Encrypt Your Cloud

Davi Ottenheimer
flyingpenguin

Session ID: DAS-210

Session Classification: Advanced

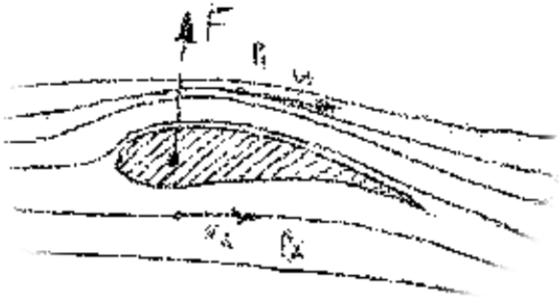
RSACONFERENCE
EUROPE 2012

AGENDA

- Introduction
- Cryptography Keys in Clouds
- Examples

Introduction

flyingpenguin
the poetry of information security



flying \fly"ing\, a. [From fly, v. i.]

moving with, or as with, wings; moving lightly or rapidly; intended for rapid movement

penguin \pen"guin\, n.

short-legged flightless birds of cold southern especially Antarctic regions having webbed feet and wings modified for water

Cloud

- “The web’s household names got where they are today by mining the information that their users generate and turning it into business advantage.”

The Harsh Light of Data Presentation, O’Reilly Strata Jumpstart 2011 conference

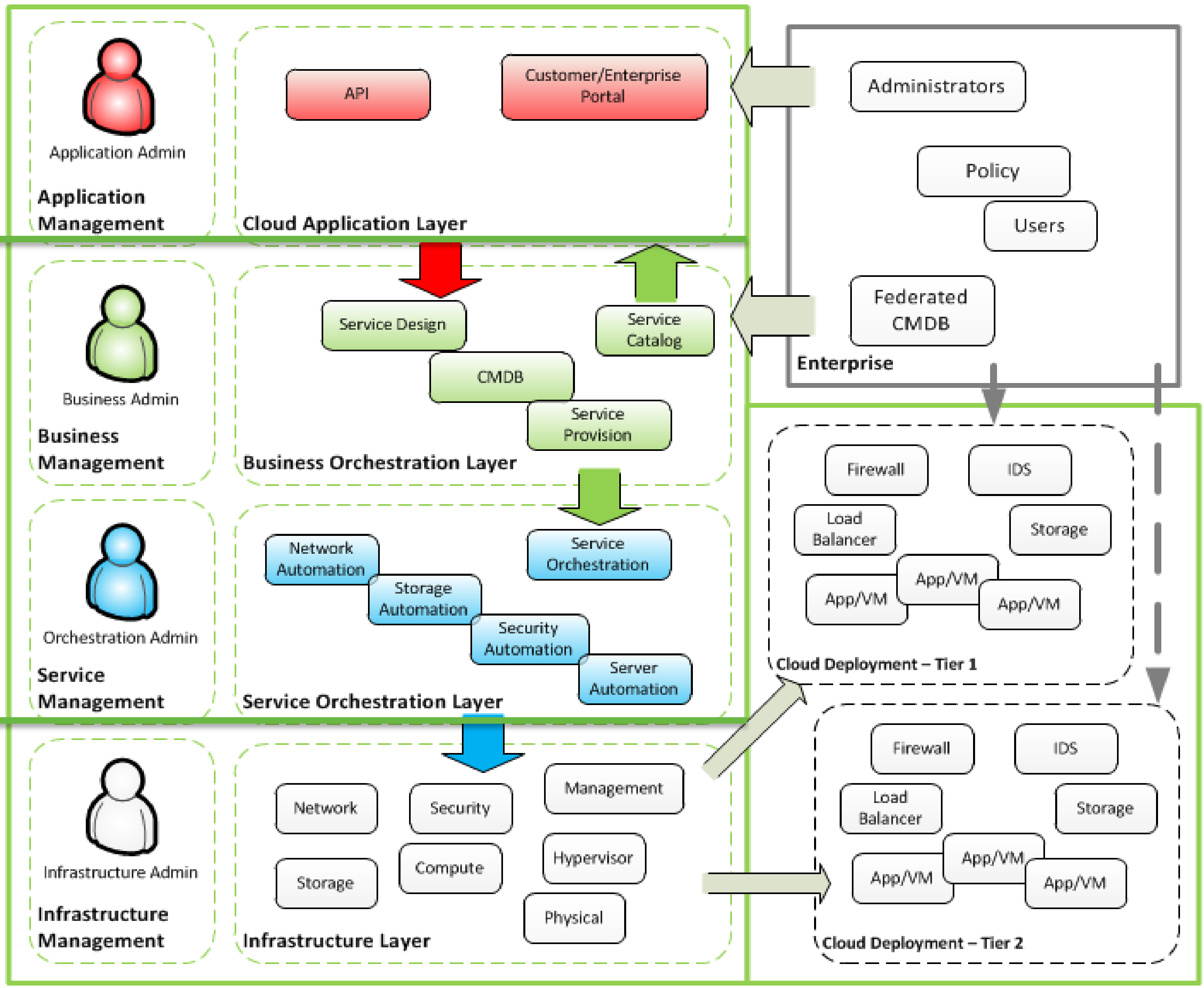
- “The top issue overall was a perceived lack of security and service level agreements (SLAs), with 45% of respondents referring to it.”

http://www.interxion.com/cloud-insight/index.html

Cloud

Software

Platform



Application Admin

Application Management

API

Customer/Enterprise Portal

Cloud Application Layer

Business Admin

Business Management

Service Design

Service Catalog

CMDB

Service Provision

Business Orchestration Layer

Orchestration Admin

Service Management

Network Automation

Storage Automation

Security Automation

Server Automation

Service Orchestration

Service Orchestration Layer

Infrastructure Admin

Infrastructure Management

Network

Security

Management

Storage

Compute

Hypervisor

Physical

Infrastructure Layer

Administrators

Policy

Users

Federated CMDB

Enterprise

Firewall

IDS

Load Balancer

Storage

App/VM

App/VM

App/VM

Cloud Deployment – Tier 1

Firewall

IDS

Load Balancer

Storage

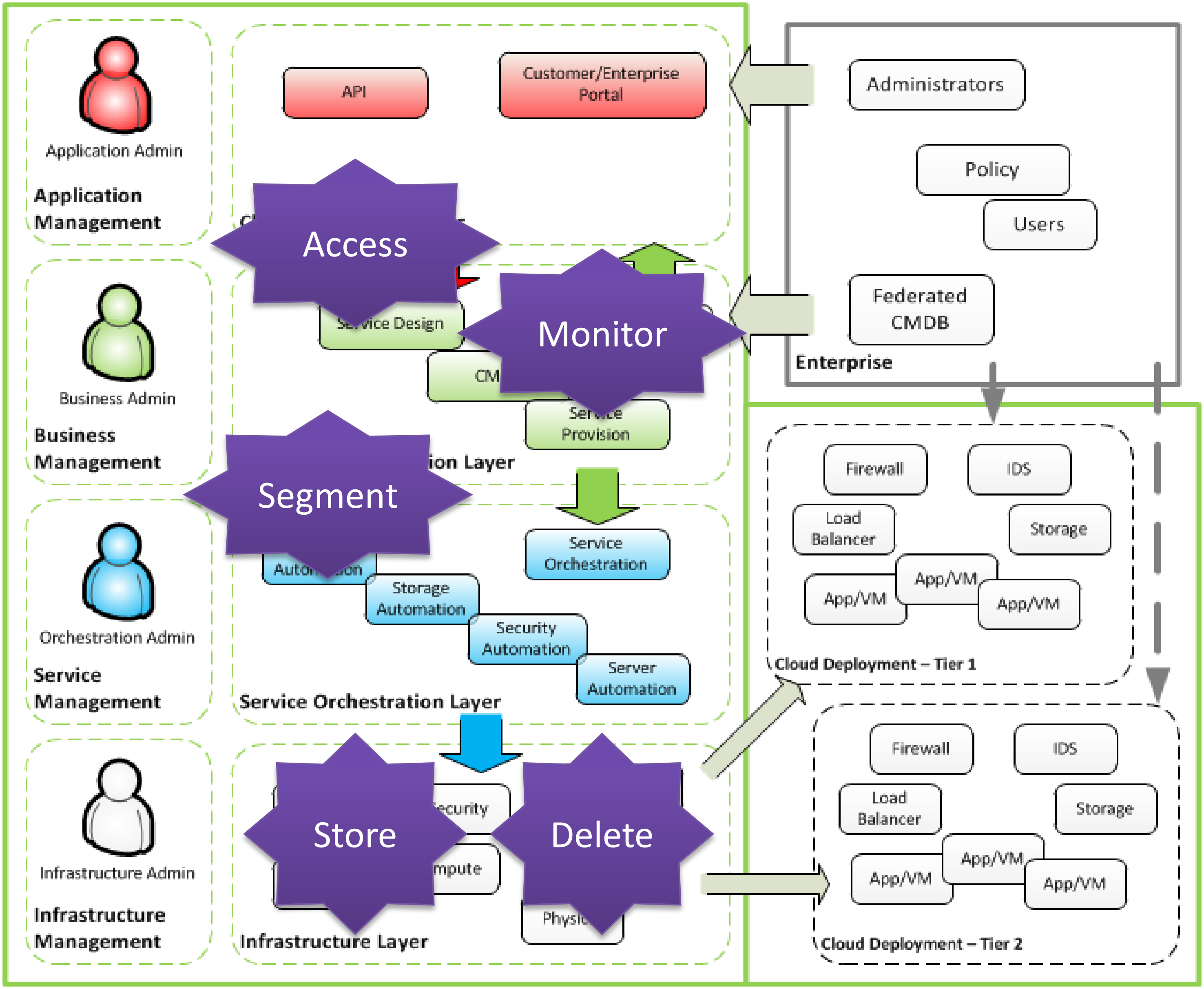
App/VM

App/VM

App/VM

Cloud Deployment – Tier 2

Cloud


API
Customer/Enterprise Portal
Application Admin
Application Management
Administrators
Policy
Users
Federated CMDB
Enterprise
Access
Monitor
Business Admin
Business Management
Service Design
CM
Service Provision
ion Layer
Segment
Service Orchestration
Autom tion
Storage Automation
Security Automation
Server Automation
Orchestration Admin
Service Management
Service Orchestration Layer
Firewall
IDS
Load Balancer
Storage
App/VM
App/VM
App/VM
Cloud Deployment – Tier 1
Store
Delete
ecurity
mpute
Physic
Infrastructure Admin
Infrastructure Management
Infrastructure Layer
Firewall
IDS
Load Balancer
Storage
App/VM
App/VM
App/VM
Cloud Deployment – Tier 2

Cloud

CIOs Worry About…

Outsourced Responsibilities

- "Due-diligence"
- Reasonable

Photo © 2012 Davi Ottenheimer

CIOs *Need* Cloud Security Controls

	Want	Need
1	Data Deletion	Secure Wipe (Key Deletion)
2	Boundary Definition	Segmentation (Encryption)
3	Data Access (Apps)	Input Validation
4	Access Monitoring	Log Management
5	Data Storage	Encryption (Key Management)

> **"Key management is the hardest part of cryptography and often the Achilles' heel of an otherwise secure system."**
>
> — Bruce Schneier, Preface to Applied Cryptography, Second Edition

Crypto Terminology

- **Encryption**: *reversible* operation, cryptographically turns input into illegible cipher text
- **Hashing**: *non-reversible* operation, cryptographically transforms input to illegible message
- **Tokenization**: reversible operation, substitutes input with data that has no inherent value
- **Key management**: life-cycle of a secret including creation, distribution, use and deletion

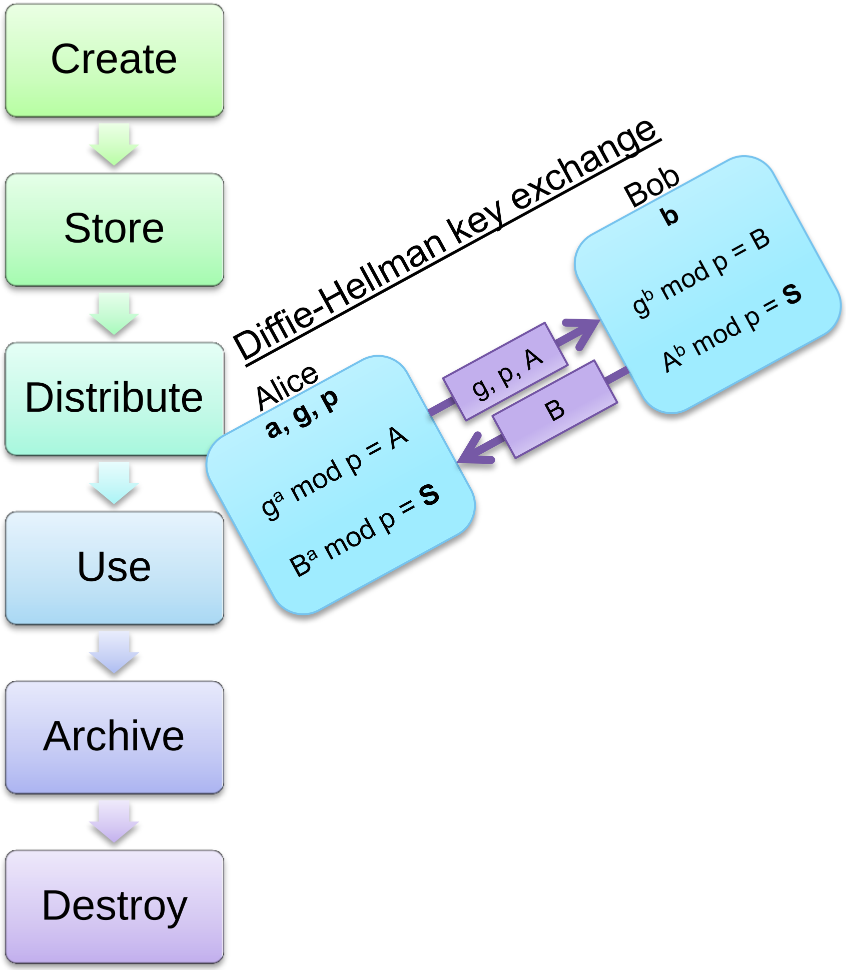
Crypto Considerations

- **Encryption**: *reversible* operation, cryptographically turns input into illegible cipher text
- **Hashing**: *non-reversible* operation, cryptographically transforms input to illegible message
- **Tokenization**: reversible operation, substitutes input with data that has no inherent value
- **Key management**: life-cycle of a secret including creation, distribution, use and deletion

Cryptography in Clouds

Crypto Considerations

- Human/Social element
  - People
  - Process
  - Policy
- Location element
  - Border restrictions
  - Standards (U.S. NIST)
    - SP 800-57
    - SP 800-131A
    - SP 800-130



Create

Store

Distribute

Use

Archive

Destroy

Diffie-Hellman key exchange

Alice

a, g, p

$g^a \bmod p = A$

$B^a \bmod p = \mathbf{S}$

g, p, A

B

Bob

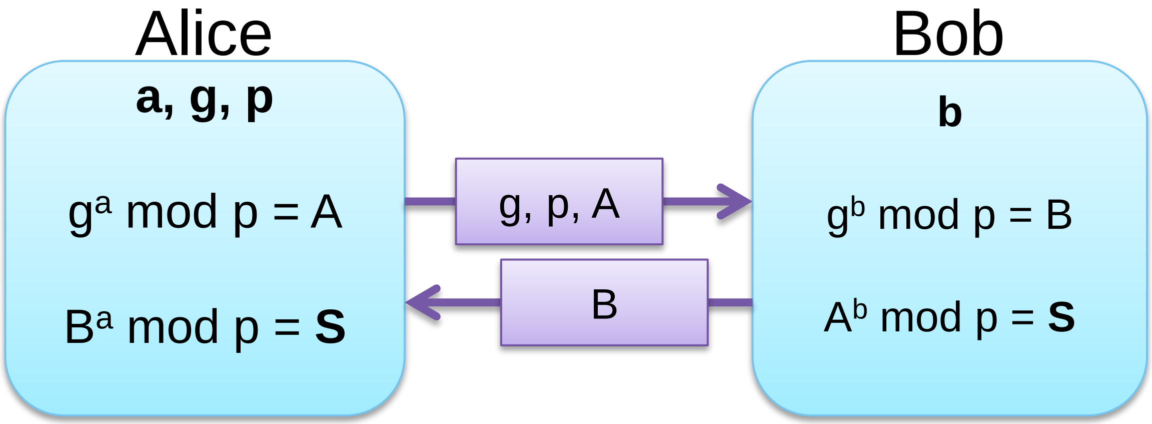
b

$g^b \bmod p = B$

$A^b \bmod p = \mathbf{S}$

Crypto Considerations

Diffie-Hellman key exchange



Alice

a, g, p

$g^a \bmod p = A$

$B^a \bmod p = \mathbf{S}$

g, p, A

B

Bob

b

$g^b \bmod p = B$

$A^b \bmod p = \mathbf{S}$

Cloud Crypto Considerations

Who has your keys?

- Human/Social element
  - People
  - Process
  - Policy
- Location element
  - Border restrictions
  - Standards (U.S. NIST)
    - SP 800-57
    - SP 800-131A
    - SP 800-130

Trusted Service Provider

Architecture

Large / Global Presence

Interoperability

Cloud Crypto Considerations

- “Portable device” technology (MA 201 CMR 17)
- Multi-tenant
- Open interfaces
  - Consumer
  - Management
  - Partner
  - Development / Application
- Multi-jurisdiction
  - Who/when
  - Where

Encryption as a Service

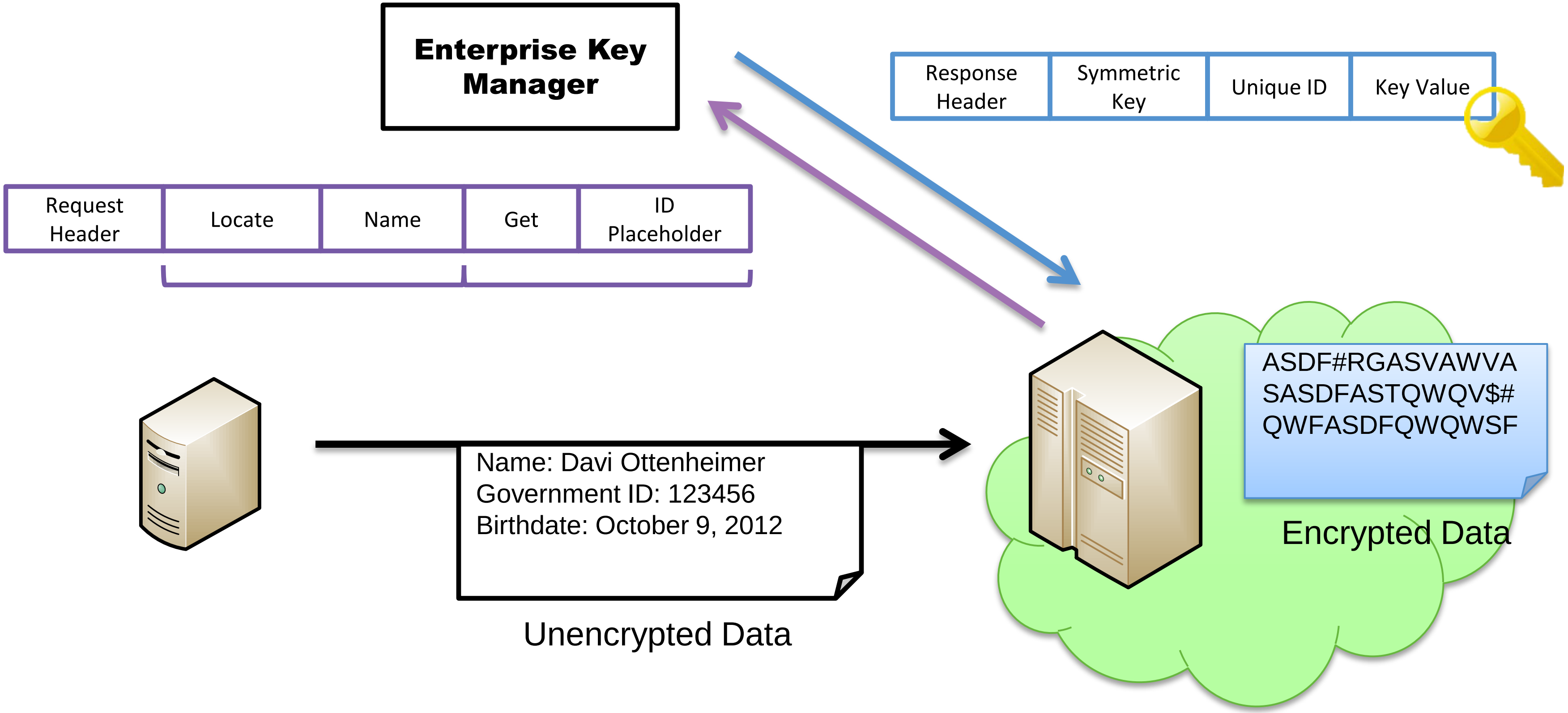
- Key management
  - Generation
  - Protection (key encryption key)
  - Expiration and Rotation
  - Deletion
- Key architecture
  - Management integration
  - Interoperability
  - Meta-data

Standards:

ANSI X9.24
ISO 11568
ISO 11770
NIST SP 800-57
IETF Keyprov
IEEE P1619.3
W3C XKMS
OASIS EKMI
OASIS KMIP

Encryption as a Service

Key Management Interoperability Protocol (KMIP)



Enterprise Key Manager

Response Header	Symmetric Key	Unique ID	Key Value

Request Header	Locate	Name	Get	ID Placeholder

Name: Davi Ottenheimer
Government ID: 123456
Birthdate: October 9, 2012

Unencrypted Data

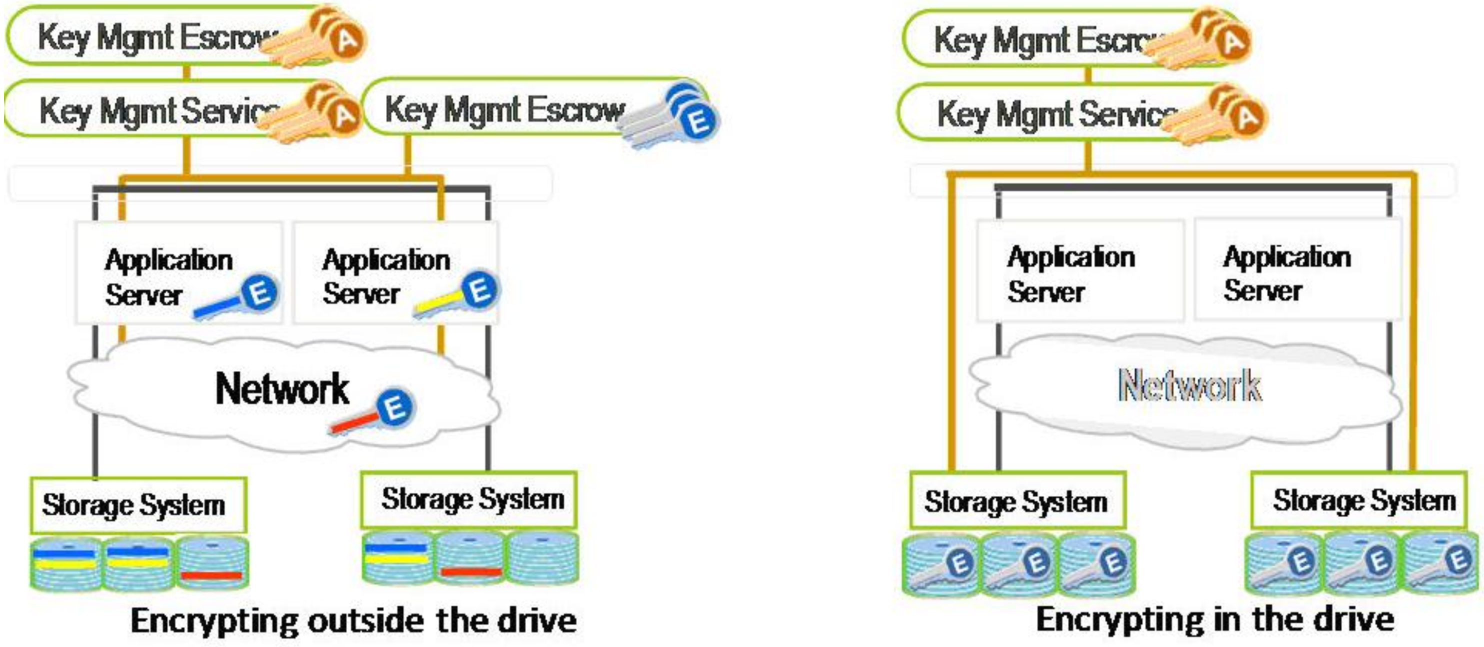
ASDF#RGASVAWVA
SASDFASTQWQV$#
QWFASDFQWQWSF

Encrypted Data

http://xml.coverpages.org/KMIP/KMIP-WhitePaper.pdf

Encryption as a Service

Enterprise Key Management Infrastructure (EKMI)



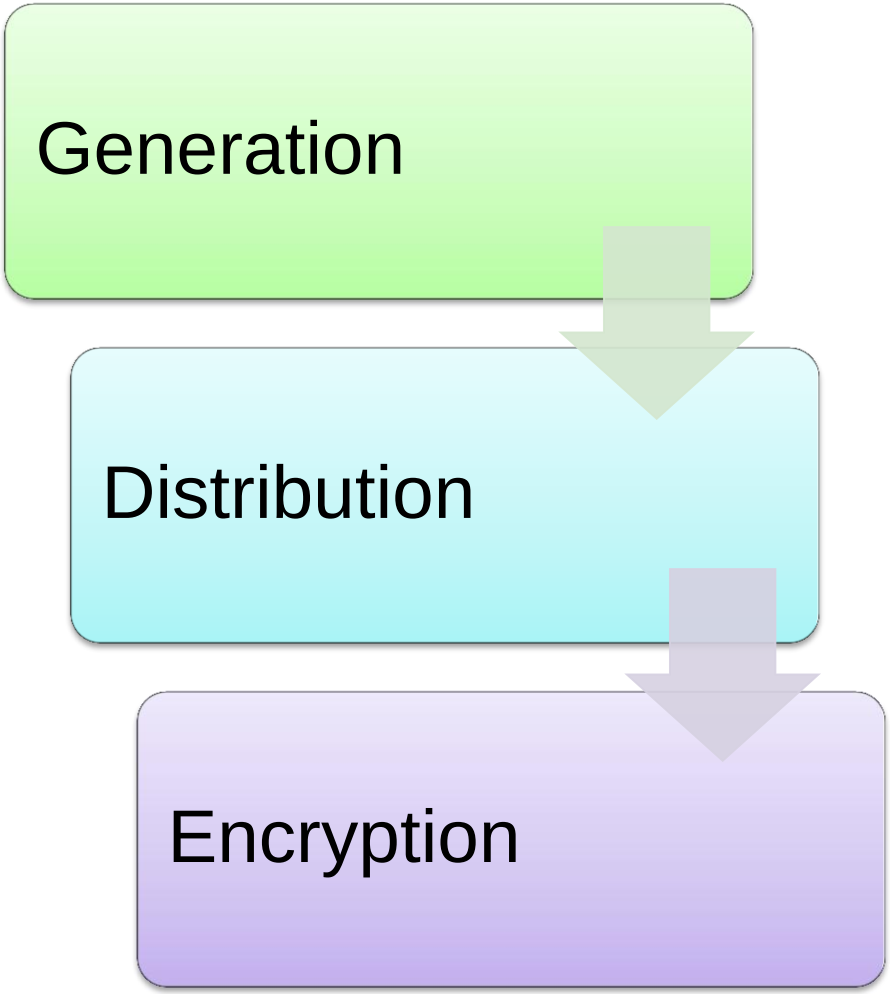
(a)

(b)

https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi

Examples

Example #1



Generation

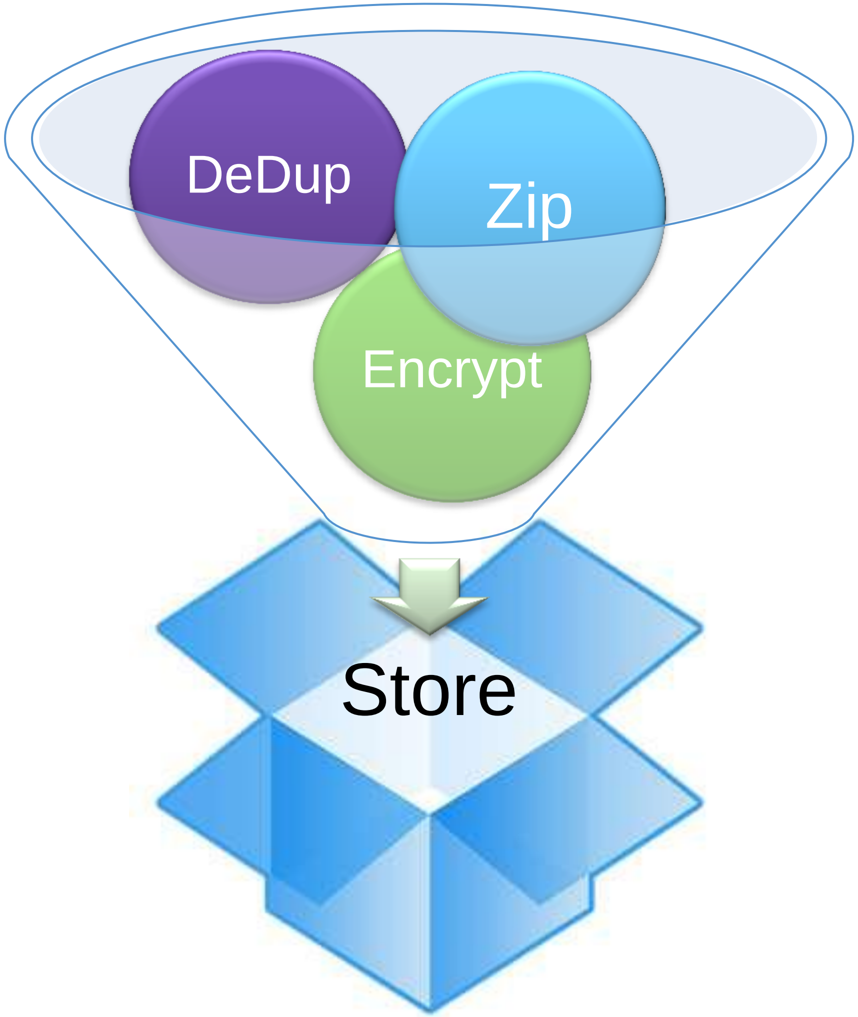
Distribution

Encryption

- Key Rotation
  - Templates
  - Snapshots
  - Offline
- Key Persistence
  - Templates
  - Snapshots
  - Reboot
  - SAN
  - Backup
  - Archive

Example #2

1. Encrypt Data
2. “Manage” Data…?
   - Analysis
   - Reports
   - Compression
   - De-duplication



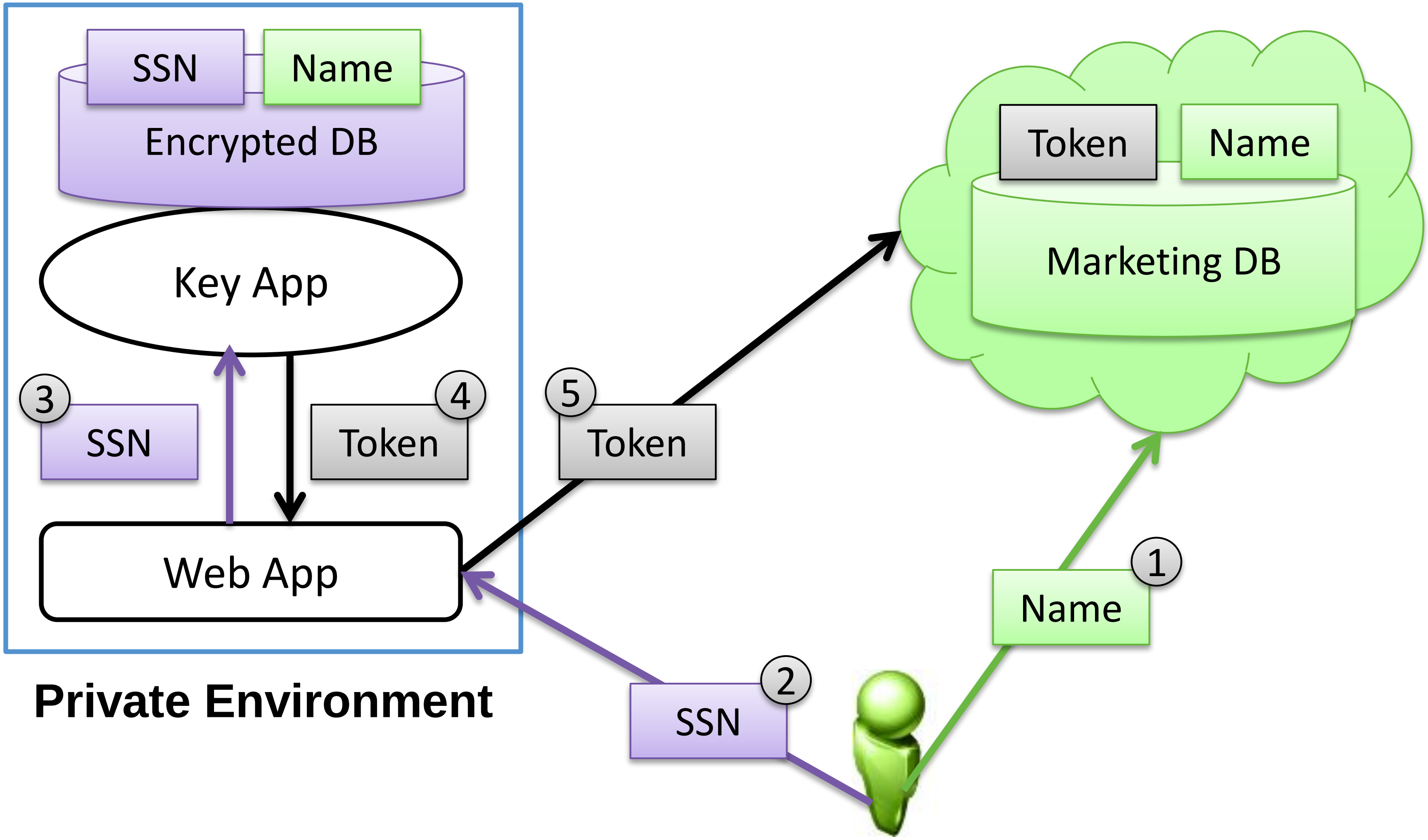
Example #3

Segmentation

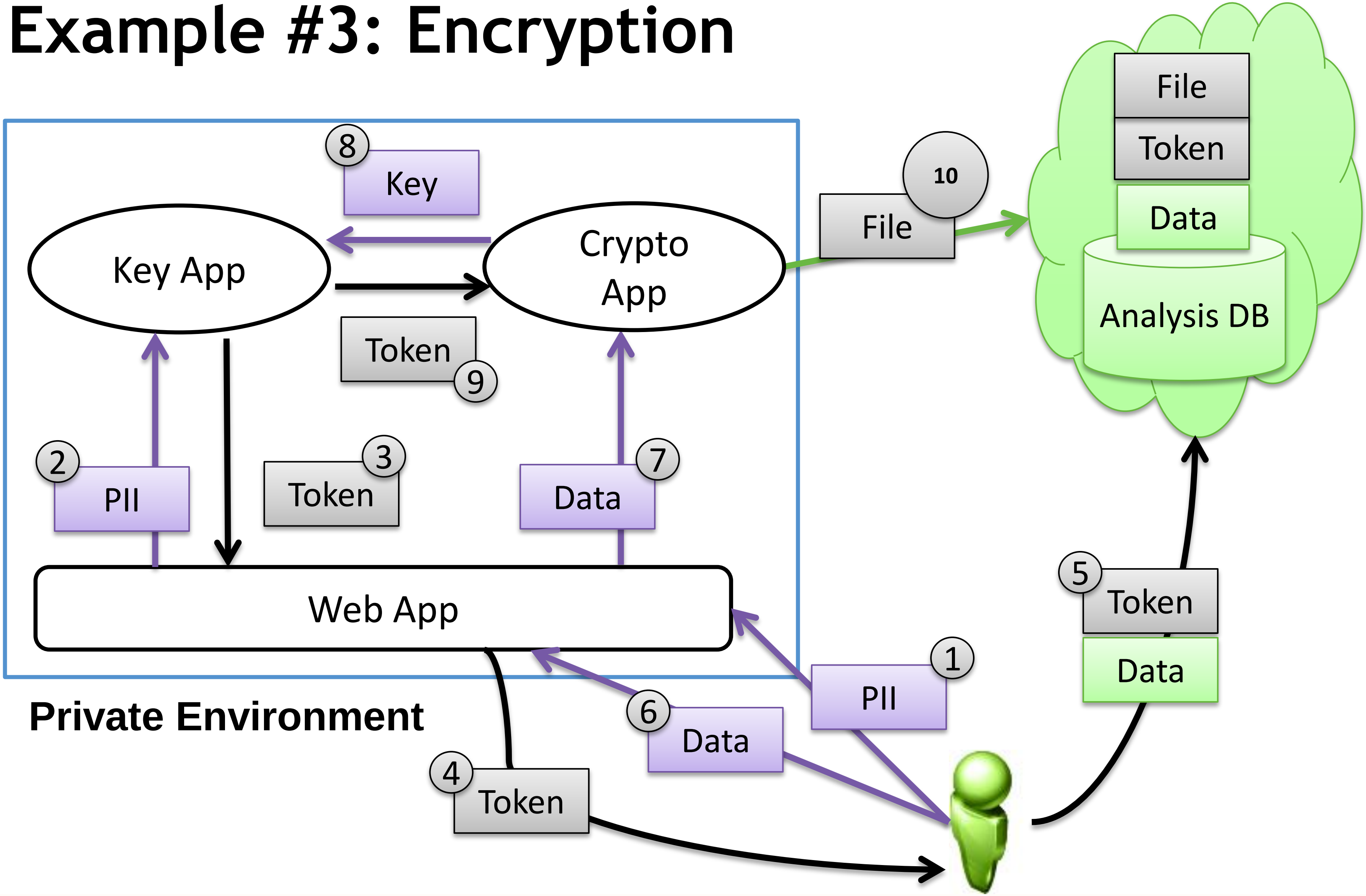
- Default
- Sensitive un-regulated (e.g. non-“material”)
- Sensitive regulated (e.g. PII, CCN, “material”)

Data Level	Treatment
3	Clear
2	Token or Encrypted
1	Token, Hashed or Encrypted

Example #3: Token



Example #3: Encryption



Private Environment

Apply

- Next 3 months
  - Classify data for segmentation
  - Setup key management policy and procedures
  - Select standards for interoperability
- Next 6 months
  - Configure apps for key and crypto management
  - Select a key app and crypto app solution
  - Plan and initiate a project to protect data in cloud

Encrypt Your Cloud

Davi Ottenheimer
flyingpenguin

Session ID: DAS-210

Session Classification: Advanced

RSA CONFERENCE
EUROPE 2012