Automating data-protection across the enterprise
About 40 years ago....

- Primary protection problem
  - Some military communications and data
  - Some financial transactions
- Primary cryptographic algorithm
  - 56-bit DES
- Key-management
  - Manual
- Volume of data to be managed
  - Megabytes? Gigabyte?
20 years ago

- Primary protection problem
  - Most military communications and data
  - Some civil communications and data
  - Most financial transactions
- Primary cryptographic algorithms
  - Triple-DES, RSA, MD5
- Key-management
  - Semi-automatic and Manual
- Volume of data to be managed
  - Gigabytes? Terabyte?
• Primary protection problem
  – Most military and civil communications and data
  – Most financial transactions
• Primary cryptographic algorithms
  – AES, 3DES, RSA, ECC, SHA-256,....
• Key-management
  – Automatic
• Volume of data to be managed
  – Petabytes? Exabytes?
Yet, the problem is....

- We're still trying to protect the network
- We're still relying on secret-key sharing for passwords
- We're still protecting data with ad hoc data-protection
  - Reacting to PCI-DSS
  - Reacting to HIPAA
  - Reacting to EU Directive
  - Reacting...
  - Reacting...
What is the solution?

- A proactive approach to security that starts by:
  - Defending the core first: the data
  - Hardening the system next
  - Assuming the network cannot be trusted
- Something to protect data on a massive scale
- Something that is ubiquitous across the enterprise (DNS)
- Something that is not an application-specific silo
- Something that meets today's needs and anticipates tomorrow's
DATA ENCRYPTION INFRASTRUCTURE (DEI)
What is a DEI? - 1

- Standard network service to encrypt/decrypt billions of documents/media files
- Hide complexity from software developers by exposing a simple web-service interface
- Work with any programming language on any platform
- Stores ciphertext anywhere - public clouds, private clouds, SAN, NAS, etc.
- Centrally manage cryptographic keys in accordance with security regulations and industry standards
What is a DEI? - 2

- Support synchronous and asynchronous services for service-prioritization
- Auto-scale cryptographic capacity to handle volume-spikes while conserving resources during volume-slumps
- Automatically load-balance to even out performance peaks/valleys
- Be highly-available
- Integrate to centralized IAM
- Support auditing at all levels of the infrastructure
DATA ENCRYPTION INFRASTRUCTURE REFERENCE IMPLEMENTATION (DEIRI)
Front-end Processors (FEP) to manage the infrastructure and serve as the primary interface to the DEI.
Auto-scaling private cloud of **CryptoEngines** to perform the cryptographic operations.
Key Management System (KMS) to manage billions of cryptographic keys centrally.
IAM system to manage centralized access control.
Private or Public Cloud, or a private SAN/NAS to store encrypted data.
Finally...

Applications to take advantage of the DEI.

Primary DC - Document Encryption Infrastructure

Secondary DC - Document Encryption Infrastructure
Performance

- **FEP**: 6-Core, 64-bit, 3.2 Ghz CPU, 16GB DRAM, 1600 Mhz, Gigabit network, 64-bit Linux, JEE5 AppServer, RDBMS
- **CE**: VM's with single-core, 64-bit, 3.1 Ghz CPU, 8GB DRAM, 1600 Mhz, Gigabit NW, 64-bit Linux, JEE5 AS
- **KMS**: 6-Core, 64-bit, 3.2 Ghz CPU, 8GB DRAM, 1600 Mhz, Gigabit network, 64-bit Linux, JEE5 AppServer, RDBMS
- **IAM**: External Active Directory
- **Storage**: NFS-mounted NAS
Performance

- 8+ Million PDF documents of 50-200K size each
- 20-25K average new documents per day; 50K peak load
- 300ms encryption
- 200ms decryption
- Base64-encoded images of 2-3K size each
- 100 WS-TPS
- Internal testing: 1-Gigabyte per minute encryption
Resources

- **Data Encryption Infrastructure (DEI)**

- **Regulatory Compliant Cloud Computing (RC3)**

- **Cryptographic engine (enables RC3 applications)**
  - [http://www.cryptoengine.org](http://www.cryptoengine.org)

- **CryptoCabinet (RC3 sample application)**
  - [http://www.cryptocabinet.org](http://www.cryptocabinet.org)
• Contact Information
  - Arshad Noor
  - arshad.noor@strongauth.com
  - www.strongauth.com
  - info@strongauth.com
  - +1 (408) 331-2000