




**HSPD-12 Tutorial**

Doug Simmons  
Principal Consultant  
[dsimmons@burtongroup.com](mailto:dsimmons@burtongroup.com)  
[www.burtongroup.com](http://www.burtongroup.com)

Date

All Contents © 2007 Burton Group. All rights reserved.

---

---

---


---

---

---

---

---



**HSPD-12 Tutorial** 2

**Speaker background**

- Doug Simmons – Principal Consultant in Directory and Security Strategies Service
  - Identity Management Consultant for over 15 years
  - X.500 developer (IBM), co-chair 1999 PKI Interoperability Challenge
  - Multiple PKI deployments

---

---

---


---

---

---

---

---



**HSPD-12 Tutorial** 3

**What you will learn**

- Overview of HSPD-12
  - What it is
  - History of the directive
  - What it is intended to address, drives behind the directive
  - What is out of scope
  - Timeline for deployment

---

---

---

---


---

---

---

---

**HSPD-12 Tutorial** 4



**What you will learn**

- Components of an HSPD-12 compliant infrastructure
  - Card Management Systems
  - Card printers
  - Card readers
  - User administration systems
  - Identity management infrastructure
- Federation across the government
  - Federal Bridge CA
  - Status
  - Federal Government e-Authentication strategy
  - Status

---

---

---

---


---

---

---

---

**HSPD-12 Tutorial** 5



**What you will learn (continued)**

- Business processes to support registration, management and revocation
  - Creating, managing and revoking cards
  - Lifecycle management
  - Identity vetting
  - PIV I and PIV II
    - Description
    - Current status

---

---

---

---


---

---

---

---

**HSPD-12 Tutorial** 6



**What you will learn (continued)**

- Where to begin
  - Assess your situation
    - What are your specific requirements and when are they due to be met?
    - What logical and physical environments must be addressed by HSPD-12?
    - Are stakeholders identified?
  - Current identity management infrastructure
    - Current state of provisioning and user lifecycle management
    - Status of PKI in your organization
  - Certificate authorities
  - Registration authorities

---

---

---

---


---

---

---

---

**HSPD-12 Tutorial**



What you will learn (continued)

- Current state of authentication environments
- Current relationships with parties external to your organization
- Possible phasing scenarios
  - Physical first
  - Logical first
  - Other possibilities?
- Getting your identity management house in order
- Best practices
- Summary and conclusions
- Q&A

---

---

---

---


---

---

---

---

**Smart Cards: Scaling to the Enterprise**



Agenda

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- Physical & Logical Components
- Standards
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---


---

---

---

---

**Smart Cards: Scaling to the Enterprise**



Agenda

- ***Introduction & Strategic Context***
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- Physical & Logical Components
- Standards
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---


---

---

---

---

**Introduction & Strategic Context** 10



**Why we're here**

- Challenged to provide stronger forms of authentication than traditional passwords and PIN in light of real and perceived security threats to information assets
- Advancements in IdM solutions enable multiple means of authentication based on resource sensitivity
- Enterprise directories are becoming common place – now want to leverage them for stronger security services
- Smart cards have been gaining attention for past decade
- Evolution of hardware devices has improved and cost of devices has decreased dramatically

---

---

---

---


---

---

---

---

**Introduction & Strategic Context** 11



**Key business drivers**

- Traditional passwords cannot adequately protect the high-value applications and information resources on today's networks
- Many networks are prime targets for attackers:
  - Sharing passwords
  - 'Shoulder surfing'/post-its
  - Network sniffing
  - Brute force attacks
  - Guessing
  - Other forms of attack

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 12



**Key business drivers (continued)**

- Simplified access to IT services increasing employee productivity and experience
- Reduced complexity of IT service access (fewer authentications to applications)
  - Single Sign On (SSO), Simplified Sign On, Reduced Sign On...
- Reduced application development time
- Reduced help desk costs for password reset
- Global physical access to facilities based on centralized policy
  - Building access, not just system access

---

---

---

---


---

---

---

---

**Introduction & Strategic Context** 13



**Key business drivers (continued)**

- Motivated by a heightened acknowledgement of risk
  - Regulation, audit, and potential costs of authentication failure
  - Increased accountability
  - Real time audit tracking
  - Post incident forensics
- Heightened awareness of risk demonstrates that authentication is an extremely important link in the enterprise's overall security posture

---

---

---

---

---

---


---

---

---

---

**Introduction & Strategic Context** 14



**Key business drivers (continued)**

- Compliance
  - HIPAA (Health Information Portability & Accountability Act) – patient record confidentiality
  - Sarbanes-Oxley – improved audit controls, protect investors
  - Gramm-Leach-Bliley Act (GLBA) – audit access to sensitive information, particularly customer information
  - FDA 21 CFR Part 11 – research, application integrity, audit, e-signatures
  - California SB 1386 – protect personal data, notification of breach
  - E-Sign Bill – legalizes e-signatures in government transactions
- Government and peer activity
  - DoD Common Access Card (CAC)
  - NIST Smart Card Interoperability Specification & rollout

---

---

---

---

---

---


---

---

---

---

**Introduction & Strategic Context** 15



**Key business drivers (continued)**

- According to the Burton Group 2003 Survey: Smart Card Deployment Survey & Best Practices
  - Most common usage is currently with secure network and VPN access
  - Other main priorities of usage varied across:
    - Single Sign-On
    - Badging and facilities access
    - Administrative access to secure applications and systems

---

---

---

---

---

---

---

---

---

---

### Introduction & Strategic Context

**Strong authentication: balance of user & infrastructure considerations**

- Scope of deployment must be well-defined
- Consider the state of the enterprise IdM infrastructure
- Factor the acceptability of certain types of authenticators
- Determine whether existing applications are supportable
- Identify business processes and policies to ensure that security gaps do not invalidate strong authenticators
- May require new relationships with HR and Facilities to create the most effective program
- Are you ready for some PKI?!

---

---

---

---

---

---

---

---

### Introduction & Strategic Context

**IdM: A set of complementary, converging technologies**

- User identity management services
- Directory services
- Provisioning services
- Authentication services
- Web-based access management services
- Authorization services

---

---

---

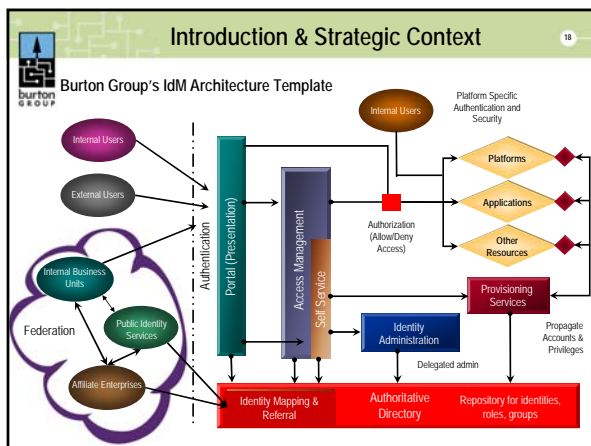
---

---

---

---

---




---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 19

**Good news!**

- Large enterprises are showing increased interest
  - Supporting IdM system deployments beginning to proliferate
  - Corporate ID cards
  - Campus systems
  - Government, Higher Education segments jumping on
- Financial market usage grew rapidly over the past 4 years – fastest growing segment

*So there \*IS\* some positive momentum*

---

---

---

---

---

---

---

---

**Smart Cards: Scaling to the Enterprise** 20

**Agenda**

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- Physical & Logical Components
- Standards
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 21

**Role of public key infrastructure (PKI)**

- Smart cards enable 'strong authentication'
- Strong authentication = multi-factor authentication
  - Something you know
  - Something you are
  - Something you have
  - Something you do (behaviors)
- Two or more of these factors provides strong authentication
- PKI-based cryptography is commonly used

---

---

---

---

---

---

---

---

## Slide 21

---

**DS1** maybe this slide can be deleted or combined with the later one that identifies strong authentication  
Doug Simmons, 5/7/2004

**Introduction & Strategic Context** 22

**Role of PKI (continued)**

- PKI is intended to enable scalable key exchange across distributed environments supporting:
  - Identity – digital signature and non-repudiation
  - Privacy – data encryption
  - Data integrity – tamper-proof ‘hash’
  - Access control based on irrefutable identity
- PKI is the set of services that allows corporations to deploy and use public key cryptography, including digital certificates
- Certificates bind a public key to an “owner”
  - Used to establish identity (a person, a company, an application)
  - Signed by a trusted party (chains of trust)

---

---

---

---

---

---


---

---

**Introduction & Strategic Context** 23

**PKI also enables other important enterprise security functions**

- Virtual private networks
  - Big savings over private networks, long-distance dialup
- Secure Web applications access
  - Enable B2B relationships; protect consumer privacy
- Secure e-mail
- Digital signatures
- Wireless/mobile identification
- Code signing
- Desktop file and folder encryption




---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 24

**Elements of a PKI**

- Key Management Software and Hardware
- Digital Certificates
- Certification Authorities (CAs)
- Certificate Repositories
- Registration Authorities (RAs)
- Digital Signatures
- Validation
- Revocation
- Trust Models
- Certificate Policies

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 25

**Key management**

- Keys exist in pairs – public key and private key
- Generation of key pairs can occur as follows
  - In client software (browser or PKI client)
  - In tamper resistant hardware (e.g., smart card)
  - By the Certificate Authority
- Keys may be stored locally in the PC (PKI client or browser file) or
  - On the tamper resistant tokens (USB or smart card)
  - On the network in a roaming PKI server
- Public key(s) generally made available via digital certificates

---

---

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 26

**Key management (continued)**

- Various cryptographic algorithms
  - Asymmetric: RSA, Elliptic Curve
  - Symmetric: DES, 3DES, DSA, RC4
  - Hashing: SHA-1, MD5
- Various key lengths for CA, RA and end users
  - Range from 256 to 4096 bits
  - Longer keys require more processing power
- Restrictions on both may be based on local regulatory or legal considerations
  - International boundaries with different limitations can make it difficult to map certificates and cross certify

---

---

---

---

---

---

---

---


---

---

**Introduction & Strategic Context** 27

**Digital certificates**

- Electronic files that contain information about the holder of the certificate
- Defined in International Telecommunications Union (ITU) X.509v3 specification
- Personal information, such as the name, address, and public key of the certificate holder
- Information about the issuing Certificate Authority
- Administrative items like the type of certificate and certificate expiration date




---

---

---

---

---

---

---

---

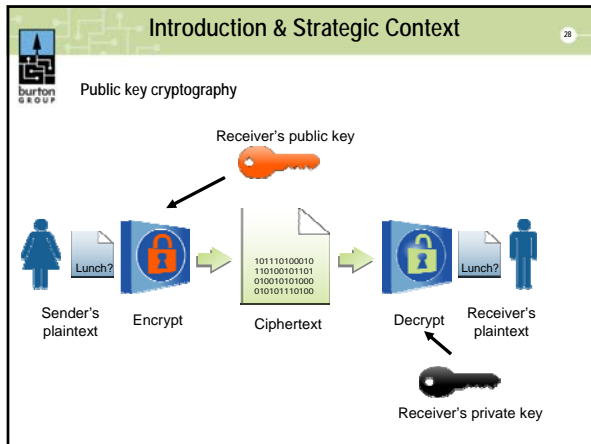
---

---

## Slide 26

---

**DS2** Out - maybe go out to Trent's or reference in recommendations  
Doug Simmons, 5/7/2004




---

---

---

---

---

---

---

---

---

---

- ### Introduction & Strategic Context
- #### Certificate Authorities
- Serves as the issuer and guarantor of digital certificates
  - Trusted Third Party
  - Generate Root Keys that are used to digitally sign all subordinate certificates, including user certificates
  - CAs maintain two important repositories
    - Private database for backup of current keys and archive of out-of-date keys, operating under CA security provisions
    - Easily accessible directory to store and distribute certificates, Certificate Revocation Lists (CRLs) and to store CA information
  - Integrated or federated Directories enhance scalability

---

---

---

---

---

---

---

---

---

---

- ### Introduction & Strategic Context
- #### PKI repositories
- Often stores certificates in a standard attribute called userCertificate, within each end user's directory entry
  - Certificates are 'publicly available' so as to make the user's public keys accessible for signature verification or data encryption
  - Typical directory requirements
    - LDAP compliance, replication, extensible schema
    - X.500 naming model, high search performance
    - Active Directory for MS PKI certificate storage
  - But the PKI/Directory relationship is much deeper
    - Affects naming of certificates, user management process ...

---

---

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 31

**Digital signatures**

- Signer's private key and the message data (e.g., bind request for strong authentication) combined to calculate unique signature value
- Function of cryptographic hardware (e.g., smart card)

```

    graph TD
      PK[Signer's Private Key] --> CS[Digital Signature Calculated]
      DM[Digital Message] --> CS
      CS --> SMS[Signed Message Sent]
  
```

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 32

**Verifying digital signatures**

- Opposite process
- Obtain signer's public key from signer's certificate
- The challenge is whether you trust the signer's certificate or not

```

    graph TD
      SMR[Signed Message Received] --> DSV[Digital Signature Verified]
      SPK[Signer's Public Key] --> DSV
      DSV --> MA[Message Accepted]
  
```

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 33

**Certificate validation**

- Certificates must be validated to be trusted
- Certificate Revocation
  - Certificates must be revoked when invalidated
  - Misuse or compromise of certificate/device
- Certificate Revocation Lists (CRL)
  - CRL distributed to participating systems, directories
  - Lists invalid certificate serial numbers
  - CRLs can grow quite large – delta CRLs
- Online Certificate Status Checking Protocol (OCSP) responders
- Signature validation process requires 'real-time' check of certificate with CRLs or OCSP service

---

---

---

---

---


---

---

---

DS3

**Introduction & Strategic Context** 34



**Scaling: It's all about trust**

- In a single security domain (intranet) it isn't too difficult
  - Usually one CA
- In a large, distributed organization, or across multiple domains, CA trust must be established
  - Certificate chain (hierarchy)
  - Cross-certification
  - Bridge CA

---

---

---

---


---

---

---


---

**Introduction & Strategic Context** 35



**PKI: Other Important Considerations**

- Certificate Policy (CP): Defines PKI rules for applications, an enterprise, or community. It governs the levels of:
  - Assurance
  - Identification and authentication
  - Liability limits
  - Security controls
  - Records management
  - Audits
- Certificate Practice Statement (CPS)
  - Document detailing of the operational procedures, standards and practices used by a CA in carrying out its functions under the CP.
- Different levels of assurance require different CPS', or Certificate Policies




---

---

---

---


---

---

---


---

**Introduction & Strategic Context** 36



**Looking forward: Federated identity and authentication**

- Enable successful authentication in partner's domain to be acceptable in your domain
- Security Assertions Markup Language (SAML) 1.1
- Liberty Alliance
  - Initiated by Sun, over 130 partners
  - Federation policy framework built around SAML
- WS-\*
  - IBM, Microsoft, Verisign
  - Competes with Liberty




---

---

---

---

---

---

---

---

## Slide 34


---

**DS3** address the 3 models in this slide  
Doug Simmons, 5/7/2004

**Introduction & Strategic Context** 37

**Looking forward: Federated identity and authentication**

- Requires trust model analogous to PKI inter-CA trusts
- Requires digital signing of identity assertions as they traverse domains
- Requires data classification policy within the Enterprise to incorporate externally-authenticated parties




---

---

---

---

---

---

---

---

**Smart Cards: Scaling to the Enterprise** 38

**Agenda**

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
    - Alternative Approaches
- Physical & Logical Components
- Standards
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---

---

---


---

---

**Introduction & Strategic Context** 39

**Smart card concepts**

- Strong authentication = two factor authentication
  - Something you have, something you know
- Something you have:
  - Credit card-like device, card reader attached to workstation
- Something you know:
  - Accessing/unlocking device requires password or PIN




---

---

---

---


---

---

---

---

**Introduction & Strategic Context** 40



Smart card concepts (continued)

- Private keys stored on device
- Microprocessor performs digital signing operations
- Evolving from simple stored value cards with crypto functions
- Increased memory for application support
- Example: Java card

---

---

---

---


---

---

---

---

**Introduction & Strategic Context** 41



Example: DoD Common Access Card

- Supports demographic information related to benefits, personnel status, DOD issued unique personnel IDs, and other profile and credential information
- Three initial Java applets on CAC:
  - Card profile
  - Demographic data
  - PKI applets
- Other departmental applets may be provisioned to the card after the initial deployment

---

---

---

---


---

---

---

---

**Introduction & Strategic Context** 42



Example: Bankcard systems

- Chip on credit card used to authenticate transactions
- Chip not often used
- Uptake slow
- Requires interoperable cards and card readers (terminals)
- Europe leading this market, currently

---

---

---

---

---

---

---

---

### Introduction & Strategic Context

**Platform interfaces, toolkits**

- Java Authentication and Authorization Services (JAAS)
  - Multi-platform support
- Microsoft CryptoAPI, Graphical Identification and Authentication (GINA), Security Support Provider Interface (SSPI)
- Novell Modular Authentication Services (NMAS)

---

---

---

---

---

---

---

---

### Introduction & Strategic Context

**Microsoft example**  
Supports smart card authentication in XP and Windows Server 2004

---

---

---

---

---

---

---

---

### Smart Cards: Scaling to the Enterprise

**Agenda**

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- Physical & Logical Components
- Standards
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 46

**Alternative methods of authentication**

- Identification and authentication methods/credential types
  - Passwords, PINs
  - Kerberos
  - Embedded PKI
  - Roaming PKI
  - Hardware tokens
  - Biometrics

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 47

**Alternative approaches: Passwords and PINs**

- By far the most popular authentication technique, improved via:
  - SSL/TLS network encryption
    - No passwords sent in the 'clear'!
  - Passwords stored as hashed values
  - SSH protocol

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 48

**Alternative approaches: Passwords and PINs continued**

- Password policies are crucial
  - Aging
  - Complexity
- Single Sign-On (SSO)
  - However, a single password becomes the 'key to the kingdom' – risk aggregation
  - Smart cards may mitigate this risk

---

---

---

---

---

---


---

---

**Introduction & Strategic Context** 49

**Alternative approaches: Credential Management Systems**

- Multiple encrypted passwords stored on a device with embedded chip
- Device (card) is PIN protected
- No PKI or end-to-end cryptography required
- Sometimes referred to as credential caches or password wallets




---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 50

**Alternative approaches: Kerberos**

- Once fading, resurrected by Microsoft Windows 200x
  - Not easily interoperable with UNIX-based MIT kerberos, but getting better (e.g., more tools)
- User executes kinit to start Kerberos authentication command
- kinit sends request to Kerberos Server/Key Distribution Center (KDC)
  - Server provides 'ticket-granting-ticket' and a ticket session key back to kinit, encrypted with user's password value
  - User's password used to decrypt ticket and session key
- Password is NOT sent over network
- Enterprises beginning to leverage Windows log-on for multi-application SSO beyond Microsoft applications

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 51

**Alternative approaches: Embedded PKI**

- Examples: Lotus and Microsoft
  - Lotus Notes ID file
    - Physical ID file on workstation or removable device
    - ID file is accessible via password
  - Supports web browsers for 'roaming'
    - Notes ID file on Notes server
    - Notes performs strong authentication, digital signatures and optional message encryption
      - Great for an all-Notes environment
  - Microsoft S/MIME support in Outlook
  - SSL support in IE browser
  - XP and Windows 2003 Server

---

---

---

---

---

---

---

---

**Introduction & Strategic Context** 52

**Alternative approaches: Roaming PKI**

- Users access their private signature and decryption keys stored on network servers
  - Access is via password
- Keys are downloaded for use during session
- Roaming PKI is not a standards-based feature
  - Vendors implement differently (e.g., Lotus)
- Keep in mind that implementing a roaming solution can reduce the security level of the PKI system

---

---

---

---

---

---


---

---

**Introduction & Strategic Context** 53

**Alternative approaches: One Time Password tokens**

- Supports One Time Password (OTP) model
- Random passwords synchronized between user's token and the authentication system
  - Prevents password replay
- Zero foot print appeal
- Started as purely tactical in deployment, has enjoyed broader success in recent years, though not ubiquitous
- Market led by RSA SecurID
  - ACE Authentication Server, SecurID token fob
- Cell phones and PDAs can support OTP
  - SMS wireless network coverage issues
  - Device ownership issues (User's or company's? Does everyone have either?)




---

---

---

---

---

---


---

---

**Introduction & Strategic Context** 54

**Alternative approaches: Challenge-Response tokens**

- Authentication system offers a 'challenge' to user when connecting to system
- User enters the challenge into the token's keypad
- Token provides a response synchronized with the authentication system
- User enters response into authentication system log in screen




---

---

---

---

---

---

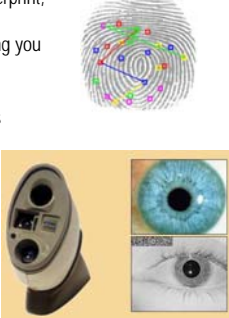
---

---

### Introduction & Strategic Context

Alternative approaches: Biometrics

- Mathematical representation of fingerprint, retina, facial structure
  - Something you **are**, not something you 'know'
- Capable of being spoofed
  - Gummy fingers – perfect replicas
  - Please don't rip my eyeball out!
- Some user misgivings
  - Biological databanks
- Perhaps best near-term use is to unlock/access smart card
  - Enables 3-factor authN




---

---

---

---

---

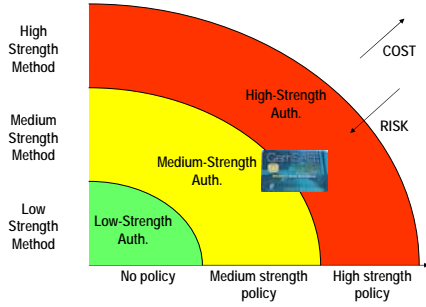
---

---

---

### Introduction & Strategic Context

Alternative approaches: Balance of cost vs. risk




---

---

---

---

---

---

---

---

### Smart Cards: Scaling to the Enterprise

Agenda

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- **Physical & Logical Components**
- Standards
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---

---

---

---

---

**Physical and Logical Components** 58

**Types of cards and tokens**

- **Card**
  - Plastic with embedded microchip
  - Credit card form factor
  - More real estate
  - Massive production capability because of bank card market
  - Good "wallet appeal"
- **USB Token**
  - Same chip stored in USB device
  - Often looped for "keychain dongle"
  - No reader required
  - Easy to embed antenna
  - Good size to add biometric
  - But lack of real estate prevents badging

---

---

---

---

---

---

---

---

---

---

**Physical and Logical Components** 59

**Smart cards are not...**

- **Magnetic stripe cards**
  - Like most bank debit/credit cards
  - Loyalty cards
  - All processing is performed off-card
  - Stripe encodes small amount of data
  - (A smart card can add a mag stripe)
- **Memory cards**
  - Flash (or other) RAM for stored values onboard
  - Processing performed off-card
  - Fairly large memory sizes available today (USB drives)
  - (Smart cards contain memory, but it's secondary to the CPU)

---

---

---

---

---

---

---

---

---

---

**Physical and Logical Components** 60

**The chip**

- **Interfaces**
  - Contact (ISO 7816)
  - Contactless (ISO 14443)
- **Processing**
  - General microprocessor unit (MPU/CPU)
  - Cryptographic operations
  - Random number generator
- **Memory**
  - Flash for persistent
- **Countermeasures**
  - Anti-DPA
  - Electrical protection

Source: Fujitsu

---

---

---

---

---

---

---

---

---

---

**Physical and Logical Components** 41

**Card operating system (COS)**

- Responsible for input/output
- File and data management
- Access control
- Can be dedicated to a particular application (e.g. ePurse) or multi-application
- Trend is toward the latter
  - MULTOS: Multiple Application Operating System (backed by MasterCard)
  - STARCOS (Giesecke & Devrient [G&D])
  - JavaCard: JVM onboard for applet execution (backed by Sun)
  - The above COS's provide general application platform, create better interoperability, and improve card capabilities

---

---

---

---

---

---

---

---

**Physical and Logical Components** 42

**Types of interfaces**

- Contact
  - Require physical contact between reader and the card
  - Conductive module on the surface of the card
  - Data, algorithm, and other information transmitted via physical reader
- Contactless
  - Embedded antenna
  - Passive: radio frequency from reader provides power
  - Nonbattery cards need 2-3 inch proximity
  - Classic use: drive-through toll booths
- Hybrid (combi-cards)
  - Contains both interfaces
  - Contactless might serve as premises access mechanism

---

---

---

---

---

---


---

---

**Physical and Logical Components** 43

**Readers (terminals)**

- One of the stumbling blocks for standard smart card deployment
- Uptake in Europe presumed better partially because of reader infrastructure
- Built-in readers becoming more widespread: e.g. Dell
  - Also, millions of SIM chips in phones, but no real uptake for identity apps




---

---

---

---

---

---

---

---

**Physical and Logical Components** 64

**Embedded smart cards**

- Idea: put smart card functionality inside the computing device
- Trusted Computing Group (TCG)
  - Formerly Trusted Computing Platform Alliance (TCPA)
  - Creates specifications for trusted platform module (TPM)
  - Secure storage, registers, and crypto functions
  - Can provide smart card functionality + trusted platform assurance
  - Close to 60 organizations involved
- Products available today
  - IBM ThinkPad notebooks and NetVista desktops
  - HP D530 desktops
  - Intel D865GRH motherboard

---

---

---

---

---

---

---

---

**Physical and Logical Components** 65

**Middleware**

- Driver software
  - PC/SC
  - CAPI CSP & PKCS#11
- APIs for application support
  - Cryptographic functions
  - Data storage
  - Card management
- Special-purpose features
  - Password management
  - Single sign-on

---

---

---

---

---

---

---

---

**Physical and Logical Components** 66

**Server environment**

- Card management
- Public Key Infrastructure
- IdM systems
  - Provisioning
  - Directories
- Single sign-on platforms
- Legacy remote access
  - SecurID (ACE servers)
  - Dial-up and VPN (RADIUS / TACACS+)

---

---

---

---

---

---

---

---

### Physical and Logical Components

**SmartBadge**

- User picture
- Company logo
- 1D barcode
  - ID number
- 2D barcode
  - Biometric or other information
- Magnetic stripe
- Wireless/proximity antenna
- Smart chip

---

---

---

---

---

---

---

---

---

---

---

---

### Smart Cards: Scaling to the Enterprise

**Agenda**

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- Physical & Logical Components
- **Standards**
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---

---

---

---

---

---

---

---

---

### Standards

**Technology**

- ISO 7816
  - Main smart card standard
  - Four core parts
    - 1: Physical characteristics (stress levels, EMR protection)
    - 2: Contact layout (pinouts and location of chip)
    - 3: Transmission protocols (electrical standards)
    - 4: Standard card commands (read, write, erase, verify, get challenge, ...)
- ISO 14443
  - "Proximity" radio frequency
  - Higher power and speed, smaller distance (up to 10 cm)
  - Secure channel for contactless chip communication
- ISO 15693
  - "Vicinity" radio frequency
  - Lower power and speed, greater distance (up to 1 meter)
  - Often used for premises access (door badging)

---

---

---

---

---

---

---

---


---

---

---

---

**Standards** 70



**Programming**

- PC/SC API
  - wincard.dll on Windows; OpenSC/MUSCLE on open source
  - Low level abstraction for talking to reader
- Windows cryptography API (CryptoAPI or CAPI)
  - Programming interface for cryptographic functions in Windows
  - Card vendors provide cryptographic service provider (CSP) that implements the API
  - Example calls: CryptHashData(), CryptGenKey(), CryptEncrypt()
- PKCS#11 (also called cryptoki)
  - "Cryptographic Token Interface Standard"
  - Similar concept to CAPI for cross-platform environments
  - Developed by RSA
  - Used by Netscape, Mozilla, and other security applications
  - Example calls: C\_Digest(), C\_GenerateKey(), C\_Encrypt()

---

---

---

---

---

---


---

---

---

---

**Standards** 71



**Key and file system management**

- PKCS#12
  - "Personal Information Exchange Syntax Standard"
  - Another part of RSA's public key cryptography standards
  - Secure transport of private keys, certificates, and other secrets
  - Typically passphrase-protected
  - Often used to transfer keys from card to card
- PKCS#15
  - "Cryptographic Token Information Format Standard"
  - Interoperable format for placing information on cards
  - Independent of the access method (PKCS#11, CAPI, etc.)
  - Standardizes management of applications, keys, certificates, and other data on cards

---

---

---

---

---

---

---

---

---

---

**Standards** 72



**Certification and accreditation**

- FIPS 140-2
  - "Security Requirements for Cryptographic Modules"
  - NIST program for assessing security of crypto
  - Four rating levels (1-4) to indicate increasing security assurance
- Common Criteria
  - ISO 15408: international standard for security criteria
  - Successor to TCSEC, ITSEC
  - Several smart card protection profiles (PPs)
    - Smart Card Security User Group Smart Card Protection Profile (SCSUG-SCPP)
    - Java Card Protection Profile
    - EUROSIMART Protection Profile

---

---

---

---

---

---


---

---

---

---

**Standards** 71



**Government Smart Card Interoperability Specification**

- Important U.S. Government-driven effort
- Based on existing standards to create concrete guidelines for implementation
  - For example, extends ISO 7816/4 to formalize card commands
- Goals
  - Provide standard, high-level smart card services interface for applications
  - Card vendor neutral
  - Work with any card reader driver layer
- Has improved interoperability, but lacks some elements
  - Card initialization, key management, biometrics integration

---

---

---

---


---

---

---

---

**Standards** 74



**Consortia**

- Open Security Exchange
  - Technical interoperability specifications for physical/logical infrastructure (premises and computer authentication)
- Europay, Mastercard, VISA (EMV)
  - Smart card-based payment network in Europe
- Trusted Computing Group
  - TPM standards extending to other devices (PDAs, keyboards, ...)
- Trade groups
  - EUROSART, Smart Card Alliance, International Smart Cards Association Network (ISCAN)

---

---

---

---


---

---

---

---

**Standards** 75



**Good, bad, and ugly: Where standards fall short**

- Progress over the last few years...
  - Multi-application card OS
  - Standard drivers and interfaces
  - Congealing contactless standards
- ...but still work ahead
  - How to use multi-application platforms over disparate security domains
  - Standard way to use card real estate (mag stripes, printing, etc.)
  - Biometric integration and data interpretation
  - Mixed success with optical features (such as holograms)
- Policy and privacy are big issues
  - What information can/should be stored/revealed in various contexts?

---

---

---

---

---

---

---

---

### Smart Cards: Scaling to the Enterprise

**Agenda**

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- Physical & Logical Components
- Standards
- ***Smart Card Life Cycle Management***
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

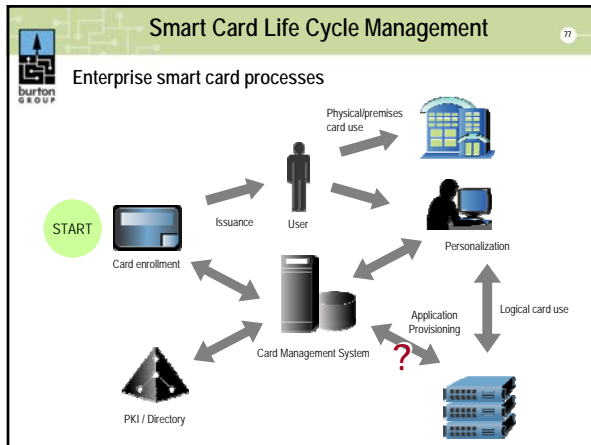
---

---

---

---

---




---

---

---

---

---

---

---

---

### Smart Card Life Cycle Management

Card management system

- Important part of the smart card IT environment
- Smart card integration and management is complex
- Many processes are manually intense without automation
  - Card damage, loss, replacement
  - PIN resets
  - Key management
- Fills gaps in other infrastructure
  - PKI provides some functions, but not all
- However, doesn't solve the whole problem
  - Often other integration is required with applications or IdM

---

---

---

---

---

---

---

---

**Smart Card Life Cycle Management** 79

**Card enrollment**

- Form of inventory management of cards
- Card information added to card management system
- Shared secrets often propagated to cards
  - Master administrative keys
  - Personalization codes (for future use)
- Card management system is nexus for integration
  - Web portal for self-service, enterprise directory, CA

---

---

---

---

---

---

---

---

---

---

**Smart Card Life Cycle Management** 80

**Issuance to user**

- Physically give card to user
- For badge environments, take picture
- For combined premises access, provision proximity system
  - Possibly link premises system user data to IdM infrastructure and/or card management system
  - Often requires custom integration

---

---

---

---

---

---

---

---

---

---

**Smart Card Life Cycle Management** 81

**Personalization**

- Populate logical credentials (X.509, etc.) onto smart card
- Often driven from a network operating system (NOS) or enterprise directory record
- Use Web portal, terminal service, or other mechanism to place certs on card
- Card management software mediates
- Archive keys for recovery
  - Sometimes PKI does this
- Activate self-service functions
  - Interactive "questions and answers"
  - Now if you're brave, take away the passwords

---

---

---

---

---

---

---

---

---

---

**Smart Card Life Cycle Management** 82

**Application provisioning**

- Ideally, when card management system learns about enrollee, it propagates to end systems
  - In reality this does not happen
  - Some enterprises have built glueware
  - In general, great deal of integration work
- Provisioning / meta-directory products provide scalable solution
  - Although you need to assess how well they handle PKI
  - Bi-directional feedback incomplete

Card Management System      Application Provisioning

---

---

---

---

---

---

---

---

---

---

**Smart Card Life Cycle Management** 83

**Loss, replacement, and end-of-life**

- Different versions of "lost"
  - Forgotten PIN
  - Damaged card
  - Misplaced card
  - Gone forever
- Same for replacement
  - PIN reset
  - Card reformat/reload
  - Re-provisioning card
- End-of-life
  - Central revocation of credentials
  - Still need to retrieve the hardware

---

---

---

---

---

---

---

---

---

---

**Smart Card Life Cycle Management** 84

**Card management summary**

Lifecycle step	Without card management	With card management
Issue card	Administration of multiple systems to issue credentials	Central interface: credentials tied to individual and card
Add credential or application to card	Possibly manual process; may require card presence	Remote update via self-service portal
Reset PIN	May be out of luck; or time-intensive (and \$\$) help desk call	Self-service reset via portal and user Q&A (or password)
Replace card	Manually suspend/revoke credentials and recover keys	Issue temp card, automatically suspend lost card, revoke credentials, recover keys
Deprovision card	Administration of multiple systems to revoke credentials	Central interface causes cascade of revocation

---

---

---

---

---

---

---

---

---

---

**Smart Cards: Scaling to the Enterprise** 85

**Agenda**

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- Physical & Logical Components
- Standards
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---

---

---

---

---

**Product Implementations** 86

**Product segments**

- Card providers
  - Plastic & chips
- PKI solutions
  - X.509 certificates
- Lifecycle management software
  - Automation of identity card processes
- System integrators
  - Consulting and glue between systems

---

---

---

---

---

---


---

---

**Product Implementations** 87

**Card providers**

- Axalto (formerly Schlumberger)
  - Cryptoflex: USB or card form factor
- Giesecke & Devrient (G&D)
  - Strong focus on bank card and payment solutions
- Gemplus
  - SafesITe: logical or premises access
  - Often works with integrator for full solution
- RSA Security
  - SecurID Passage smart card
- Oberthur
- SafLink/SSP-Litronic
- Siemens




---

---

---

---

---

---


---

---

**Product Implementations**

**PKI solutions**

- VeriSign
- Entrust
- Betrusted (formerly Baltimore Technologies)
- RSA Security
- Geotrust
- Microsoft
- Comodo




---

---

---

---

---

---


---

---

**Product Implementations**

**Lifecycle management software**

- ActivCard
- Alacris
- BellID
- DataCard
- DataKey
- Intercede
- SmartTrust
- Card vendors beginning to add lifecycle management functions, as well




---

---

---

---

---

---


---

---

**Product Implementations**

**System integrators**

- Big list: Includes independents, consultants, and government contractors
- Four major duties
  - Project planning
  - Policy and procedure creation
  - Actual technology integration
  - Vendor project management (tie the threads together)
- Can provide crucial services, but don't discount your own abilities
  - Most organizations mature and learn a lot during the project
  - End up realizing they can do many things themselves




---

---

---

---

---

---

---

---

**Product Implementations** 91

**Burton group market assessment**

- No clear market leaders identified
- No one vendor with clear advantage
- Vendors tend to concentrate in application areas of expertise
  - Smart cards are generally not used the same in each application
  - Example: Payment and bank cards distinct from SIM cards
  - ID and smart badges are among the few convergences
  - (Although things are beginning to change with contactless)
- Successful projects draw from all market segments
  - Card provider + PKI/credentialing + lifecycle management + premises system + identity management + integrator

---

---

---

---

---

---

---

---

---

---

**Smart Cards: Scaling to the Enterprise** 92

**Agenda**

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- Physical & Logical Components
- Standards
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---

---

---

---

---

---

---

**Issues and Risks** 93

**Card factors to consider**

- How reliable is the card?
  - Failure rates
  - Use environments: damp, cold, hot, greasy, ...
  - Expected number of inserts: is contactless a better choice?
- How much storage capacity does the chip have?
  - Number of certificates: signing, authentication, encryption
  - Number of applications/applets
  - Stored values: credential cache or payment info onboard
  - Example: 64K card quickly erodes when cardOS + applets + certificates + password storage are all added
- Can cardholders easily use the cards?
  - Software and hardware required
  - Training for how and when to use cards for physical and logical access

---

---

---

---

---

---

---

---

---

---

**Issues and Risks** 94

**Card factors to consider (continued)**

- How fast is the card read rate?
  - Amount of data processed and transferred by the card
  - Especially in contactless: speed of recognition
- What standards does the card comply with?
  - Laundry list in the above slides
  - Most important is testing interoperability with the applications you plan to deploy or integrate
- How much processing power does the card have?
  - Credential cache has fall lower requirements than digital signatures
  - Planning for the future is very important
  - New applets might require more cycles

---

---

---

---

---

---

---

---

**Issues and Risks** 95

**Smart card costs**

- Cost per card averages \$25
- Cost per add-on reader (USB) averages \$20
  - Should consider one reader per workstation
  - Could lower cost per reader by deploying workstations that have integrated readers
  - Costs are trending downward
  - Embedded "smart card" (TPM) is an alternative
- Physical access contactless readers average \$1,000 per server
  - May need to replace existing physical access systems to work with chosen smart card system




---

---

---

---

---

---

---

---

**Issues and Risks** 96

**Additional costs for deployment**

- Badging and photographic systems to produce the employee likeness and information on the smart card
- PKI server to load on the system access credential
- Administrators for managing the credentials
- Database for storing and distributing the credentials for validation
- Administrator and employee training
- Application development to utilize smart card access on workstation applications
- Integration with existing or emerging IdM infrastructure
- Cost of developing new administrative, business, and access policies
- Design/deployment of smart card services across all sites

---

---

---

---


---

---


---

---

**Issues and Risks** 97

 **Security concerns**

- High-level threats
  - Differential power analysis (DPA)
  - Electrical analysis
  - IEEE JVM attack
  - Algorithm failures
  - FIPS 140-2 best way to hedge
- Operational concerns
  - Policies about PIN use and protection
  - Administrator malfeasance/errors
  - Fallback authentication mechanisms
  - Identity vetting procedures
  - Proper key recovery




---

---

---

---


---

---

---

---

**Issues and Risks** 98

 **Integration issues**

- Desktop support
  - Much smaller concern, with built-in Windows support and stronger middleware
  - Linux drivers are emerging
  - Still need to test in the target environment
- Holes between IdM/directory, smart card management, and building access systems
- Help desk
  - "People problem": can they answer user questions?
  - Do they have access to required information to resolve problems?

---

---

---

---

---

---

---

---

**Smart Cards: Scaling to the Enterprise** 99

 **Agenda**

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- Physical & Logical Components
- Standards
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---

---

---

---

---

**Case Studies** 100

**Aerospace company**

- Background
  - 250,000+ employees and contractors
  - Wanted a common "smart badge" for logical/physical access
  - Project started before 9/11, but was accelerated afterward
- Goals
  - User login to Web SSO
  - Windows desktop login
  - Password wallet
  - Dual certificates (encryption and signing/authentication)
  - Premises access




---

---

---

---

---

---

---

---

**Case Studies** 101

**Aerospace company**

- Successes
  - Initial pilots completed
  - 94% of users successfully install and use readers
  - 85% of users successfully initialize cards
    - Software versions and "not following instructions"
  - Project engaged physical security team at the start
  - Pre-existing software distribution system helped rollout
- Challenges
  - Badge management software was home-grown, so integration was difficult
  - Help desk not trained early enough
  - Desired Web services interfaces between components
  - "Overbooked" the system integrator
    - Underestimated their own abilities
    - Company was able to do many things themselves

---

---

---

---

---

---


---

---

**Case Studies** 102

**Energy company**

- Background
  - Another smart badge project at large company
  - Using Microsoft CA for PKI certificate issuance
  - 35,000 premises smart cards deployed so far
  - 5,500 of those have logical credentials provisioned
- Goals
  - Converge building and logical systems access
  - Soft token applet - SecurID (for legacy remote access)
  - PKI certificates
  - Ability to let departments choose applications as required
    - E.g. phone group created punch clock application for time tracking
  - WebTrust for CAs audit (comprehensive control environment)




---

---

---

---

---

---

---

---

**Case Studies** 103

**Energy company**

- **Successes**
  - Use terminal services for strong user self-service
  - Key recovery, PIN reset, card replacement quite smooth
  - Utilized local registration agents to help with ID and card issuance
    - E.g. manufacturing foreman
  - Developed comprehensive Q&A system for user authentication
  - Charge departments \$150 for card replacement
- **Challenges**
  - Linux users often unhappy with limited support
  - Because of multiple apps, must get several groups working/talking together
  - Users want uniform point of contact for support calls
  - "You'll have to pry my password from my cold, dead fingers"
  - Creating Q&As is English-only and may be culturally bound

---

---

---

---

---

---


---

---

**Case Studies** 104

**Government agency**

- **Background**
  - Public works agency of national government
  - Receives plans and designs from 20,000 field engineers
  - Wanted to expedite 20 million annual plan reviews
- **Goals**
  - Create electronic document workflow
  - Rely on recent legislation for legal enforcement of digital signatures
  - Strong identity vetting




---

---

---

---

---

---

---

---

**Case Studies** 105

**Government agency**

- **Successes**
  - Smart card management system helped provide multi-platform support
  - Users saw immediate ROI: time and money greatly reduced for document submission
    - Allowed for quick adoption
  - Smart card served dual-use as professional association member card and credential store
- **Challenges**
  - Engineers don't have common operating environments
    - All aspects of solution had to be multi-platform
  - Integrator was required to add several features to document display and signing engine
    - Certificate validation
    - Timestamping
    - Workflow approval
  - Long-term electronic document retention unproven

---

---

---

---


---

---

---

---

**Smart Cards: Scaling to the Enterprise** 106



**Agenda**

- Introduction & Strategic Context
  - Key Business Drivers
  - Role of PKI
  - Smart Card Concepts
  - Alternative Approaches
- Physical & Logical Components
- Standards
- Smart Card Life Cycle Management
- Product Implementations
- Issues & Risks
- Case Studies
- Recommendations & Best Practices

---

---

---

---


---

---

---

---

**Recommendations and Best Practices** 107



**Think "Big Picture"**

- Implement smart cards as part of an enterprise IdM initiative, not solely a PKI initiative
  - Certificate and account provisioning and de-provisioning
  - Security policies and business processes to support and potentially automate deployment and account, card provisioning
  - Directory Services
  - Web Access Management, SSO solutions
  - Provisioning solutions
  - Federated trust and technology models

---

---

---

---


---

---

---

---

**Recommendations and Best Practices** 108



**Think "Big Picture" (continued)**

- Consider issues such as:
  - IdM component support for smart card authentication, PKI
    - Proven interoperability with specific smart card management and PKI products
  - Availability of readers
  - Policies for dealing with lost or stolen cards
  - How to manage remote users and business partners
    - Again, part of the overall IdM infrastructure
  - Enterprise's "legal readiness" to establish and maintain trust relationships

---

---

---

---


---

---

---

---

**Recommendations and Best Practices** 109



**Managing the project**

- Establish objectives
- Make sure the organization has a stake in the project's success
- Get management approval and support
- Set a budget
- Designate a project manager
- Assemble a project team and create a team vision

---

---

---

---


---

---

---

---

**Recommendations and Best Practices** 110



**Managing the project (continued)**

- Assess the card and reader options
- Write a detailed specification for the system
  - Stick to standards
- Assess vendors and issue RFI/RFP
  - Make sure the technology is mature enough for your requirements
  - Before vendor is chosen, have them give a live demonstration of the functional system
- Set a realistic schedule with good milestones
- Establish the security parameters for users and the system
- Phase-in each system element: Test as you deploy

---

---

---

---


---

---

---

---

**Recommendations and Best Practices** 111



**Managing the project (continued)**

- Reassess for security problems
- Train the key employees responsible for each area
- Set-up a system user manual
- Check the reporting structures
- Have contingency plans should problems arise
- Deploy and announce
- Advertise and market your system

---

---

---

---


---

---

---

---

**Recommendations and Best Practices** 112



**Enterprise Directory**

- Determine if certificates and CRLs are to be replicated to multiple repositories and directories for wider application use
  - Can you leverage the existing Enterprise Directory (assuming you have one)?
  - What method will you use to integrate multiple directory instances?
    - PKI certificate publishing utility
    - Meta-directory
    - Native directory replication protocol

---

---

---

---


---

---

---

---

**Recommendations and Best Practices** 113



**Enterprise Directory (continued)**

- Make sure the directory infrastructure is highly available
  - Directory design is non-trivial and must be factored into architecture
- Define how applications will search the directory for certificates
  - Example: LDAP search on certificateSubjectDN
  - Publish integration programming recommendations to developers

---

---

---

---


---

---

---

---

**Recommendations and Best Practices** 114



**Certificate naming**

- Consider industry regulations that may mandate whether user names *must or may not* be included in certificate subject names
- Is there an existing naming convention that the PKI must accommodate?
- Test for interoperability between PKI software, certificate repository, and applications early
- "Interpretation" of various standards, including naming, can arise in a multi-vendor infrastructure
  - Which you will undoubtedly need

---

---

---

---


---

---

---

---

**Recommendations and Best Practices** 115



**Application integration**

- Determine what platforms are to be integrated
- Use Java for multi-platform solutions
  - JAAS
  - Java cards
- Microsoft CAPI, XP, Windows Server 2003 may afford easier integration
  - If the predominant application environment is compatible
- Try to identify and assess compatibility of all applications that will leverage the smart card and strong authentication service infrastructure
  - Both internally-developed and commercial applications

---

---

---

---

---

---

---

---

**Recommendations and Best Practices** 116



**Organizational ownership and accountability across processes**

- Enterprise security policy definition
- Security monitoring and auditing functions and requirements
- User provisioning and asset management
  - Card issuance
  - Card lifecycle management
  - Identity vetting
- Incident response
- Business continuity planning for disaster recovery

---

---

---

---


---

---

---

---

**Conclusions** 117



**What you have learned**

- Business drivers are pushing enterprises toward stronger authentication methods
  - Many want SSO or RSO, but don't want risk aggregation
  - Regulations, identity assurance, audit-ability, risk mitigation, others
- Smart cards supporting strong authentication gaining mind share and deployment is increasing
- PKI likely to play a vital infrastructure role in your solution

---

---

---

---


---

---

---

---

**Conclusions** 118



**What you have learned (continued)**

- Deploy smart cards as part of an overall Identity Management initiative within the enterprise
  - Think Big Picture
  - This is a smart way to ensure scalability
- Protect information assets with an authentication strategy that meets specific data classification levels
  - Federation techniques must incorporate this strategy and policy
  - Trust models are crucial to scaling beyond the Enterprise

---

---

---

---


---

---

---

---

**Smart Cards: Scaling to the Enterprise** 119



**References and further reading**

- Burton Group Directory and Security Strategies
  - Leveraging Smart Cards for Strong Identity
  - Strong Authentication Deployment Drivers and Obstacles
  - Cryptographic Systems Provide Foundation for Information Security
  - Directory and Security Services Reference Architecture
  - Reference Architecture Technical Position: PKI
  - Smart Card Deployment Survey Results (Methodologies & Best Practices)
  - Toward Federated Identity Management: The Journey Continues
  - SAML: Bringing on the First Wave of Federation
  - Electronic Signatures: Solutions Maturing as Regulatory Deadlines Loom

---

---

---

---


---

---

---

---

**Smart Cards: Scaling to the Enterprise** 120



**References and further reading (continued)**

- NIST smart card standards and research
  - <http://smartcard.nist.gov/>
- FIPS 140-2
  - <http://csrc.nist.gov/cryptval/>
- Smart Card Alliance
  - <http://www.smartcardalliance.org>
- Open Security Exchange
  - <http://www.opensecurityexchange.com>
- Trusted Computing Group
  - <http://www.trustedcomputinggroup.org>

---

---

---

---

---

---

---

---