

#### Too Many Encryption Keys Los Angeles ISSA July 15, 2009

Brian Tokuyoshi Product Marketing Manager PGP Corporation

btokuyoshi@pgp.com

© 2009 • PGP Corporation • Confidential

und lut Xd4ilaxW3z55zbJnJ1E

#### Agenda

RaRctYkrUxAfnFPpyhTxBCADLb2Sb50 iMm0EnBEGzb50iMm0EnBEGzOv1BCAD Is2U0iMm0EnBEGzOv1BCADPDd1rxLz/

#### **Overview**

f0G34y5BcdFGob7blnRVvU12x4Xv LtJ2lhUbPGPDd1rxLz/8MT2U@iM RChSVvBgkCRYkr97+kCINighrhw

RaRctYkrUxAfnFPpyhTxBCADLb2Sb5@ iMm@EnBEGzb5@iMm@EnBEGzDv1BCAD it2U@iMm@EnBEGzDv1BCADPDd1rxLz/

#### **Market Drivers**

ndEnBEG2Uv18CADLb2SbSdbonkt f0G34y5BcdFGob7blnRVvU12x4Xv LtJ2lhUbPGPDd1rxLz/8MT2U@iM wRaRChSVvBgkCRYkr97+kCINighrhw

RaRctYkrUxAfnFPpyhTxBCADLb2Sb5@ iMm@EnBEGzb5@iMm@EnBEGzOv1BCAD :2U@iMm@EnBEGzOv1BCADPDd1rxLz/ :2Sb5@babR1zfc00G34v5BcdECab2

# Analysts

f0G34y5BcdFGob7binRVvU12x4X LtJ2ihUbPGP≬d1rxLz/&MT2U@iM aRChSVvBgkCRYkr¶7+kCINighrhw

Questions to Ask your Vendor

eachBEG20v1BCADEBESBBBBB CONCOFCdFGob761nRVvU12x4X LtJ21hUbPGPDd1rxLz/8MT2U@iM wRaRChSVvBgkCRYkr97+kCINighrhy

RaRctYkrUxAfnFPpyhTxBCADLb2Sb50 IMm@EnBEGzb50iMm@EnBEGzOv1BCAD :2U@iMm@EnBEGzOv1BCADPDd1rxLz/

#### **Quick Hits**

#dEnBEGzUv1BCADLb2Sb5dbank f0G34y5BcdFGob7LlnRVvU12x4X\ LtJ2lhUbPGPDd1rxLz/&MT2U@iM wRaRChSVvBgkCRYkr97+kCINighrhw

RetYkrUxAfnFPpyhTxBCADLb2Sb5@ IMm@EnBEGzb5@iMm@EnBEGzOv1BCAD :2U@iMm@EnBEGzOv1BCADPDd1rxLz/

#### Conclusions

HQENBEG2UVIBCADLb2Sb5db60 f0G34y5BcdFGob7blnRVvU12x4X LtJ2lhUbPGPDd1rxLz/&MT2UQiM RChSVvBgkCRYkr97+kCINighrhw

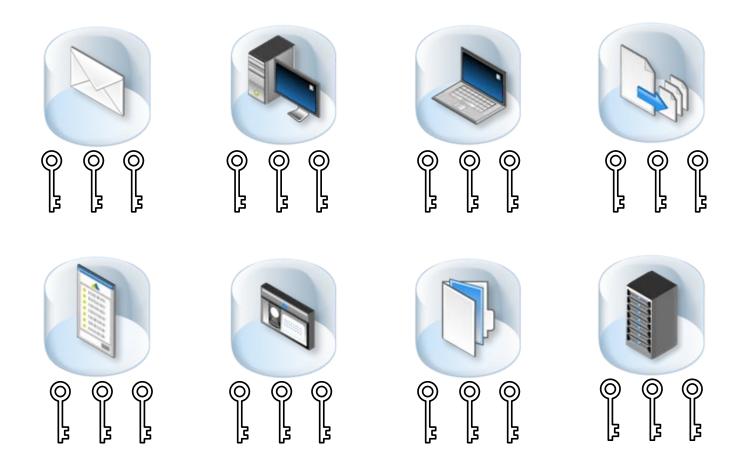
#### PGP

PGP®

---BEGIN PGP MESSAGE oDbyMt2UQiMmQEnBEGZOV 1zff0G34y5BcdFGob7BCAI QbohR1zff0G34y5BcdFGob7 xLz/&MT2UQiMwRaRChSVvB JxAfnFPpyhTxBCADLb2SH3AP Sb5QiMmQEnBEGzb5QiMmQEnF EnBEGzOv1BCADPDd1rxLz/&MT2U ND PGP MESSAGE--

Overview

## **Enterprises Are Here today**





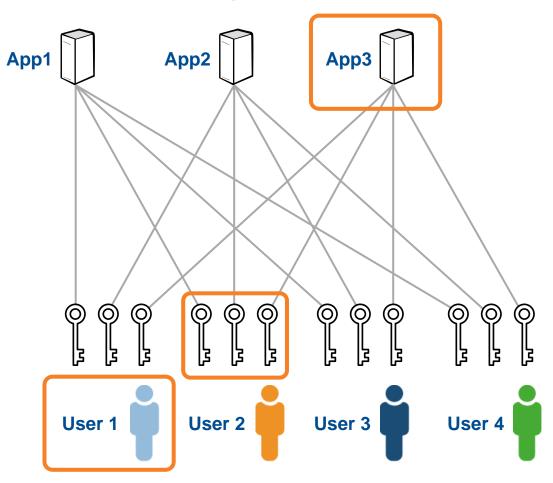
# **Enterprises Say They Are Going To This**



© 2009 • PGP Corporation • Confidential

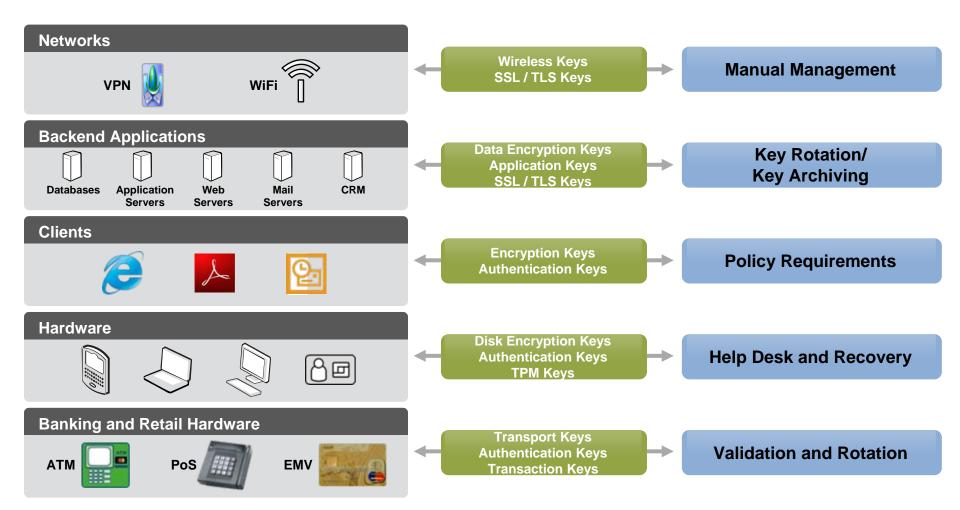
#### **Managing Encryption Is Tough**

#### **Key Management Today**



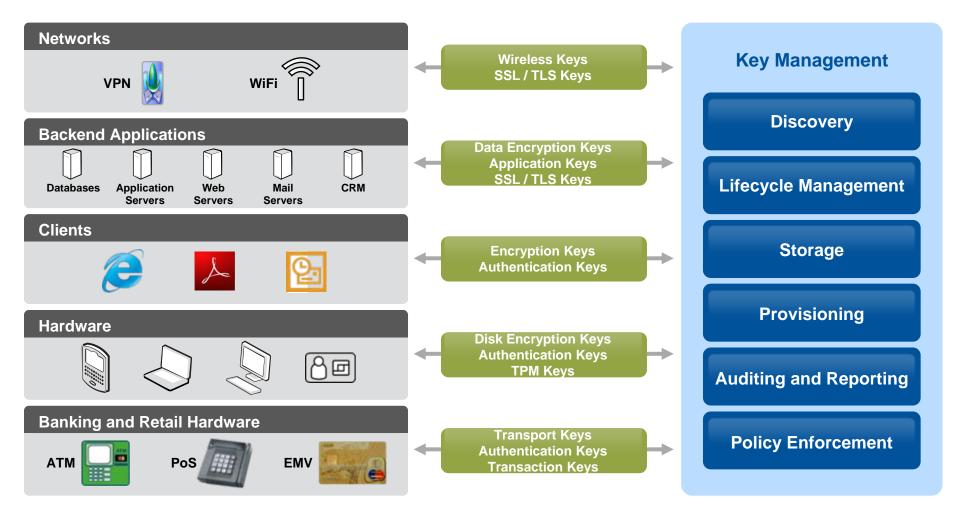


#### **Common Problems with Keys**





#### **Addressing the Problem**





PGP®

---BEGIN PGP MESSAGE oDbyMt2UQiMmQEnBEGzOv lzff0G34y5BcdFGob7BCAI QbohRlzff0G34y5BcdFGob7 xLz/&MT2UQiMwRaRChSVvBr uxAfnFPpyhTxBCADLb2SH3AP Sb5QiMmQEnBEGzb5QiMmQEnF Sb5QiMmQEnBEGzb5QiMmQEnF Sb5QiMmQEnBEGzb5QiMmQEnF

#### **Market Drivers**

# **Compliance!**

# **Data Breaches!**

Compliance and protection from data breaches are not the drivers for Enterprise Key Management

Deploying encryption without good key management is causing the problem.

- Tight deadlines place emphasis on the goal, without considering the ramifications about the path taken
- Compliance only talks about getting the data encrypted, not how fast it should be decrypted. That's e-discovery.
- The coming hangover
  - Key Management is often done poorly
  - No overall strategy
  - GAO report on Federal efforts for DAR
  - Enterprise is next
- Deploying encryption without a plan to manage keys is the driver for enterprise key management



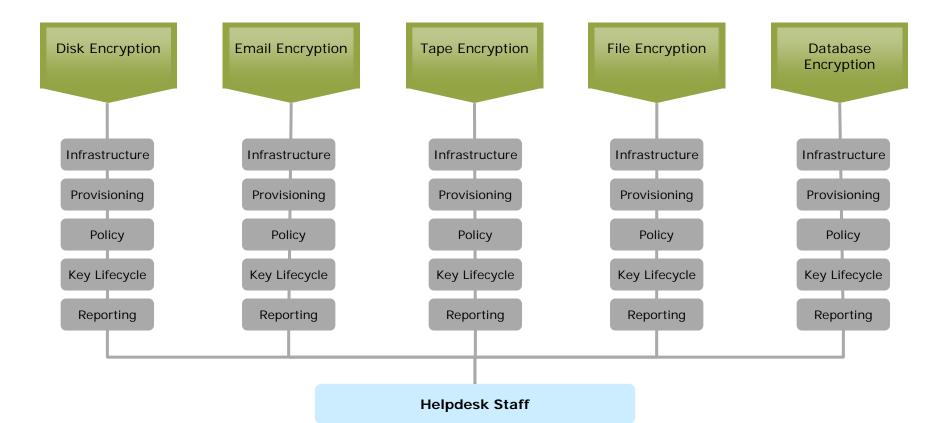
#### **Best Practices**

| 1 | Survey and catalog existing data            |
|---|---|
| 2 | Plan your long term encryption requirements |
| 3 | Develop an enterprise policy on keys        |
| 4 | Deploy a framework to manage encryption     |
| 5 | Deploy data protection solution             |
| 6 | Tackle the next project                     |



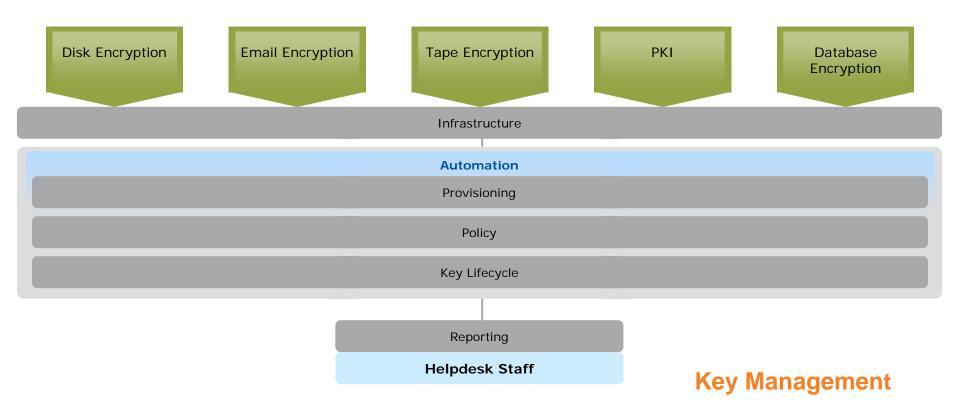
#### **Key Management Silos**

#### **Point Product Proliferation**



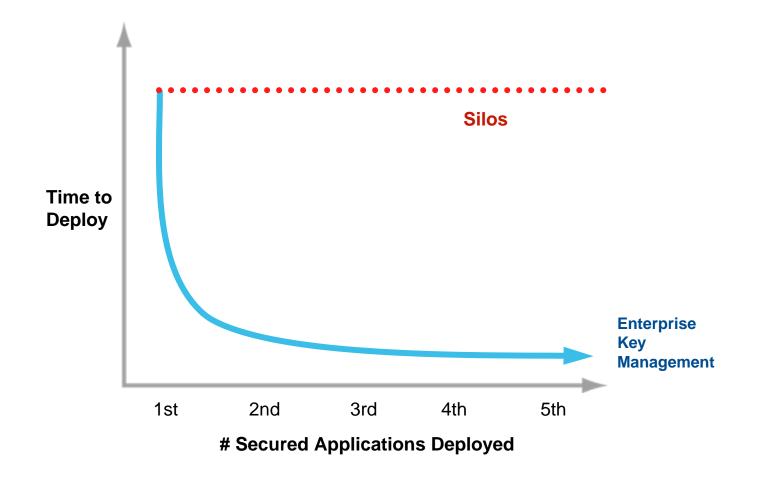


#### **A Common Infrastructure**





#### **Effort Comparison**





- Makes encryption manageable
- Replaces custom tools
- Protects business continuity by eliminating mistakes from inadvertent key expiration
- Reduces administrative cost
- Provides the foundation for new initiatives

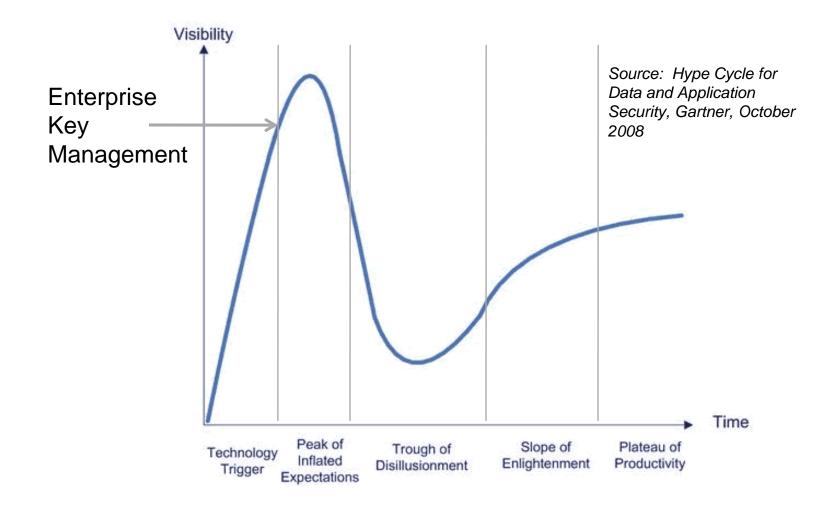


PGP®

---BEGIN PGP MESSAG oDbyMt2UQiMmQEnBEGzO lzff0G34y5BcdFGob7BCA QbohRlzff0G34y5BcdFGob xLz/&MT2UQiMwRaRChSVvBr UxAfnFPpyhTxBCADLb2SH3AP Sb5QiMmQEnBEGzb5QiMmQEnF EnBEGzOv1BCADPDdlrxLz/&MT2Ur ND PGP MESSAGE--

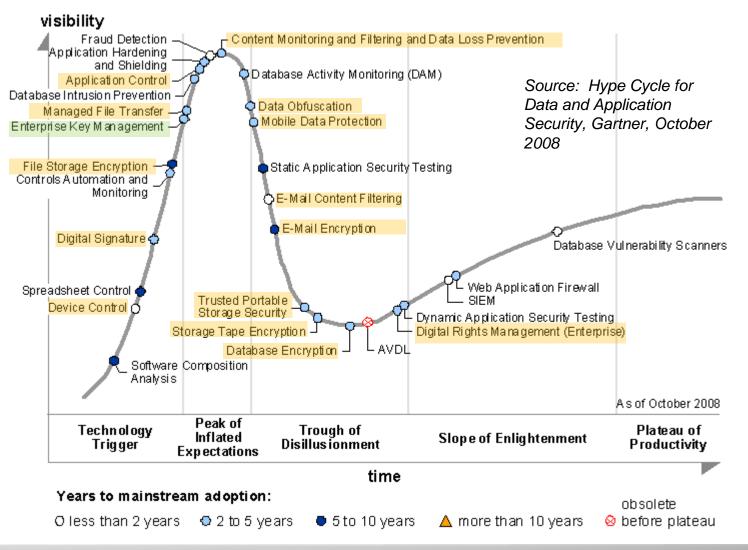
## Analysts

#### **Gartner Hype Cycle**





#### **Gartner Hype Cycle**





#### **Forrester Research**

#### Will pilot or adopt in Source: The Enterprise IT the next 12 months Already adopted Security Buyer Profile:2009. High spenders 50% 18% Forrester Research, May 13, **Email encryption** 14% 44% Low spenders 2009 22% 49% Network storage encryption 13% 40% 25% 47% Information/data leak protection 22% 34% 24% 43% Application encryption platform 21% 33% 21% 39% Desktop full disk encryption 19% 31% 23% 20% 39% Enterprise key management solution 30% 20% 38% Digital rights management 17% 28% 23% 35% Public key infrastructure technology 17% 27%

#### "What is your organization's interest in adopting each of the following data security technologies?"

Base: 260 North American and European enterprise IT security decision-makers Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2008

High spenders defined as spending > %12.6 of budget on security



#### **Trust Catalyst**



Figure 4: How much time has your organization spent preparing for key management issues?

Source: 2008 Encryption and Key Management Industry Benchmark Report, Trust Catalyst, October 2008



PGP

---BEGIN PGP MESSAG oDbyMt2UQiMmQEnBEGZO 1zff0G34y5BcdFGob7BCA QbohR1zff0G34y5BcdFGob7 xLz/&MT2UQiMwRaRChSVvB JxAfnFPpyhTxBCADLb2SH3AP Sb5QiMmQEnBEGzb5QiMmQEnF EnBEGzOv1BCADPDd1rxLz/&MT2U ND PGP MESSAGE--

# Questions to Ask your Key Management Vendor

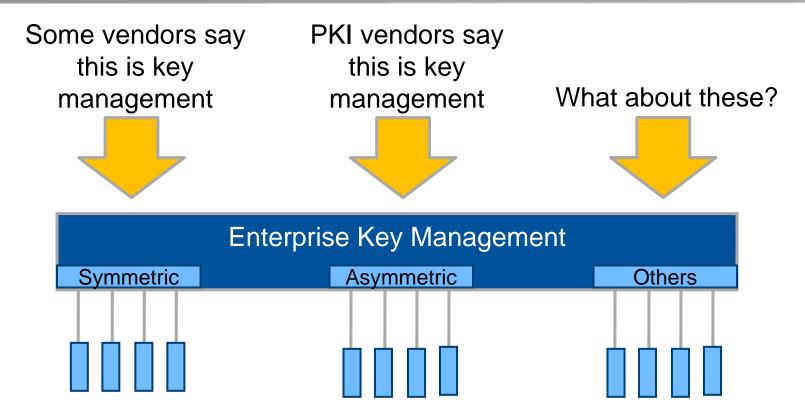
Is it key management or ENTERPRISE key management?

- There are many products that offer key management
  - Few are enterprise key management
  - Some are silos in disguise (key management appliances)
  - Doesn't mean they are not valuable. But it's not enterprise key management.



Are you talking about symmetric or asymmetric keys?

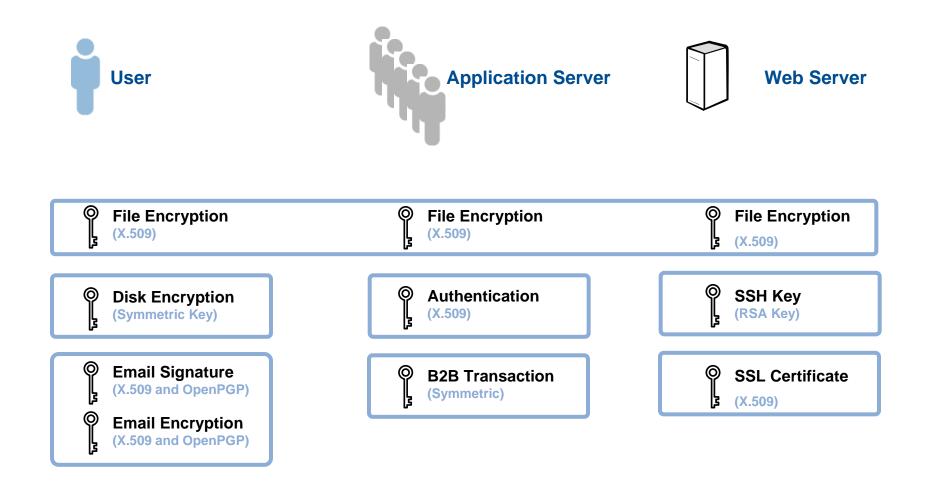
#### Symmetric / Asymmetric





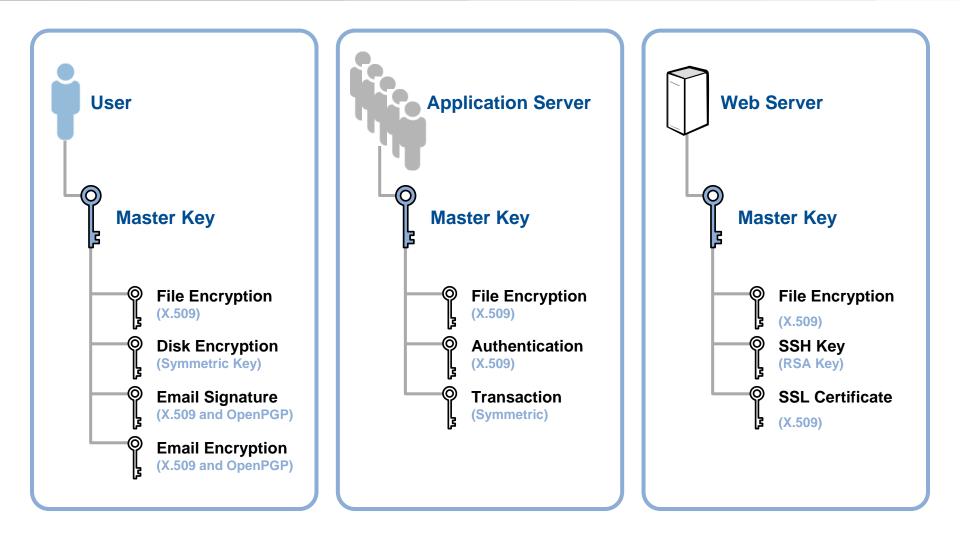
#### How do you handle keys in context?

#### **Key Organization without Key Management**





#### **Group Related Keys Together**

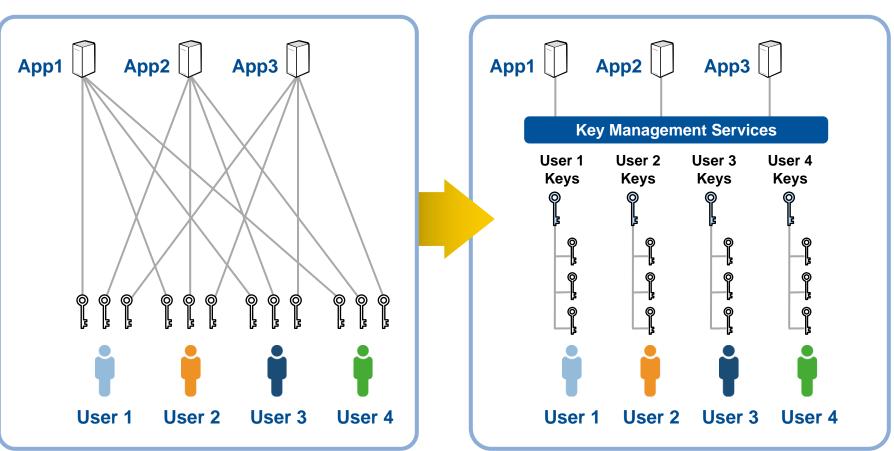




#### **Before and After**

#### Without Key Management

With Key Management





PGP®

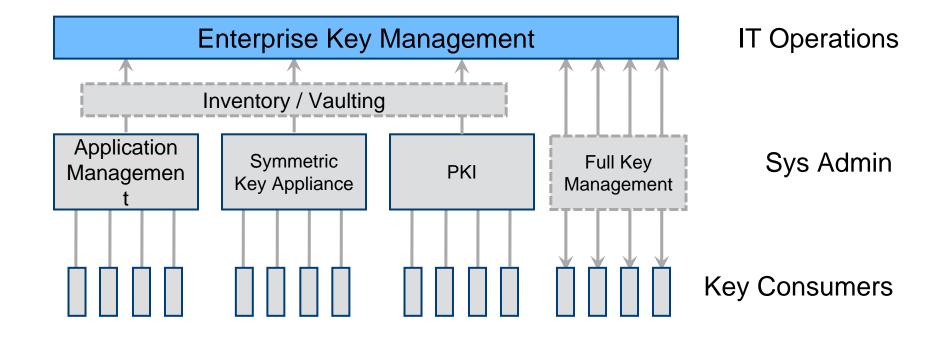
---BEGIN PGP MESSAG oDbyMt2UQiMmQEnBEGZD 1zff0G34y5BcdFGob7BCA QbohR1zff0G34y5BcdFGob xLz/&MT2UQiMwRaRChSVvB UxAfnFPpyhTxBCADLb2SH3AP Sb5QiMmQEnBEGzb5QiMmQEnF EnBEGzOv1BCADPDd1rxLz/&MT2U/ ND PGP MESSAGE--

# Quick Hits Use Cases That You can Use

#### **Key Inventory**

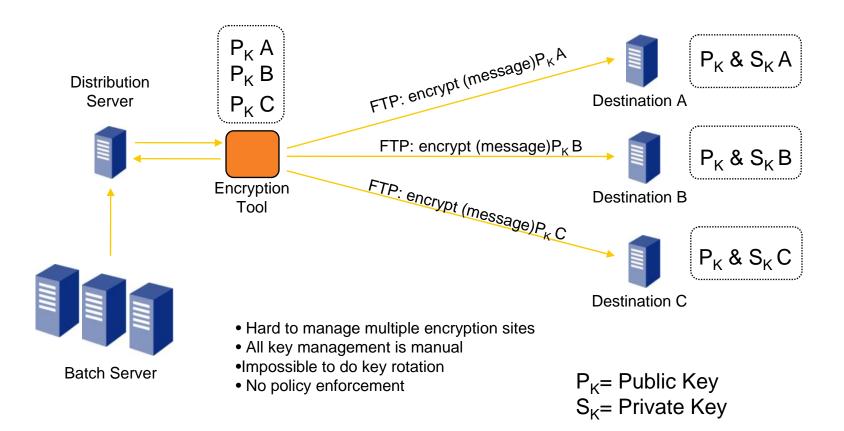
|                     | lessage   | / - Message (HTML) | -             | =     | ×  |
|---------------------|---|--------------------|---------------|-------|----|
| You replie          | ed on 5/4/2009 6:01 PM.   |                    |               |       |    |
| From:<br>To:<br>Cc: | Cali Martin   | Sent:              | Tue 4/21/2009 | 11:31 | AN |
| Subject:            | Key inventory   |                    |               |       |    |
| office o            | doing an inventory of all our keys that<br>r any other building key (not furniture )<br>on the key. |                    |               |       |    |
|                     |   |                    |               |       |    |





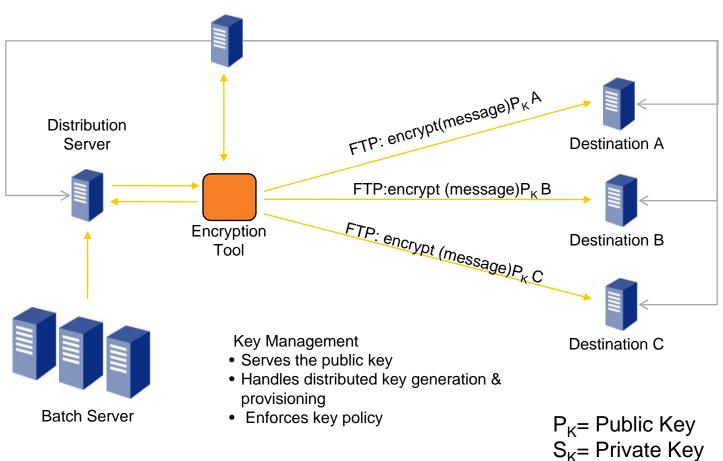


#### **File Distribution**





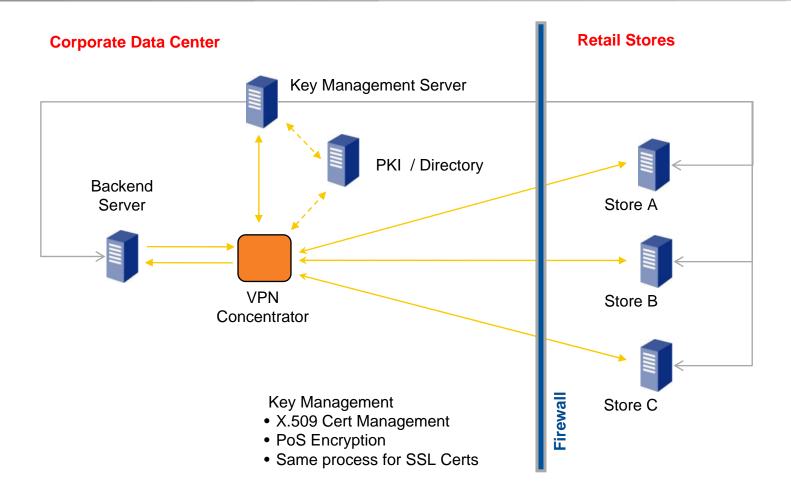
#### **Secure File Distribution (Encryption)**



Key Management Server



#### **VPN / SSL Certificate Management (Authentication)**





PGP®

---BEGIN PGP MESSAGE oDbyMt2UQiMmQEnBEGzOv lzff0G34y5BcdFGob7BCAI QbohRlzff0G34y5BcdFGob7 xLz/&MT2UQiMwRaRChSVvBr uxAfnFPpyhTxBCADLb2SH3AP Sb5QiMmQEnBEGzb5QiMmQEnF Sb5QiMmQEnBEGzb5QiMmQEnF Sb5QiMmQEnBEGzb5QiMmQEnF

## Conclusions

- 1. Add Enterprise Key Management to the environment that you have
  - Inventory / Vaulting alone solves a critical issue with key recovery
  - Positions you to get ready for future challenges
- 2. Build flexible key management infrastructure and build on top of it
  - Got to start somewhere
  - Starting with a good foundation helps to address future challenges



#### **Points to Consider** From 10+ Years of Managing Keys & Applications

- Symmetric & Asymmetric are both part of a key management strategy
  - Key lifecycle management needed for both
  - No single key type
  - No single format
  - No single protocol
- Applications are not good key managers
  - Overlay needed not just a database

- Keys in Context
- Basic Key Management Services
  - Discovery
  - Lifecycle Management
  - Provisioning
  - Storage
  - Auditing & Reporting
  - Policy
- Must adapt to wide range of use cases, with implementation flexibility
  - Corporate recovery
  - Access Control
  - Extensible integration
  - No single Key Management Protocol





# Thank You



© 2009 • PGP Corporation • Confidential