对云进行加密

Davi Ottenheimer
flyingpenguin

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

议程

- 简介
- 云中的加密技术
- 示例

简介

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

flyingpenguin
the poetry of information security

flying \fly"ing\, 会飞的，形容词，[由不及物动词 fly 转化而来]

使用翅膀移动或随翅膀一起移动；轻盈或快速地移动；意在快速移动

penguin \pen"guin\, 企鹅，名词

生长在寒冷的南半球（尤其是南极地区）的一种不会飞的短腿鸟，长有能够适应水中环境的有蹼的脚和翅膀

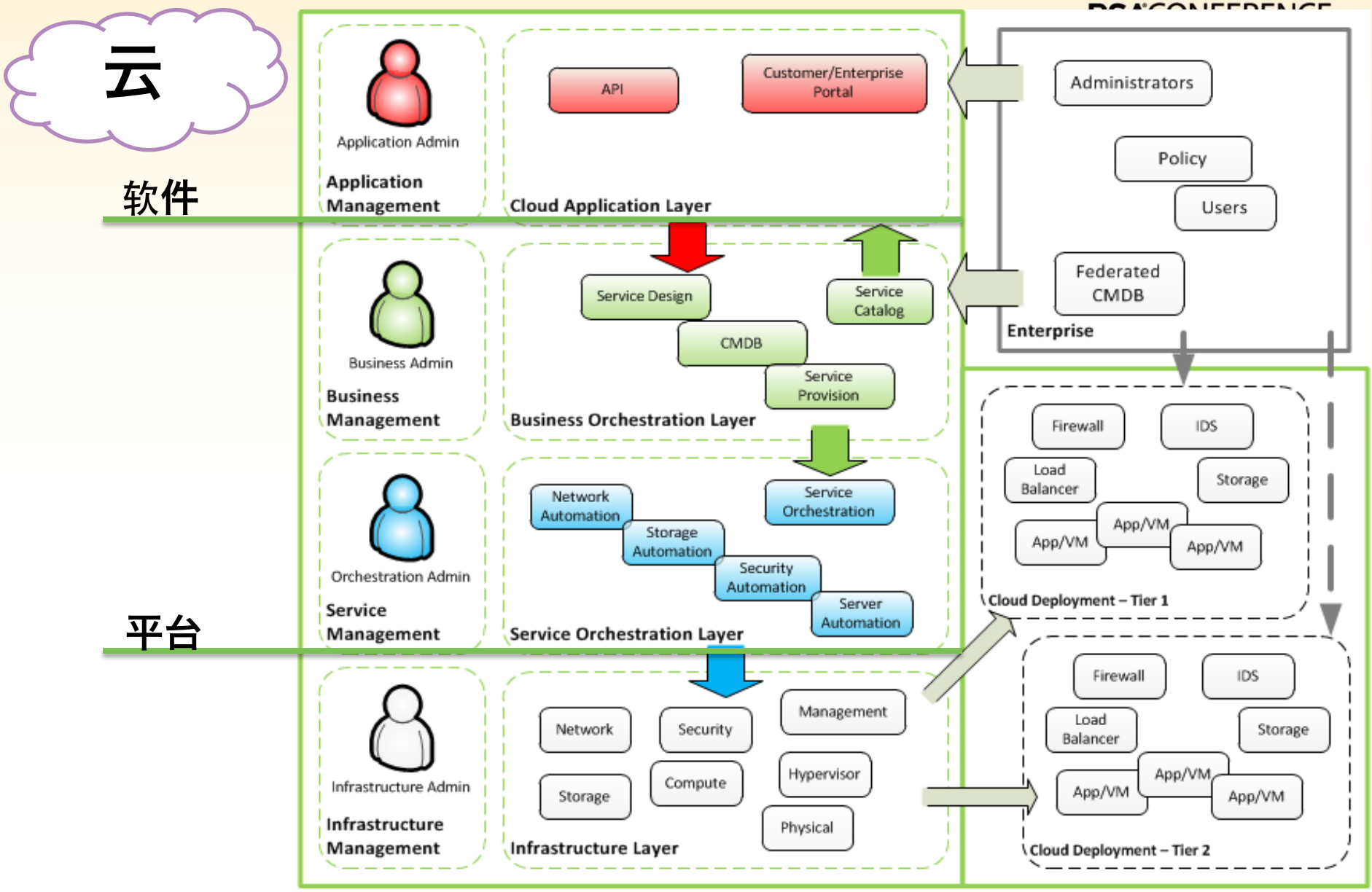
云

- “网络上一些家喻户晓的企业都是通过挖掘其用户生成的信息并将这些信息转换为业务优势而取得成功的。”

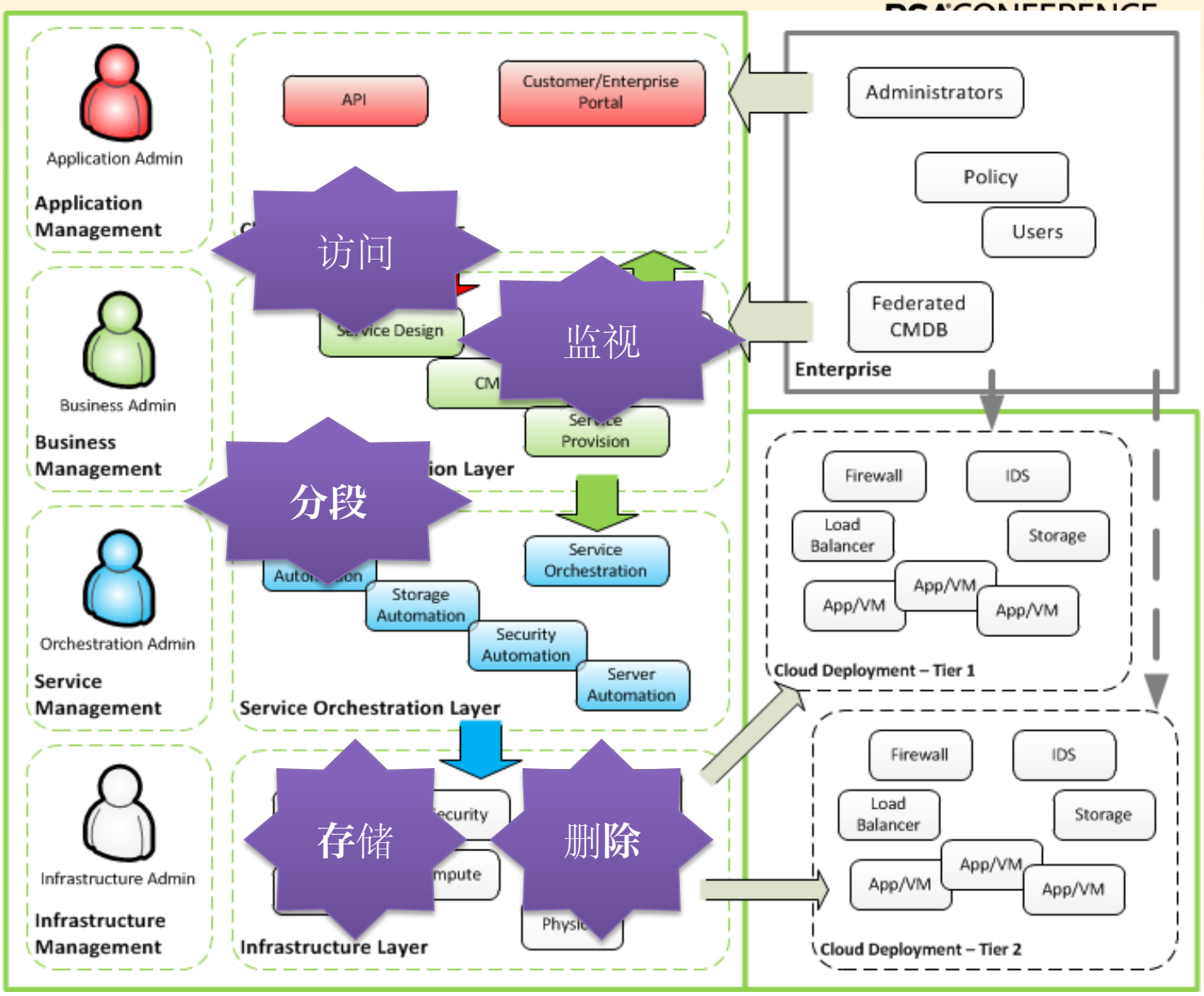
数据呈现的亮点，O’Reilly Strata Jumpstart 2011 大会

- “总体来说，最重要的问题是缺乏安全观和服务级别协议 (SLA)，45% 的受访者提到这一点。”

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


云
软件
平台
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

云


Application Admin
Application Management
Business Admin
Business Management
Orchestration Admin
Service Management
Infrastructure Admin
Infrastructure Management
API
Customer/Enterprise Portal
访问
监视
分段
存储
删除
Service Design
CM
Service Provision
Service Orchestration
Storage Automation
Security Automation
Server Automation
Service Orchestration Layer
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


云

CIO 们担心...

外包职责

- “恪尽职守”
- 合理

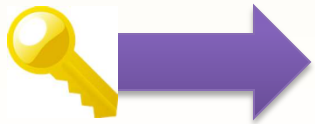
Photo © 2012 Davi Ottenheimer

CIO 们*需要*云控制权

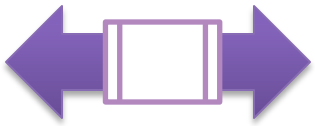
	目的	措施
1	数据删除	安全擦除（密钥删除）
2	边界定义	分段（加密）
3	数据访问（应用程序）	输入验证
4	访问监视	日志管理
5	数据存储	加密（密钥管理）

加密术语

- **加密：*可逆*操作，通过密码将输入内容转换为难以辨认的密文**



- **哈希：*不可逆*操作，通过密码将输入内容转换为难以辨认的消息**

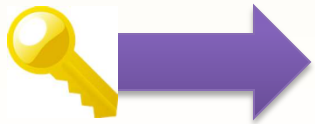


- **令牌化：可逆操作，将输入内容替换为没有固有值的数据**

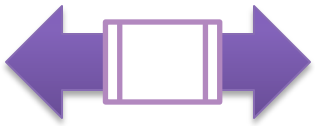
- **密钥管理：密码的生命周期，包括创建、分发、使用和删除**

加密注意事项

- **加密：*可逆*操作，通过密码将输入内容转换为难以辨认的密文**



- **哈希：*不可逆*操作，通过密码将输入内容转换为难以辨认的消息**



- **令牌化：可逆操作，将输入内容替换为没有固有值的数据**

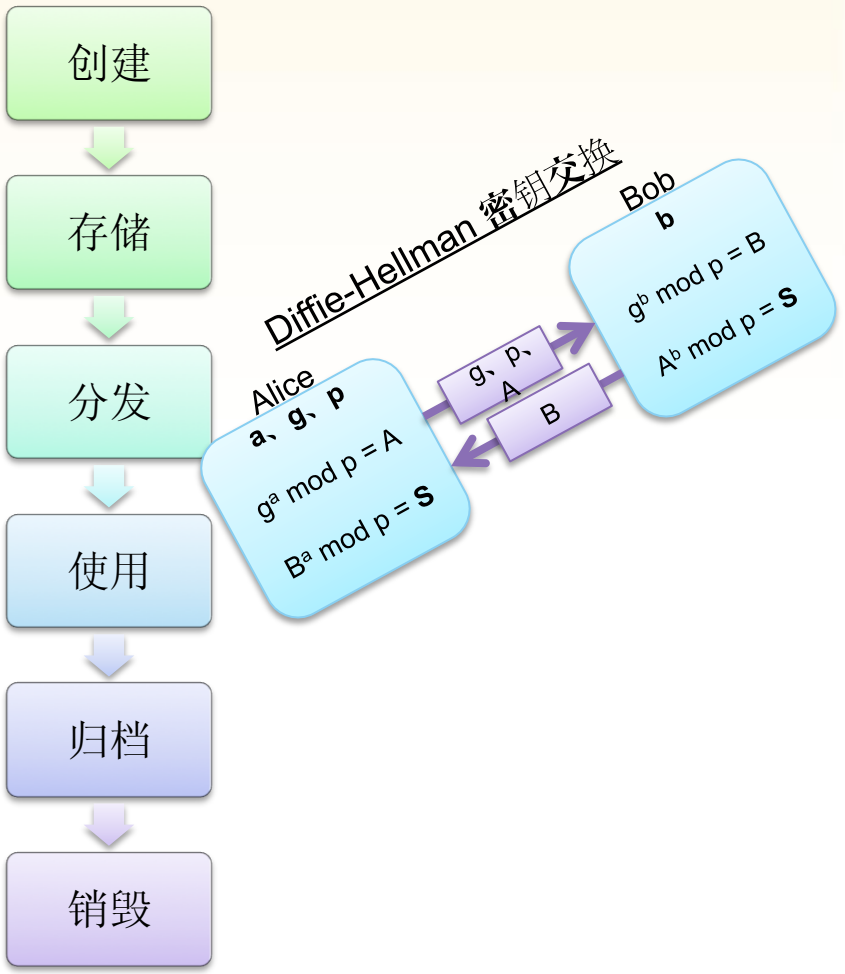
- **密钥管理：密码的生命周期，包括创建、分发、使用和删除**

云中的加密技术

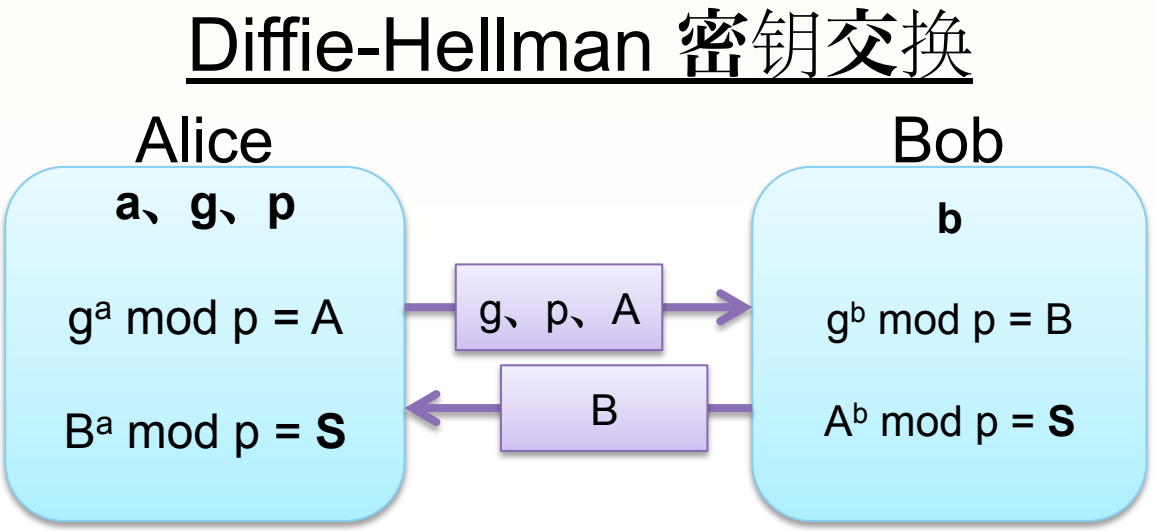
RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

加密注意事项

- 人/社会元素
  - 人员
  - 流程
  - 政策
- 位置元素
  - 边界限制
  - 标准（美国 NIST）
    - SP 800-57
    - SP 800-131A
    - SP 800-130

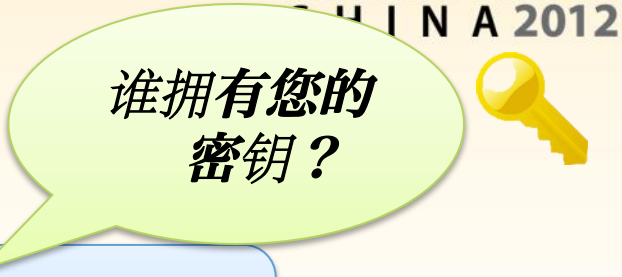


加密注意事项


Diffie-Hellman 密钥交换
Alice
Bob
a、g、p
b
g^a mod p = A
B^a mod p = S
g、p、A
B
g^b mod p = B
A^b mod p = S

云加密注意事项

- 人/社会元素
  - 人员
  - 流程
  - 政策
- 位置元素
  - 边界限制
  - 标准（美国 NIST）
    - SP 800-57
    - SP 800-131A
    - SP 800-130



受信任的服务提供商

体系结构

大型/全球部署

互操作性

云加密注意事项

- “便携式设备”技术 (MA 201 CMR 17)
- 多租户
- 开放接口
  - 消费者
  - 管理
  - 合作伙伴
  - 开发/应用
- 多管辖权
  - 人物/时间
  - 地点

加密即服务

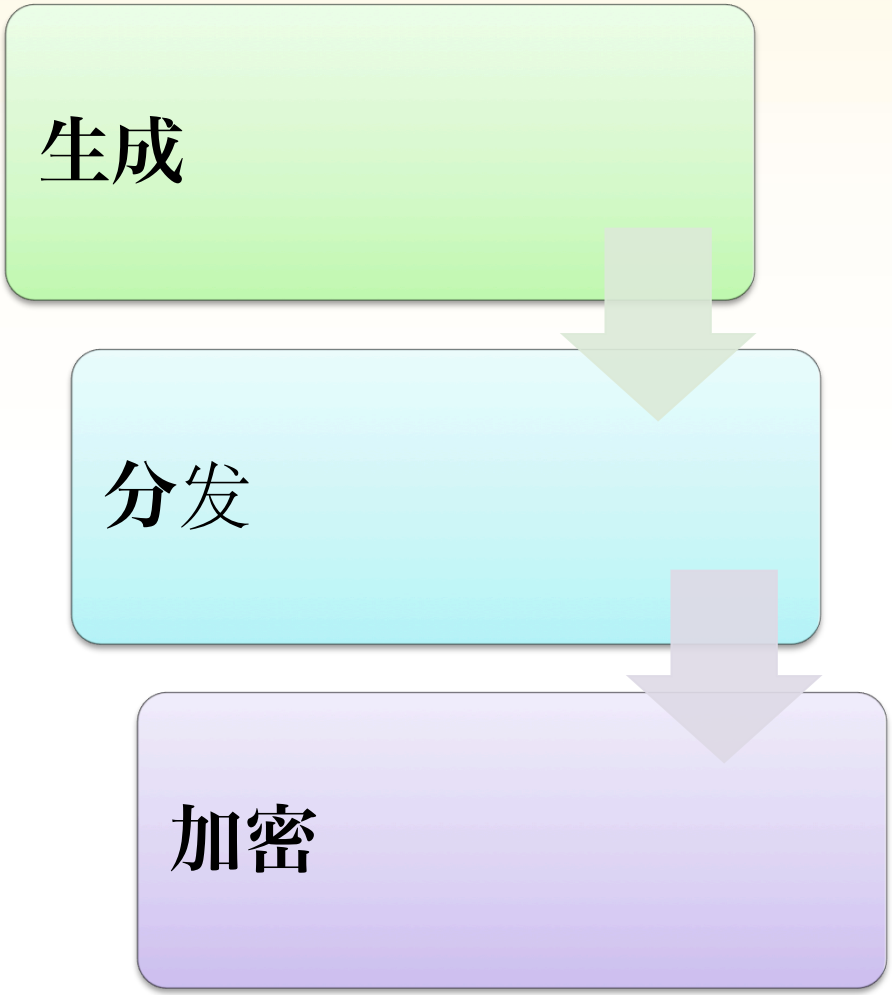
- 密钥管理
  - 生成
  - 保护（密钥加密密钥）
  - 过期和轮换
  - 删除
- 密钥体系结构
  - 管理集成
  - 互操作性
  - 元数据

标准：
ISO 11568
ISO 11770
NIST SP 800-57
IETF Keyprov
OASIS EKMI
OASIS KMIP

示例

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

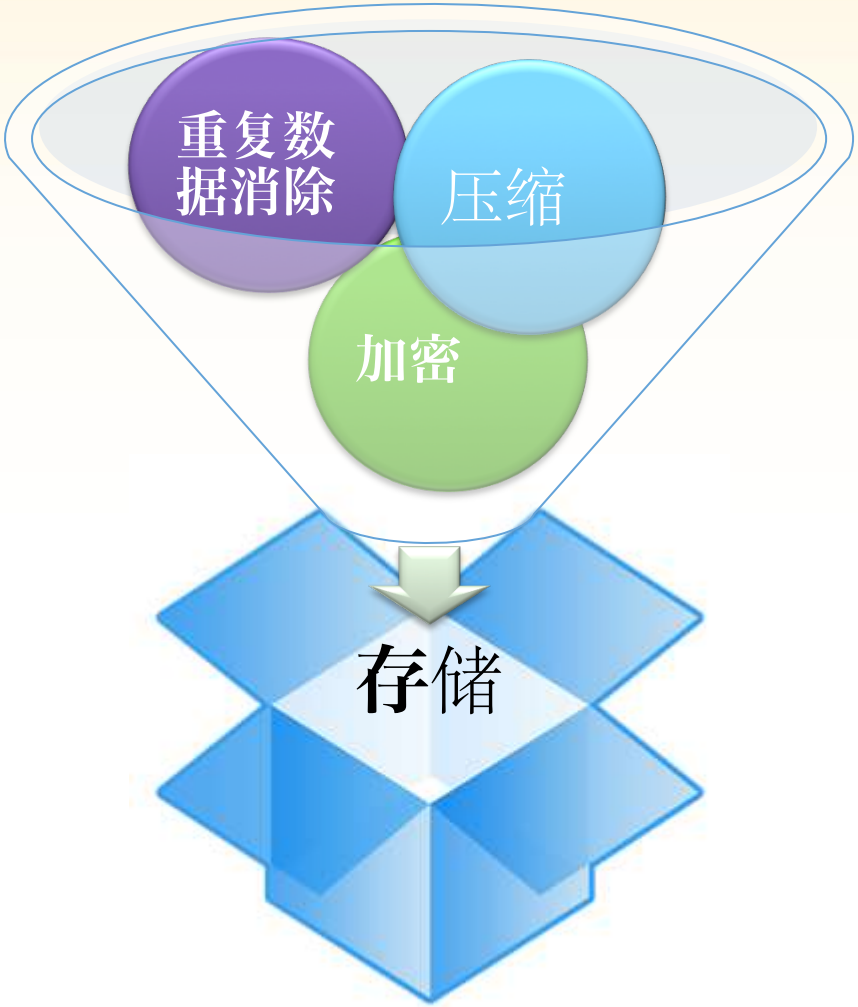
示例 1



- 密钥轮换
  - 模板
  - 快照
  - 离线
- 密钥持久性
  - 模板
  - 快照
  - 重新启动
  - SAN
  - 备份
  - 归档

示例 2

1. 对**数据**进**行加密**
2. **“管理”数据…？**
   - **分析**
   - 报**告**
   - 压缩
   - **重复数据消除**



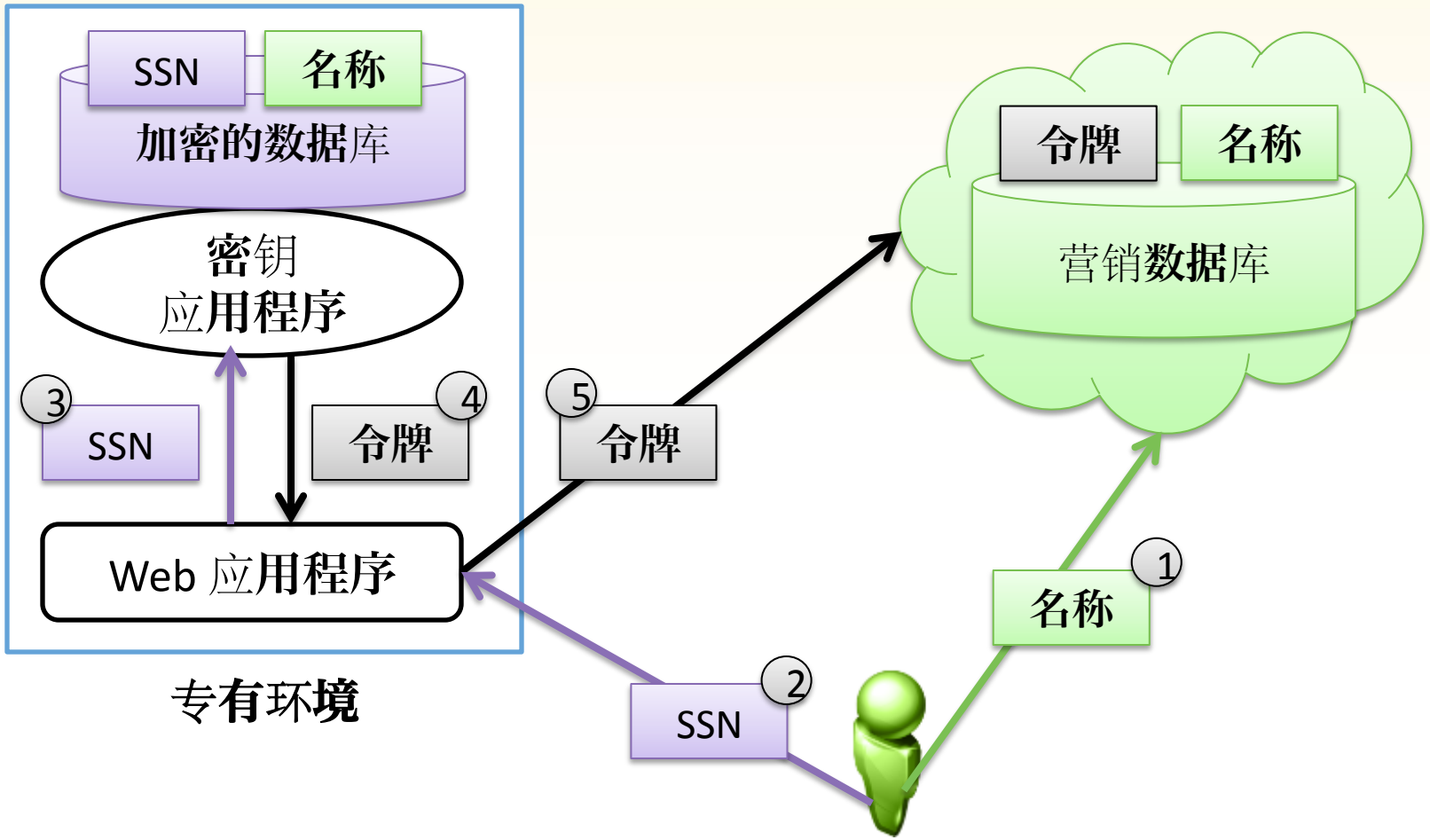
示例 3

细分

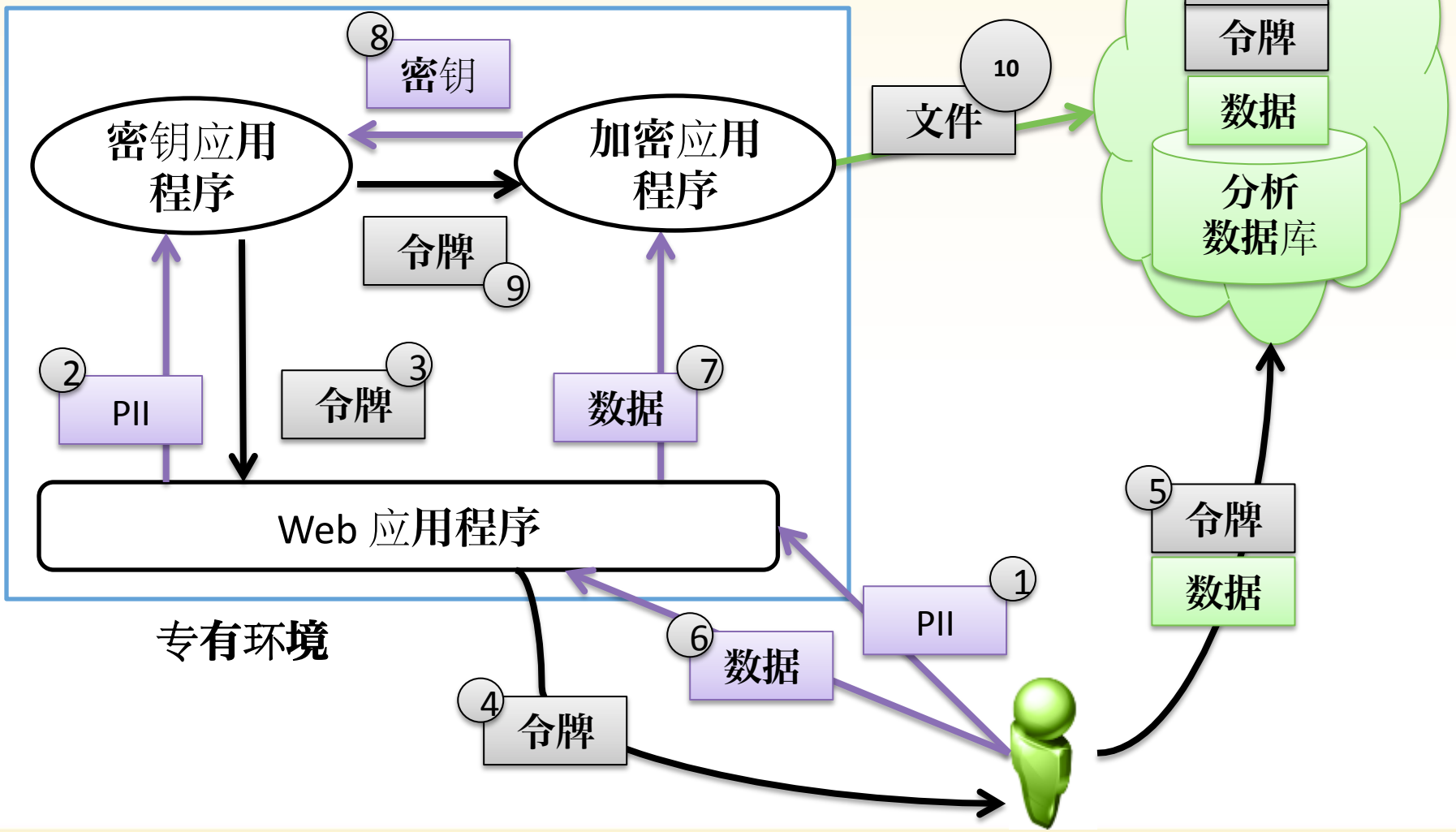
- 默认
- 敏感且不受管控（例如，非“物质”）
- 敏感且受管控（例如，PII、CCN、“物质”）

数据级别	处理
3	清除
2	令牌或加密
1	令牌、哈希或加密

示例 3：令牌


SSN
名称
加密的数据库
密钥
应用程序
3
SSN
4
令牌
Web 应用程序
专有环境
5
令牌
令牌
名称
营销数据库
1
名称
2
SSN

示例 3：加密


8
密钥
密钥应用程序
加密应用程序
令牌
9
10
文件
文件
令牌
数据
分析数据库
2
PII
令牌
3
数据
7
Web 应用程序
专有环境
5
令牌
数据
1
PII
6
数据
4
令牌

对云进行加密

- 接下来的 3 个月
  - 对数据进行分类以进行细分
  - 设置密钥管理策略和过程
  - 选择互操作性标准
- 接下来的 6 个月
  - 配置应用程序以进行密钥和加密管理
  - 选择密钥应用程序和加密应用程序解决方案
  - 规划并启动项目以保护云中的数据

对云进行加密

Davi Ottenheimer
flyingpenguin

RSA CONFERENCE 2012