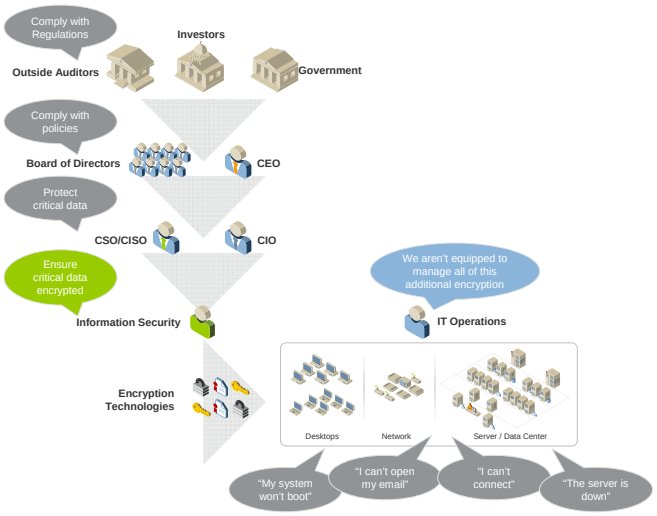
A Holistic Approach to Key Lifecycle Management

Joe Skehan, Director of Product Management

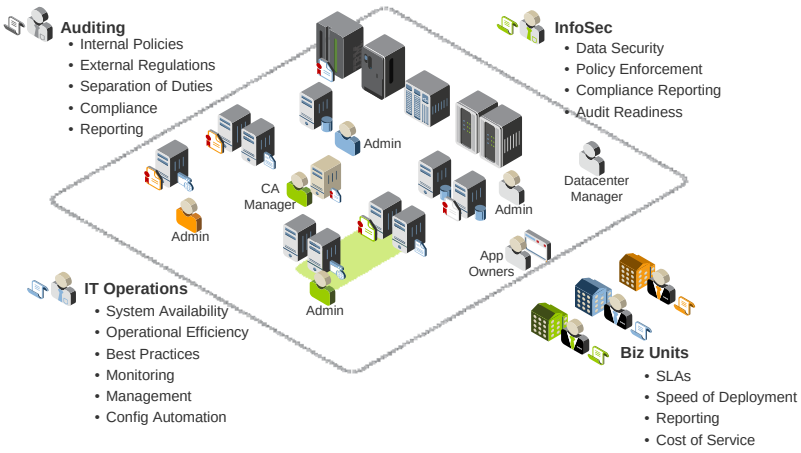
Encryption. **Managed.**

June 10, 2009

Pressure Driving the Use of Encryption



Who Owns Encryption?



Encryption Challenges

Challenges	Causes
INFOSEC	
Data Security	Assuring encryption is used where needed for data in transit and at rest across highly distributed environments
Key Security	Implementing effective key management processes in spite of operational requirements, application constraints, and other organizational factors
Enforceability	No ability to measure, prove or enforce compliance with policies
InfoSec Agility	Potentially high risk exposure from limited pace of encryption adoption/deployment
Audit Readiness	Responding to compliance audits is resource intensive, expensive
IT OPS	
Operational Efficiency	Managing encryption keys and certificates manually; reacting to incidents and emergencies.
System Availability	Unexpected certificate expiration causing critical system downtime and outages.
Reputational Risk	Losing customers, missing transactions, unnecessary human interaction, brand erosion
Business Continuity/ Disaster Recovery	Insufficient disaster recovery plans to respond rapidly to catastrophic encryption failures, including intermediate root expirations, CA compromises, and broken algorithms.
Sourcing Costs	Ad hoc distributed certificate acquisition
Best Practices	No ability to enforce and demonstrate adherence to best practices (i.e., ITIL)
PRIVACY	
Brand Risk Reduction	Brand impacting disclosures due to loss of customer and employee data
Safe Harbor Coverage	Inability to enforce policies that leverage safe harbors

Encryption Landscape

Information Risk Management

Enterprise-Wide Compliance and Control
(Encryption Discovery & Monitoring Platform)

Client	Server	Network	Storage
Client Data Protection (EFS)	Web System Encryption Management	Network Encryption (SSL Accelerators)	Encrypted Database Management
Secure Communications (Outlook)	Middleware and App. Server Management	Router Encryption Management	Encrypted Tape Key Management
Strong Auth for Remote Access (VPN)	Mainframe	Firewalls	NAS
Disk Encryption (BitLocker)	SSH Management	Switches	SANs
Wireless Encryption Management	PGP	Wireless	Offline Storage
more…	more…	more…	more…

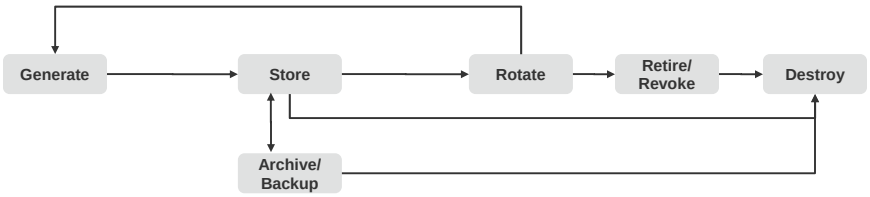
Diversity of Encryption Types

Encryption Types:

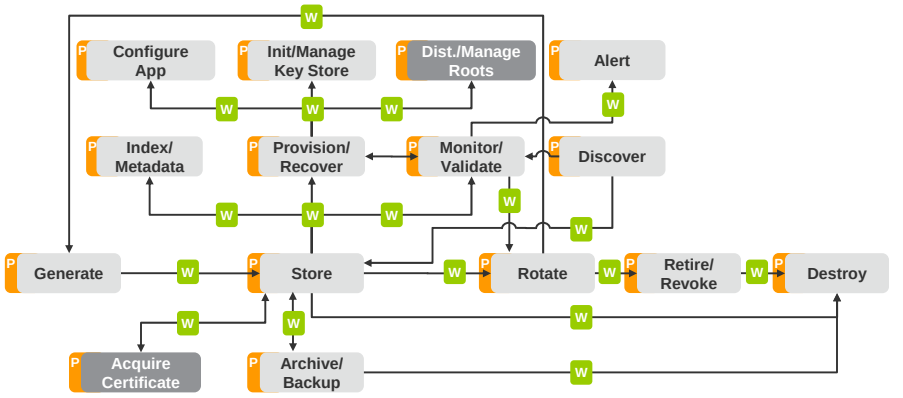
- **- Certificate**
- **- Symmetric**
- **- Asymmetric**
- **- Other**

Client	Server	Network	Storage
Client Data Protection (EFS)	Web System Encryption Management	Network Encryption (SSL Accelerators)	Encrypted Database Management
Secure Communications (Outlook)	Middleware and App. Server Management	Router Encryption Management	Encrypted Tape Key Management
Strong Auth for Remote Access (VPN)	Mainframe	Firewalls	NAS
Disk Encryption (BitLocker)	SSH Management	Switches	SANs
Wireless Encryption Management	PGP	Wireless	Offline Storage
more…	more…	more…	more…

Lifecycle Management



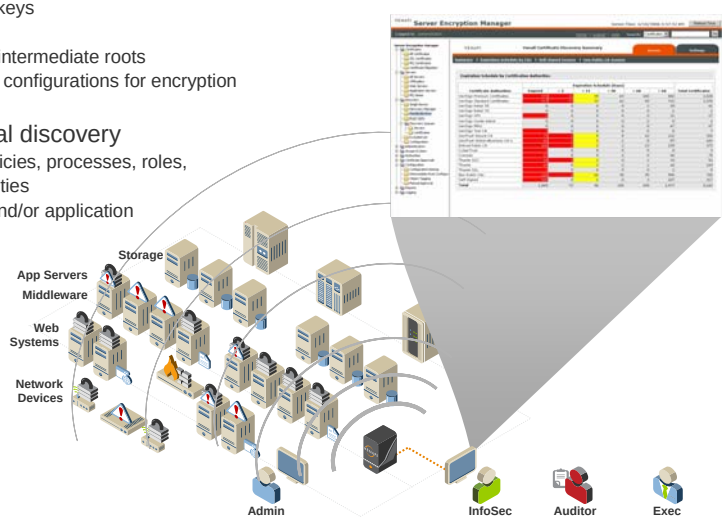
The Reality of Lifecycle Management



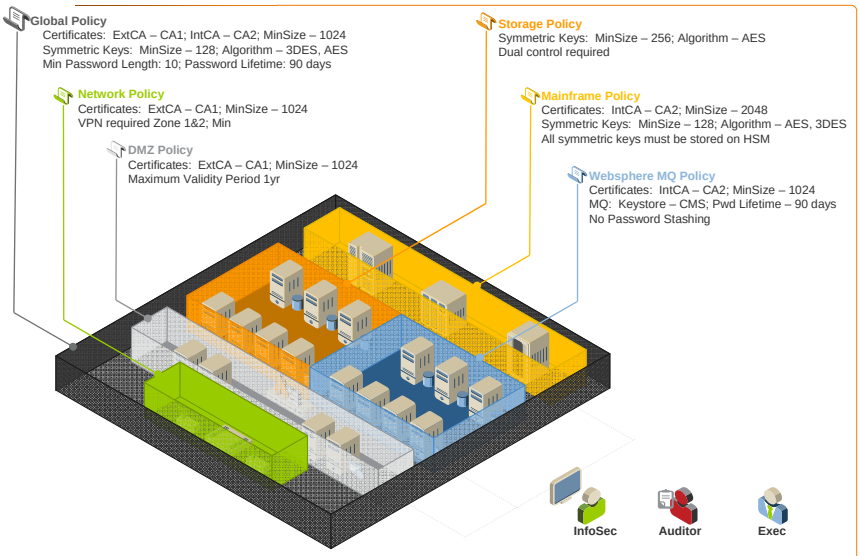
Encryption Discovery

Discover and inventory
- End-entity keys
- Certificates
- Roots and intermediate roots
- Application configurations for encryption
- Versions

Organizational discovery
- Current policies, processes, roles, responsibilities
- By group and/or application



Enterprise Encryption Policies



Enterprise Encryption Policies

Global Policy
Certificates: ExtCA – CA1; IntCA – CA2; MinSize – 1024
Symmetric Keys: MinSize – 128; Algorithm – 3DES, AES
Min Password Length: 10; Password Lifetime: 90 days

- Data
  - Standard classifications and assignment guidelines
  - System criticality
  - Sensitivity
  - Protection levels by classification type
- Discovery
  - Where to perform discoveries
  - Who performs
  - How often
- Keys
  - Key Length
  - Algorithm
  - Key validity periods (including private keys, e.g. rekeying)
  - Rekeying vs. key reuse
  - Key backup processes
  - Key duplication processes
  - Distribution methods
  - Generation (central or local)
  - Backup and recovery rules
  - Storage requirements
  - Key access methods (password, token, M-of-N)
  - Access controls (assigned admins and rights)
- Certificates
  - Approved Certificate Authorities
  - Certificate Validity Period
  - Renewal Window
  - Subject DN Naming Guidelines
  - Certificate templates (certificate extensions, etc.)
  - Approvals and workflow
  - Roots and trust

Network Policy
Certificates: ExtCA – CA1; MinSize – 1024
VPN required Zone 1&2; Min

DMZ Policy
Certificates: ExtCA – CA1; MinSize – 1024
Maximum Validity Period 1yr

Storage Policy
Symmetric Keys: MinSize – 256; Algorithm – AES
Key Store Paths and filenames

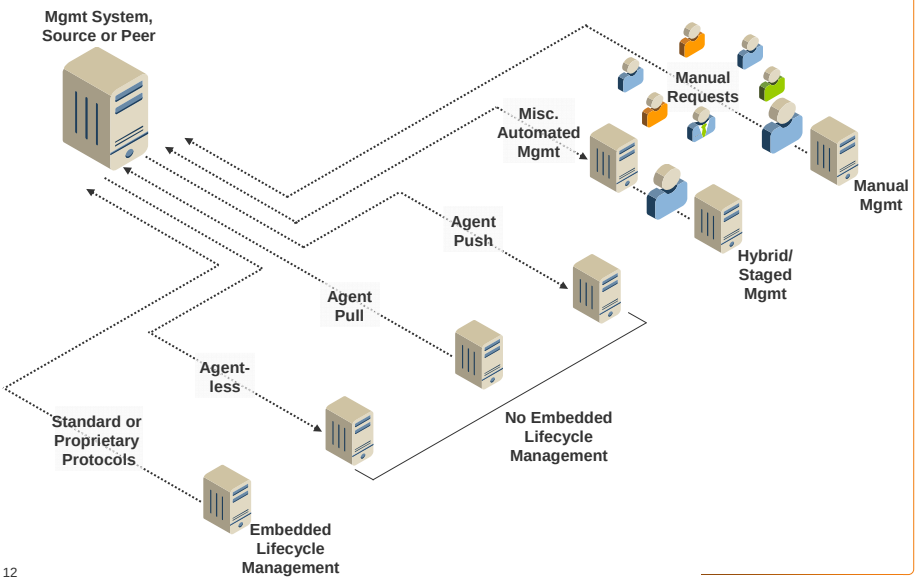
Mainframe Policy
Certificates: IntCA – CA2; MinSize – 2048
Symmetric Keys: MinSize – 128; Algorithm – AES, 3DES
All symmetric keys must be stored on HSM

Websphere MQ Policy
Certificates: IntCA – CA2; MinSize – 1024
MQ: Keystore – CMS; Pwd Lifetime – 90 days
No Password Stashing

- Key Stores
  - Key Store Paths and filenames
  - Password Length
  - Password content rules
  - Password lifetime maximums
  - Password stashing
  - Key store types (HSM, PKCS#12, CMS, JKS, PEM, etc.)
  - Key store authentication method (Certificate, Key, Pwd, M-of-N)
  - Access controls (assigned admins and rights)
- Applications
  - Application configuration
  - Device configuration
  - Minimum application versions
- Disaster recovery
  - Backup/Restore
- Validation and monitoring
  - Validating Operation
  - Validating Integrity
- Reporting
- Workflow and Processes
  - Workflow steps for each process
  - Notifications and alerts (which events, who to notify, when…)
  - Timing of events (renewal windows, etc.)
  - Escalation paths
  - Allowed encryption management models
- Roles and rights assignments
  - Separation of duties
- Lots more…

InfoSec Auditor Exec

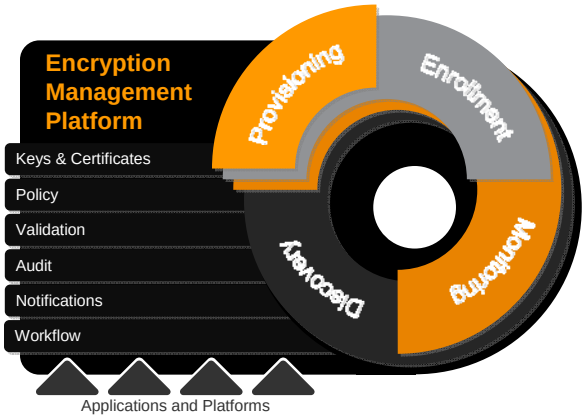
Encryption Management and Distribution Models



Requirements and Constraints Driving Encryption Management Models

Requirements/Constraints	Manual	Hybrid	Built-in LM	Agent Push	Agent Pull	Agent less
No automation on production systems (operations)	🟡	🟢	🔴	🔴	🔴	🔴
Manual handling of keys prohibited (security)	🔴	🔴	🟢	🟢	🟢	🟢
Agents not possible (policies, appliances, etc.)	🟡	🟢	🟢	🔴	🔴	🟢
Remote access not allowed	🟡	🟢	🟢	🔴	🟢	🔴
App configuration policies must be enforced	🟡	🟡	🟡	🟢	🟢	🟢
Synchronous duplication of keys required	🟡	🟡	🟡	🟢	🟡	🟢
Centralized monitoring and alerting required	🔴	🔴	🟡	🟢	🟢	🟢
Others…	?	?	?	?	?	?

Encryption Management Platform



VENAFI

Questions?

Joe.Skehan@venafi.com

VENAFI