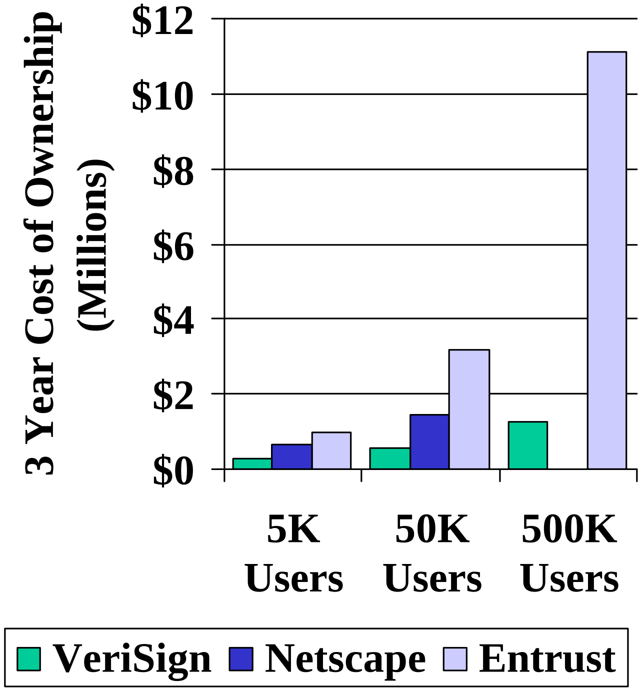
"Certificate authority products and services market participation will grow through 1999 before consolidation occurs (0.8 probability)."

Source: GartnerGroup: "Certificate Authority Magic Quadrant," (May 1998) - Reprinted with permission, July 1999.

CA Sample Cost of Certificate Issuance

- ***Major Differences for 500K Users:***
  - Netscape not available 500K capacity
  - Entrust software license and staffing represent the main delta in cost (does not represent web enabled CA product)

Cost of Ownership for Digital Certificate Projects



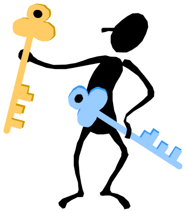
Source: Aberdeen Group, “Evaluating the Cost of Ownership for Digital Certificate Projects” July 1998 - Reprinted with permission, July 1999.

Sample Government Pilots

- **VeriSign**: DoD National Guard, IRS
- **Cybertrust**: DISA ADNET, Intelink
- **Motorola CAW**: MISSI DMS, NSANET
- **Netscape**: DoD PKI Medium Assurance Working Group
- **Entrust**: Canadian Government
- **Cylink**: Secure Postal Payment Process
- **CertCo**: Utah State

Sample Commercial Pilots

- **VeriSign**: Texas Instruments, Microsoft, Kodak, VISA, IREN
- **Cybertrust**: MasterCard, American Express, Wells Fargo Bank
- **Entrust**: Federal Express, Scotia Bank, Columbia/HCA Healthcare Corporation
- **Netscape**: Cisco, Ford Motor Co.
- **Xcert**: ABA Electronic Commerce



PKI Algorithm Component

Symmetric Keys

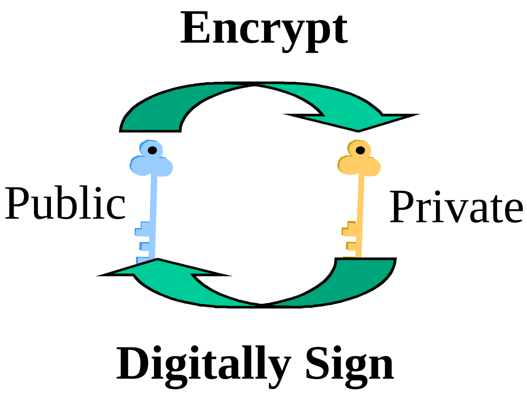
Private
Private

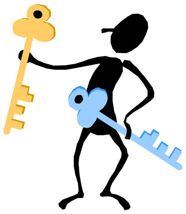
- *Symmetric Keys* historically used for Confidentiality (Encryption)

Asymmetric Keys

Public
Private

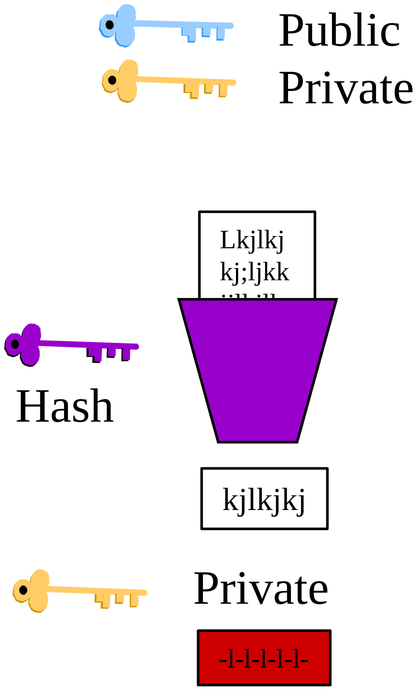
- *Asymmetric Keys* used for Digital Signatures and Encryption
  - Mathematically will NOT determine Private by Exposing Public (keep protected)
  - Inverse use of keys for Encryption and Digital Signature (Requires Both Keys Uniquely)





PKI Algorithm Component

Asymmetric Keys



Public

Private

Lkjlkj
kj;ljkk

Hash

kjlkjkj

Private

-l-l-l-l-l-

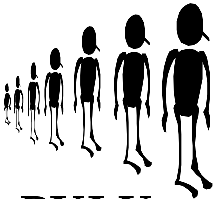
Digital Signature

- *Asymmetric Key Algorithms*:
  - – RSA (Commercial Leader, Patent Expires This Year)
  - – Diffe Hellman (Commercial)
- *Message Digest Algorithms*:
  - – MDA-5 (Commercial)
  - – SHA-1 (FIPS / Commercial)

Token Components

- ***Tokens:*** *Provide protection of privacy keys.*
  - Root Signing Keys tend to be generated on the token and protected by tamper resistance features and surroundings
  - Personal Identity Keys tend to be generated by a browser then stored either: on computer, PC Diskette, or Smartcard (used for approval by LRA).
  - Use of a privacy key requires possession of the token and / or encrypted privacy key and the password to unencrypt it for use.

PKI X.509 Certificate Issuance Component



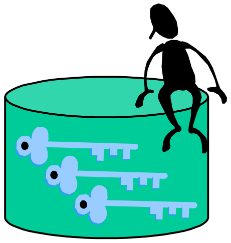
PKI Users

- *PKI Users* provide Identification Sources to receive a Certificate.

- *X.509 v3 Certificate* is used for Digital Signature Certs and Encryption Certs.

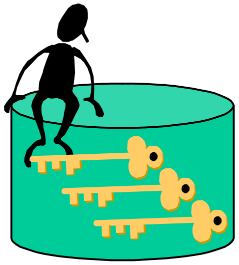
RA

- *Trusted Local Registration Authority* validates PKI User Identity, requests certificate, and Issues Certificate.



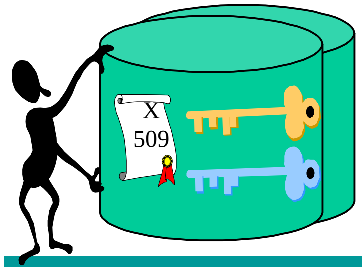
PKI Directory Component

- Public keys are posted to a ***Directory*** and protected for Issuance & Revocation
  - **X.500**: ISO/ITU Standard
    - Limited PKI Pilots: Defense Messaging System (DMS), Government Services Agency (GSA) Directory Services
  - **LDAP**: IETF Standard
    - Commercial Adoption (Predominant Presence)



PKI Key Recovery Component

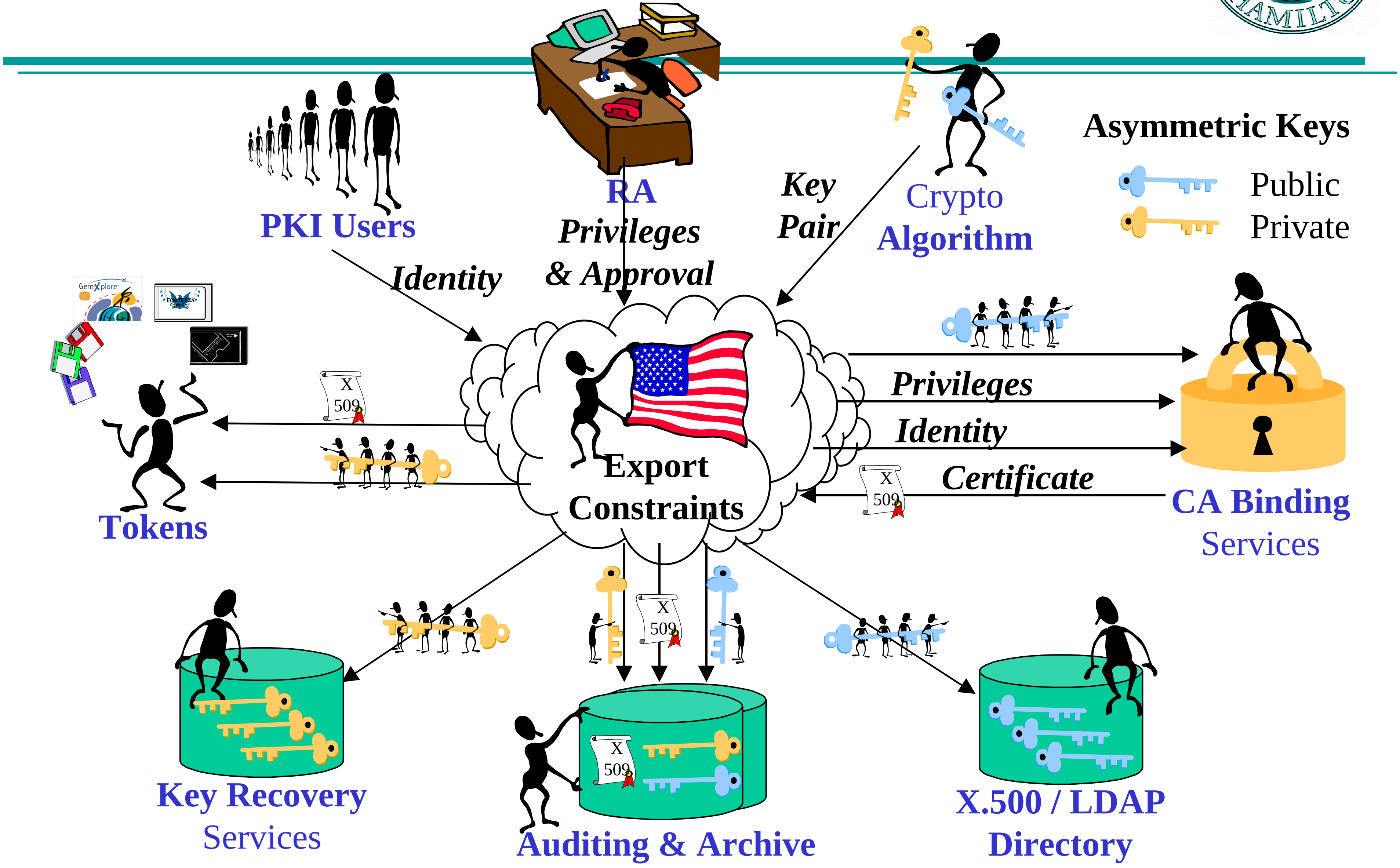
- ***Key Recovery*** is essential to protect stored, encrypted data from potential loss of the private key.
- ***Samples***
  - **TIS RecoverKey:** Trusted Third Party
  - **IBM Keyworks**: Trusted Third Party
  - **Motorola CAW:** Built into CA



PKI Audit & Archive Component

- ***Audit & Archive*** provides undeniable proof of certificate & key issuance
- Valuable data in conjunction with policies and procedures as legal liabilities are determined.
- Part of CA Services (Outsourced or Self Issued)

PKI Components Integration



PKI Users

Identity

RA

Privileges

& Approval

Key

Pair

Crypto

Algorithm

Asymmetric Keys

Public

Private

Tokens

Export

Constraints

Privileges

Identity

Certificate

CA Binding

Services

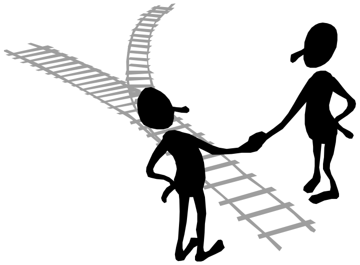
Key Recovery

Services

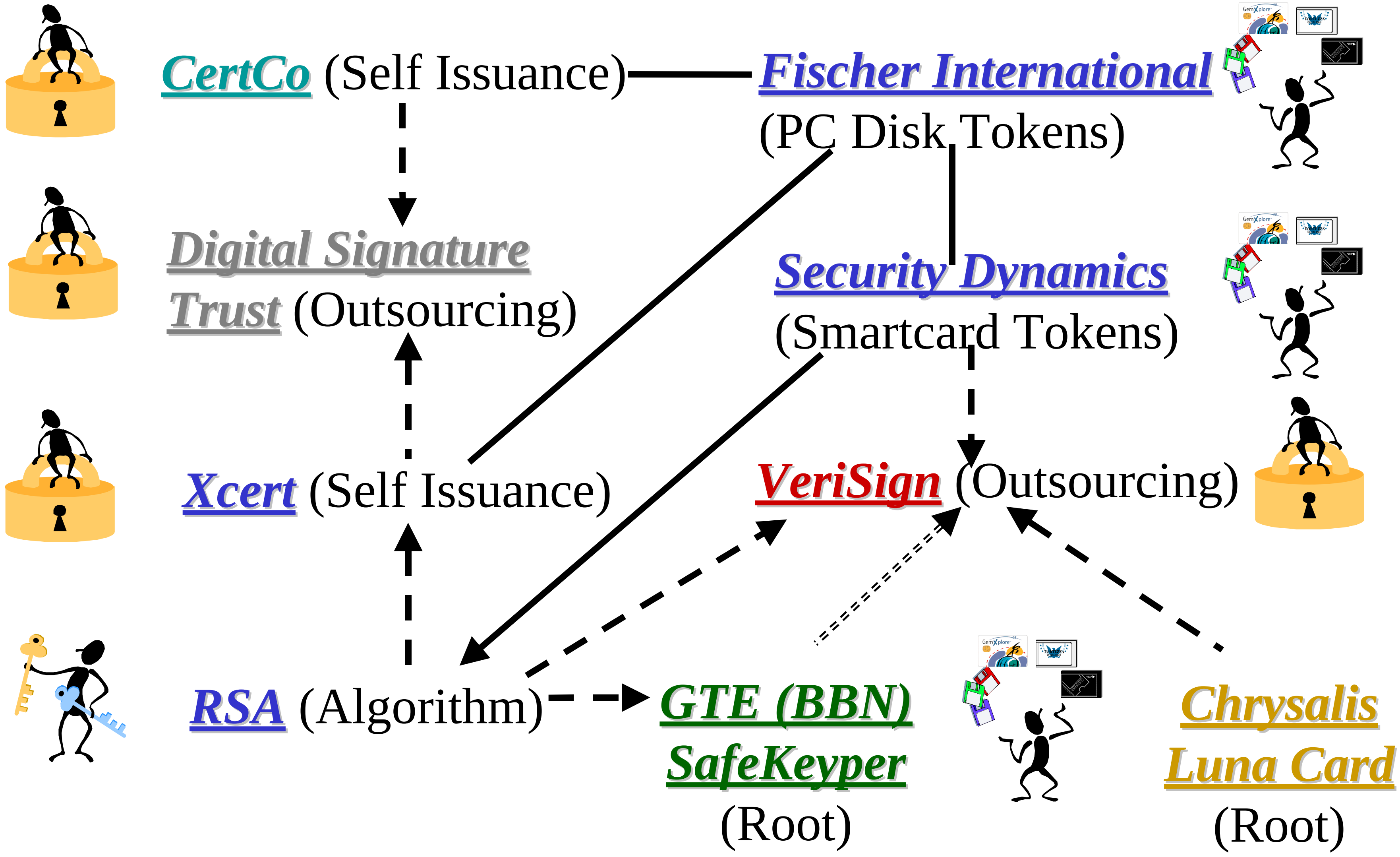
Auditing & Archive

X.500 / LDAP

Directory



Sample PKI Vendor Alliances



CertCo (Self Issuance)

Fischer International (PC Disk Tokens)

Digital Signature Trust (Outsourcing)

Security Dynamics (Smartcard Tokens)

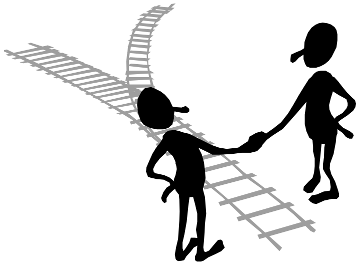
Xcert (Self Issuance)

VeriSign (Outsourcing)

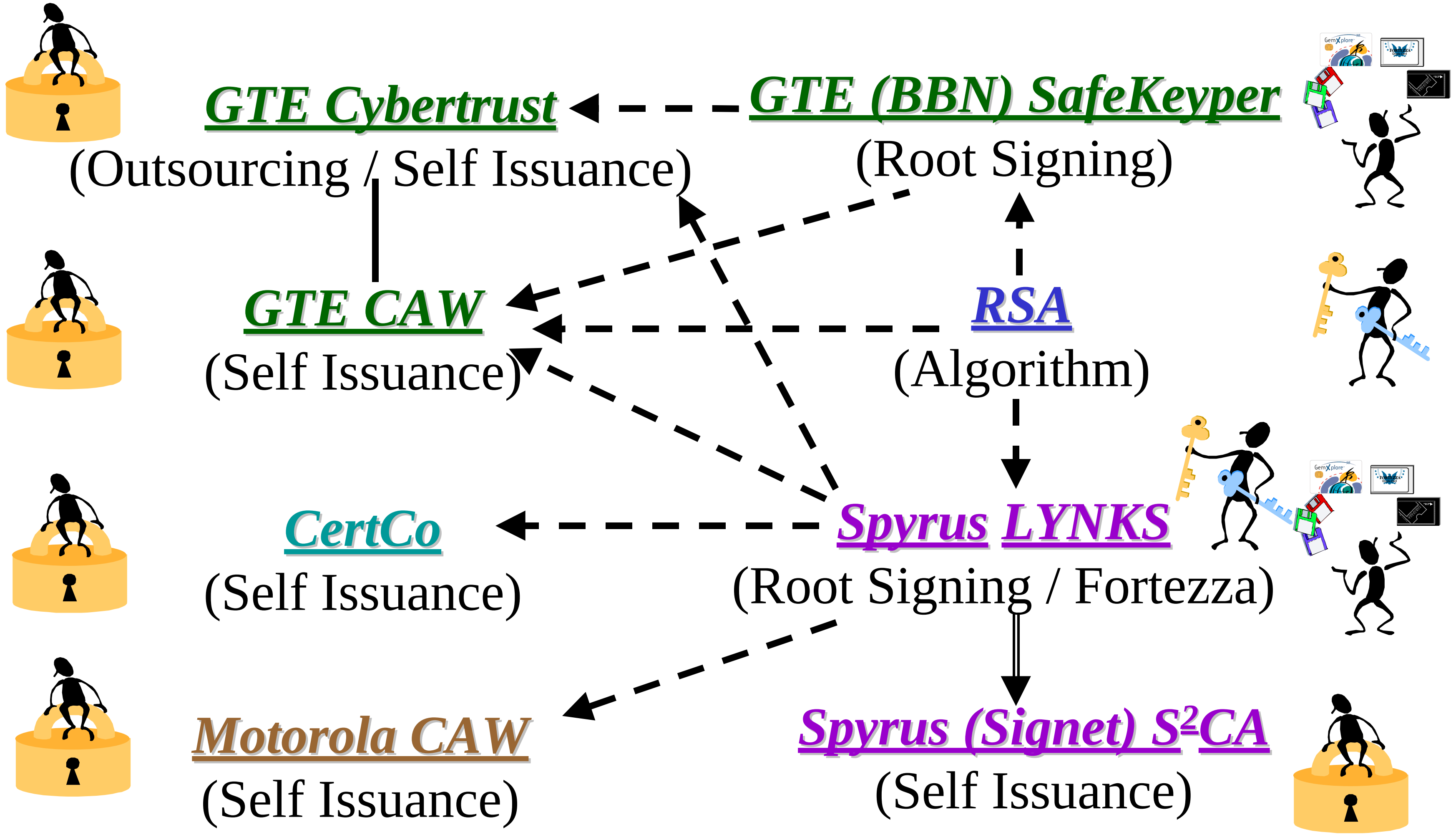
RSA (Algorithm)

GTE (BBN) SafeKeyper (Root)

Chrysalis Luna Card (Root)



Sample PKI Vendor Alliances



GTE Cybertrust
(Outsourcing / Self Issuance)

GTE (BBN) SafeKeyper
(Root Signing)

GTE CAW
(Self Issuance)

RSA
(Algorithm)

CertCo
(Self Issuance)

Spyrus LYNKS
(Root Signing / Fortezza)

Motorola CAW
(Self Issuance)

Spyrus (Signet) S²CA
(Self Issuance)

PKI Standards Influence

- ***Standards Direction***
  - X9F Subcommittee Developing Information Security Standards for the U.S. Financial Community
  - U.S. Delegation to ISO SC2/TC68/WG8
  - Internet Engineering Task Force (IETF) affecting change in PKIX Part 1
  - DoD X.509 Certificate Definition (Profile)
  - ISO Standard on Certificate Management
  - NSA Message Security Protocol (MSP) and Common Security Protocol Standards (CSP) through ISSE
  - Industry Standard Certificate Policy and Certificate Practice Statement Framework

PKI Policy Groups

- *On-Going PKI Activities*
  - Federal PKI Working Group
  - DoD PKI Working Group
  - GSA ACES Government Contract Procurement
  - MISSI Key Privilege & Certificate Management Working Group
  - Standards Activities Database for Relative Technologies for NSA
  - IATAC Serves as an Authoritative Source for Information Assurance Vulnerability Data, Methodologies, Models, and Analyses of Emerging Technologies

PKI Selection Criteria

- Vendor Market Share
- Corporate Acquisition & Mergers
- Security Risk Assessments
- Penetration Analysis & Intrusion Detection
- Interoperability
- Standards Direction & Vendor Compliance
- Outsource / Insource
- Policy Definition
- Token Tradeoffs
- CA Tradeoffs
- Algorithm Tradeoffs
- Key Recovery Tradeoffs
- Audit & Archive Tradeoffs
- Directory Tradeoffs

Plan for Realistic Cost Recovery Strategy

- Volume May Achieve Discounts
- Include Sufficient Staffing
- Single Identity Certificate Issuance
- Account for Certificate Renewal Costs
- Account for Audit & Archive Services
- Consider PKI Enabling Services (Application Toolkits, Vendor Volume Disc.)
- Track Value Delivered

PKI ROI Checklist

✓ *Solicit Management Buy-in*

✓ *Evaluate Industry PKI Impacts*

✓ *Evaluate Assets @ Risk*

✓ *Determine Scope of PKI applicability*

✓ *Determine Applicable PKI Components*

✓ *Evaluate PKI Vendor Alliances*

✓ *Plan for Realistic Cost Recovery Strategy*

✓ *Define & Enforce Applicable Policies*

PKI ROI Decision Point

“Enterprises without an urgent or a compelling business requirement to implement a PKI will gain from further pricing competition and greater market clarity during the next 24 months (.09 probability).”

Source: GartnerGroup: “Pricing Public Key Infrastructures,” (September 1998) - Reprinted with permission, July 1999.