Secure The Data, Not The Infrastructure
A New Approach to Data Protection

Mark Schertler

Voltage Security

December 2006

Data Protection Is Becoming More Complex

- Wide-ranging set of data protection drivers
  - Specific mandates
    - PCI, contractual obligations
  - Risk-management based
    - SOX, HIPAA, EU Data Protection Directive, PIPEDA
  - Mandatory disclosure
    - 17 states, upcoming Federal law

- Data protection requirements now impact entire enterprise architecture
  - No longer limited to specific business units/IT systems

Defending Networks Is Hard

- Existing networks are architected like the Winchester Mystery House in San Jose, California
  - Grown over time instead of planned
  - Constructed 24 hours a day for 38 years

- This won’t change any time soon

- Networks like these are becoming more and more integrated with those of business partners

Where exactly *is* the network perimeter?

- It’s not always clear where one network ends and another one begins
- Credit card processing
  - Merchants
  - Banks
  - Credit card companies
- Health care
  - Payers
  - Providers
- This makes defending the perimeter of the network even more difficult

Current Data Protection Models

- Focus on “vulnerable” parts of the network
  - But can you really distinguish what’s “vulnerable”?
- Assume a “them and us” mentality
  - But can you still identify “them” and “us”?
- Assume the infrastructure will protect us
  - But do you always have control over the infrastructure?

A New Approach

- Instead of protecting the network, protect the data
  - Make security data-centric instead of network-centric
- The easiest way to do this is to encrypt data, so that only an authorized user can decrypt it
- Can we find a feasible way to protect data by encrypting it?

Identity-Based Encryption

- Basic idea: Public-key encryption where identities & classifications can be used directly as *encryption* public keys

- Eliminates the need for certificates & certificate infrastructure
  - Removes the usability and manageability problems inherent in PKI-based solutions
  - Simplifies Traditional PKI

- **IBE Public Key:**

“alice@corp.com”
or
“Engineering”
or
“Restricted”

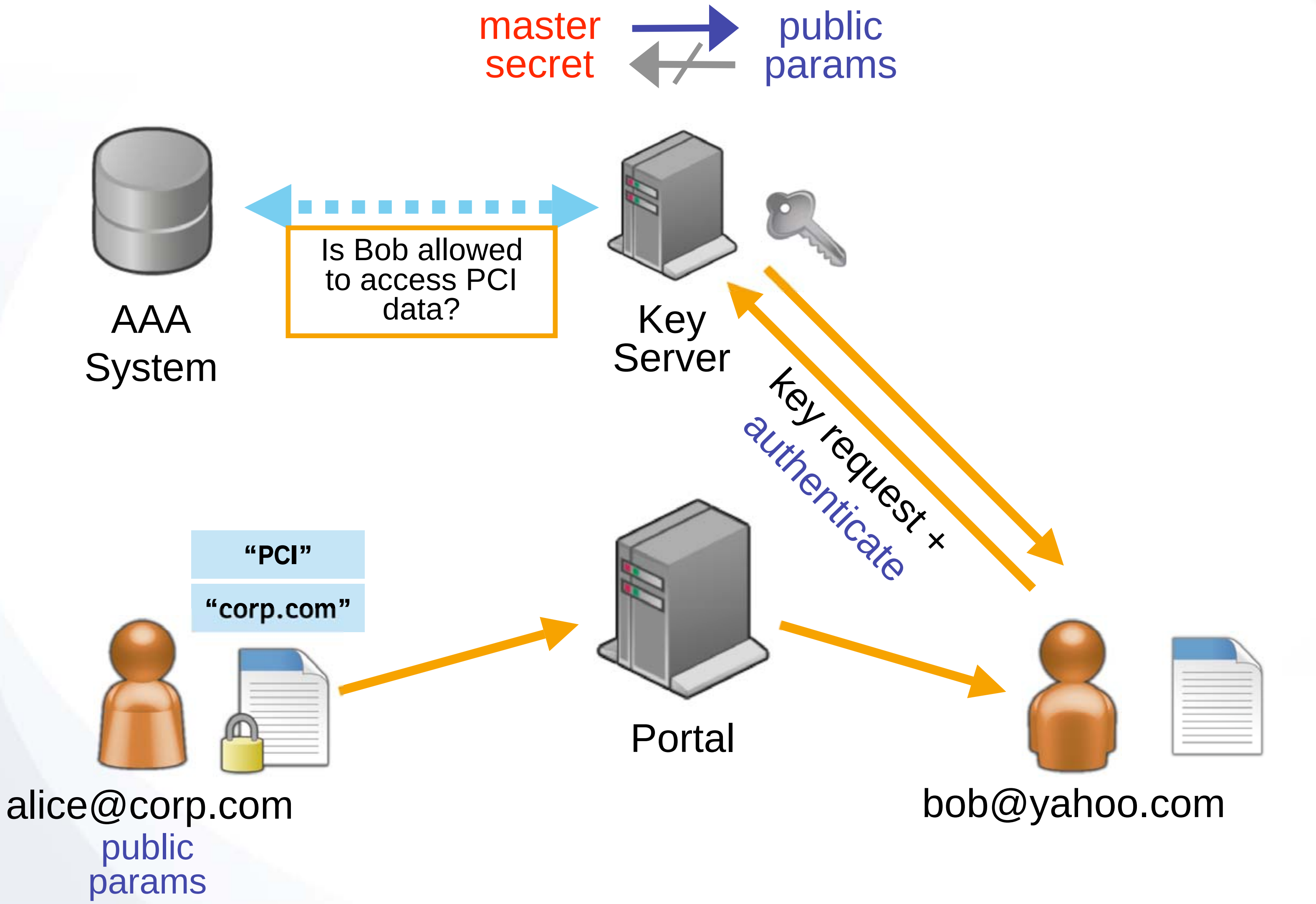
- **RSA Public Key:**

Public exponent=0x10001
Modulus=135066410865995223349603216278805969938881475605667027524485143851526510604859533833940287150571909441798207282164471551373680419703964191743046496589274256239341020864383202110372958725762358509643110564073501508187510676594629205563685529475213500852879416377328533906109750544334999811150056977236890927563

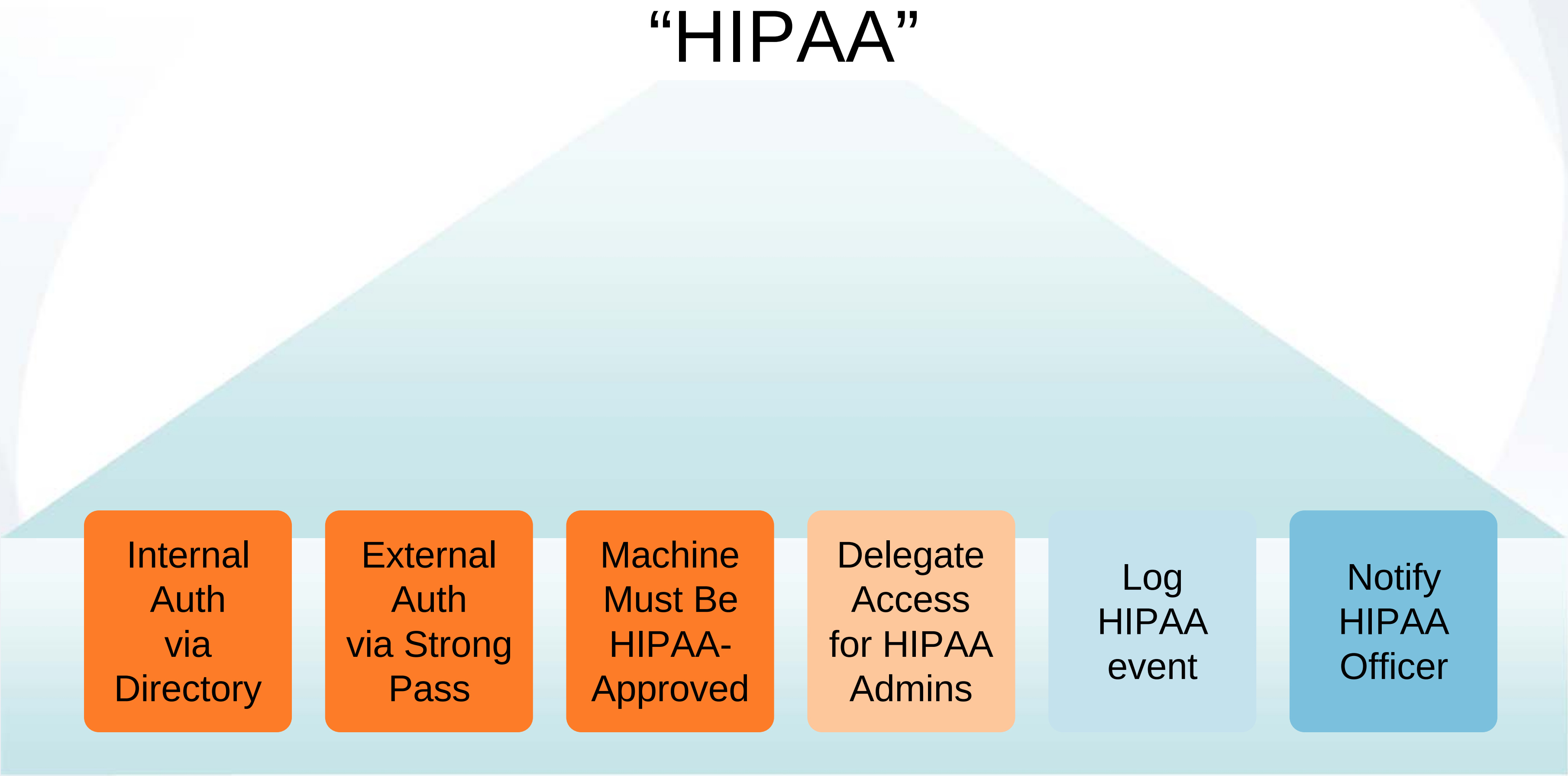
IBE: Groups and Policies

- IBE is not restricted to using identities as keys
- Encrypt to a group: **Engineering**
  - To retrieve the key, the user/application must authenticate as a member of the Engineering group
  - Leverage existing directory structures (AD, LDAP)
  - As group membership in directory changes, key access rights change dynamically as well
- Encrypt to a policy name/classification: **PCI**
  - To retrieve the key, the user/application must meet the policy defined at the server
  - Example: Asking for “PCI” key might query back-end ERP system and execute business logic
- Extremely difficult to do with PKI
  - Group certificates create major revocation and distribution problems

Policy & IBE


master
secret
public
params
Is Bob allowed to access PCI data?
AAA
System
Key
Server
key request +
authenticate
"PCI"
"corp.com"
Portal
alice@corp.com
public
params
bob@yahoo.com

Policy Definition



"HIPAA"

Internal Auth via Directory

External Auth via Strong Pass

Machine Must Be HIPAA-Approved

Delegate Access for HIPAA Admins

Log HIPAA event

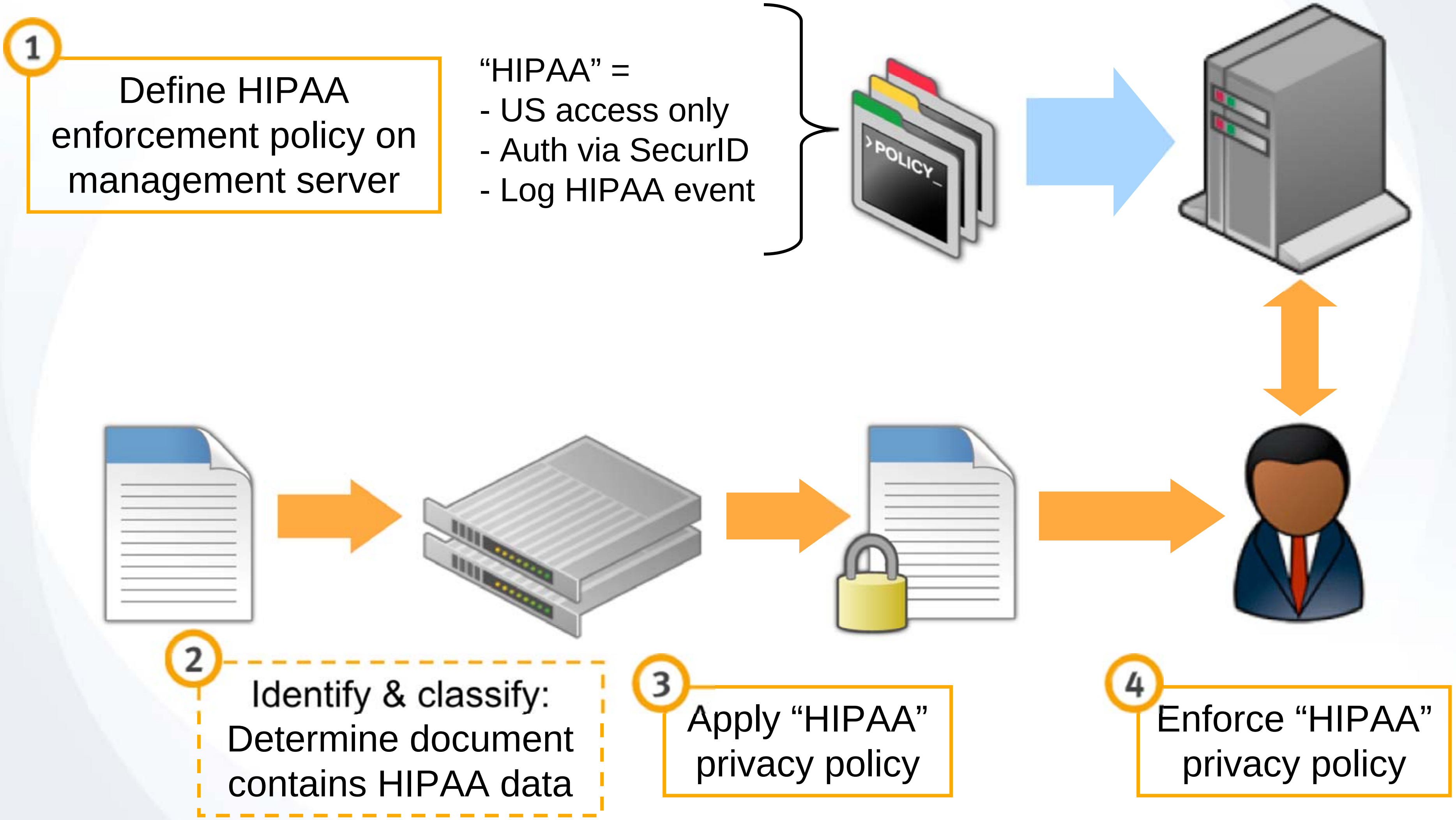
Notify HIPAA Officer

Policy-Based Encryption

- Define canonical privacy policies
  - e.g. “HIPAA”, “PCI”, “Confidential”, “Classified”, …
- Define elements of policy on server
  - e.g. “HIPAA” requires delegated access, auditing, etc.
- Encrypting agents specify privacy policy as part of key
  - Do not need to understand individual policy elements
- Privacy policy enforced by server
  - Policy can be modified over time

key = “bob@b.com || HIPAA”
key = “HIPAA”

Policy Based Encryption



1 Define HIPAA enforcement policy on management server

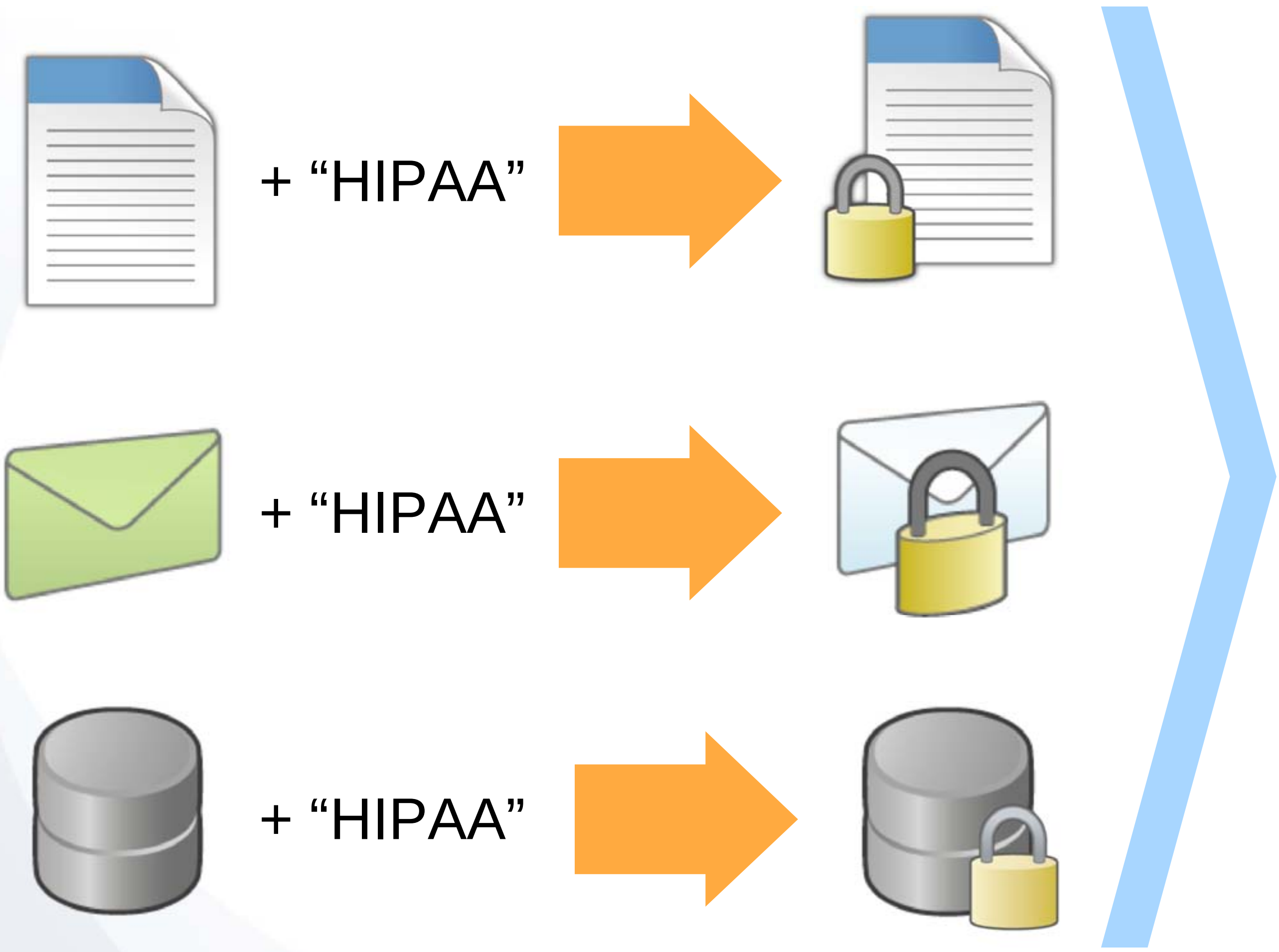
"HIPAA" =
- US access only
- Auth via SecurID
- Log HIPAA event

2 Identify & classify: Determine document contains HIPAA data

3 Apply "HIPAA" privacy policy

4 Enforce "HIPAA" privacy policy

Universal Privacy Enforcement



Privacy Policy Enforced Consistently Regardless of Application or Channel

Data-Centric Security Model

- Focus on the data, not the infrastructure
  - Assume that data can end up anywhere
- Make security travel with the data
  - Data should be protected wherever it lives, inside and outside the network
- Build security into the application layer
  - Don’t rely on surrounding infrastructure to do the right thing

Key Requirements for Data-Centric Security

- Data discovery & classification
  - Need to understand where data is created
  - Drive enforcement policies based on classifications

- Security-integrated application development process
  - Need to incorporate data protection as part of initial design
  - Remediation strategy for existing applications

- ***Centralized key management***
  - Common data protection architecture ensures interoperability across applications
  - Speeds development and deployment

Summary

- Data privacy is a growing regulatory concern
- Technological advancements in PKC and encryption usability now make broad data protection possible
- Implementing a comprehensive, policy based data centric approach drastically simplifies compliance and data protection programs

Questions?

www.voltage.com

Building and Administering Applications

What do architects & developers need to think about?

- PKI model (data-centric):
  - Who should have access to the data?
  - How do I map those access rights to a cert?
  - How do applications find the right cert?
  - How do I ensure cert validity?
  - How do you keep the CA & directory synched?
  - …

- IBE model (data-centric):
  - Who should have access to the data?