第10章 云安全机制

§10.1 加密

§10.2 哈希

§10.3 数字签名

§10.4 公钥基础设施

§10.5 身份与访问管理

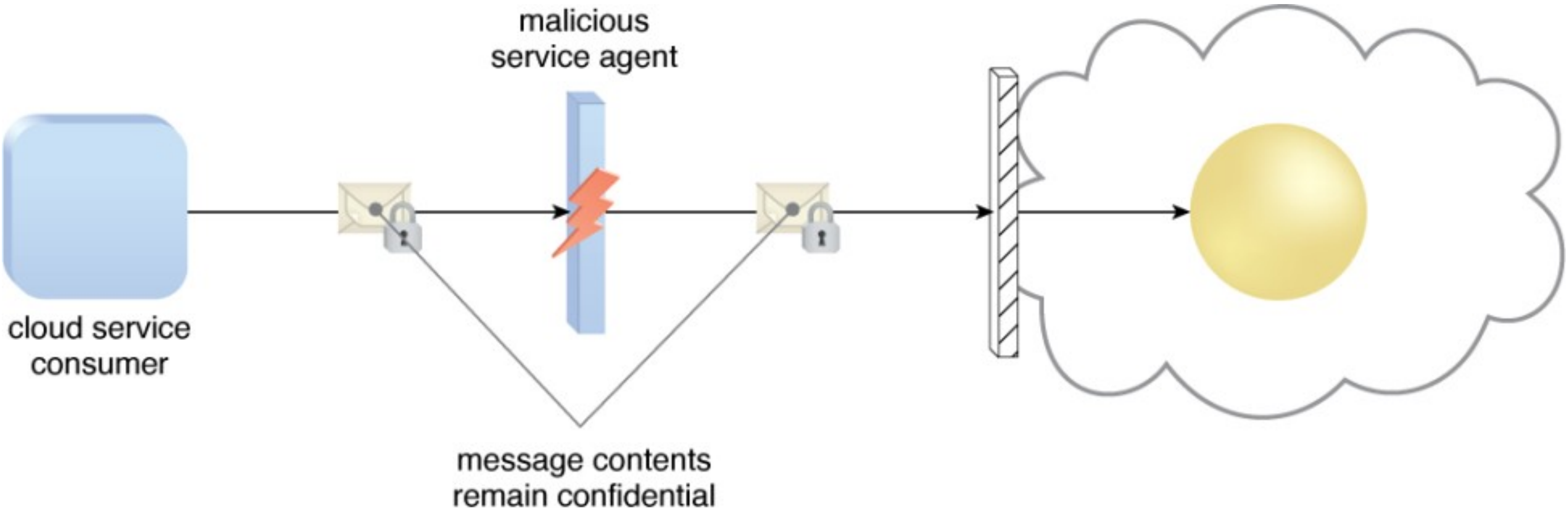
§10.6 单一登录

§10.7 基于云的安全组

§10.8 强化的虚拟服务器映像

安全属性

- 保密性(confidentiality)是指只有被授权方才能访问的特性
- 完整性(integrity)是指未被未授权方篡改的特性
- 真实性(authenticity)是指事务是由经过授权的源提供的这一特性
- 可用性(availability)是在特定的时间段内可以访问和可以使用的特性



Copyright © Arcitura Education

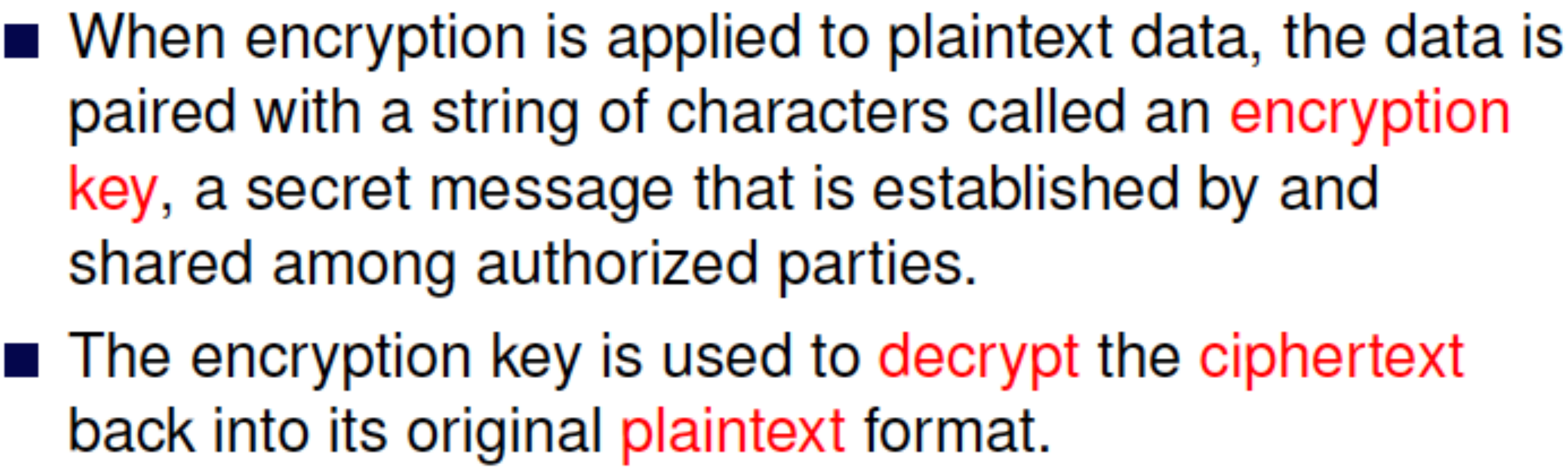
- *Figure 10.1 – A malicious intermediary is unable to retrieve data from an encrypted message. The retrieval attempt may furthermore be revealed to the cloud service consumer. (Note the use of the lock symbol to indicate that a security mechanism has been applied to the message contents.)*

加密

- 加密(encryption)
  - 是一种数字编码系统，专门用来保护数据的保密性和完整性（主要是指对称加密）。
  - 用于对抗流量窃听、恶意媒介、授权不足和信任边界重叠这样一些安全威胁。
  - Q&A：Just Explain 加密是如何对抗上述4种威胁的？

加密

- 加密部件(cipher)
  - 加密用的标准化算法，把原始的明文数据（Plaintext）转换成加密的密文数据（ciphertext）。
  - Access to ciphertext does not reveal the original plaintext data, apart from some forms of metadata, such as message length and creation date.
- Encryption key – 密钥：加密以及解密



■ When encryption is applied to plaintext data, the data is paired with a string of characters called an encryption key, a secret message that is established by and shared among authorized parties.

■ The encryption key is used to decrypt the ciphertext back into its original plaintext format.

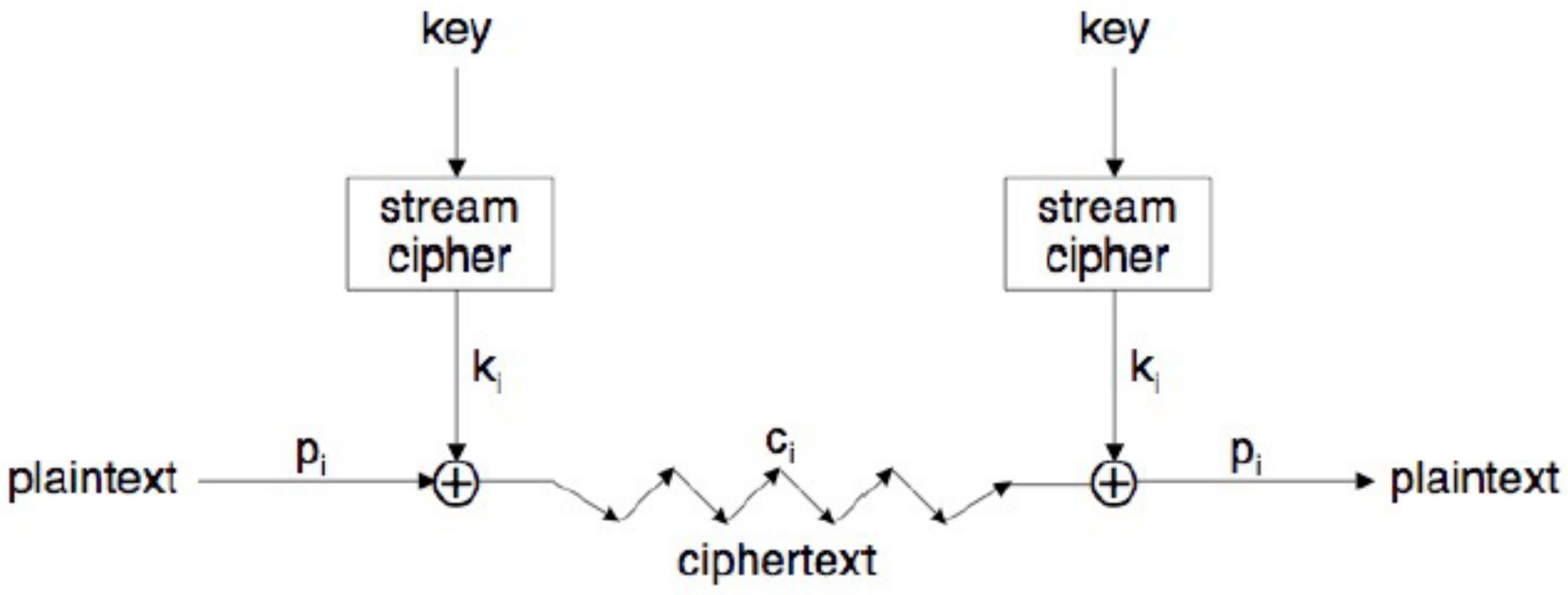
加密的类型

- Stream-based Ciphers
- Block Ciphers

Stream-based Ciphers

- Generalization of **one-time pad**
- Trade provable security for practicality
- Stream cipher is initialized with short **key**
- Key is “stretched” into long **keystream**
- Keystream is used like a one-time pad
  - XOR to encrypt or decrypt
- Stream cipher is a keystream generator
- Usually, keystream is bits, sometimes bytes

Stream-based Ciphers



- Generic view of stream cipher

- ORYX — weak cipher, uses shift registers, generates 1 byte/step
- RC4 — strong cipher, one of the most widely used, generates 1 byte/step
- PKZIP — intermediate strength, unusual mathematical design, generates 1 byte/step

Block Ciphers

- Modern version of a **codebook cipher**
- In effect, a block cipher algorithm yields a huge number of codebooks
  - Specific codebook determined by key
- It is OK to use same key for a while
  - Just like classic codebook
- Change the key, get a new codebook

加密的方法

- **Symmetric 对称加密**
  - Same key for encryption and decryption
  - Key distribution problem
- **Asymmetric 非对称加密**
  - Mathematically related key pairs for encryption and decryption
  - Public and private keys
- **Hybrid**
  - Combines strengths of both methods

  1) Asymmetrically distributes symmetric key
     - Also known as a ***session key***

  2) Symmetric provides bulk encryption

  - Example:
    - SSL negotiates a hybrid method

对称加密

Definition

Symmetric encryption uses the same key for both encryption and decryption, both of which are performed by authorized parties that use the one shared key.

Also known as secret key cryptography, messages that are encrypted with a specific key can be decrypted by only that same key.

Example

Examples of popular symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, 3DES, Skipjack, Safer+/++ (Bluetooth), and IDEA.

对称加密

---保证了保密性但是无法保证不可否认性

- Parties that rightfully decrypt the data are provided with evidence that the original encryption was performed by parties that rightfully possess the key.
- A basic authentication check is always performed, because only authorized parties that own the key can create messages.
- This maintains and verifies data confidentiality.

Proposition

Note that symmetrical encryption does not have the characteristic of non-repudiation, since determining exactly which party performed the message encryption or decryption is not possible if more than one party is in possession of the key.

非对称加密

Definition

Asymmetric encryption relies on the use of two different keys, namely a private key and a public key.

With asymmetric encryption (which is also referred to as public key cryptography),

- the private key is known only to its owner
- while the public key is commonly available.

Example

Examples of popular asymmetric algorithms include Diffie, DSS, ElGamal and RSA.

非对称加密: 秘钥加密

---真实性、不可否认性和完整性保护（不提供保密性）

- As every asymmetrically encrypted message has its own private-public key pair, messages that were encrypted with a private key can be correctly decrypted by any party with the corresponding public key.
- This method of encryption does not offer any confidentiality protection, even though successful decryption proves that the text was encrypted by the rightful private key owner.
- Private key encryption therefore offers integrity protection in addition to authenticity and nonrepudiation.

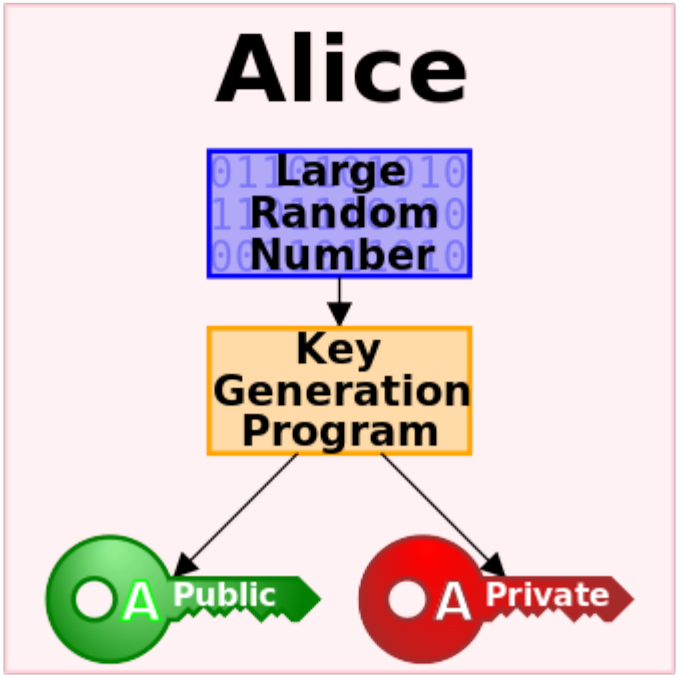
非对称加密：公钥加密

---保证了保密性（不保证完整性、真实性的保护）

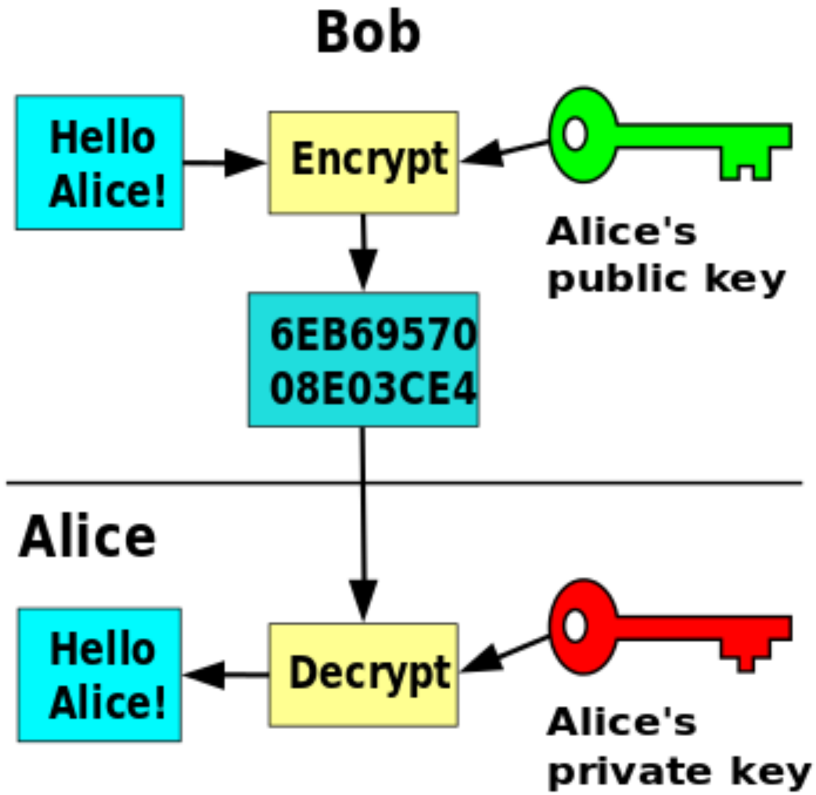
- A message that was encrypted with a public key can only be decrypted by the rightful private key owner, which provides confidentiality protection.
- However, any party that has the public key can generate the ciphertext, meaning this method provides neither message integrity nor authenticity protection due to the communal nature of the public key.

非对称加密

- 基于无法逆向求解的数学问题
  - 整数分解、离散对数、椭圆曲线等。
- 通过一个大的随机数产生一对密钥
  - 私钥、公钥



公钥加密

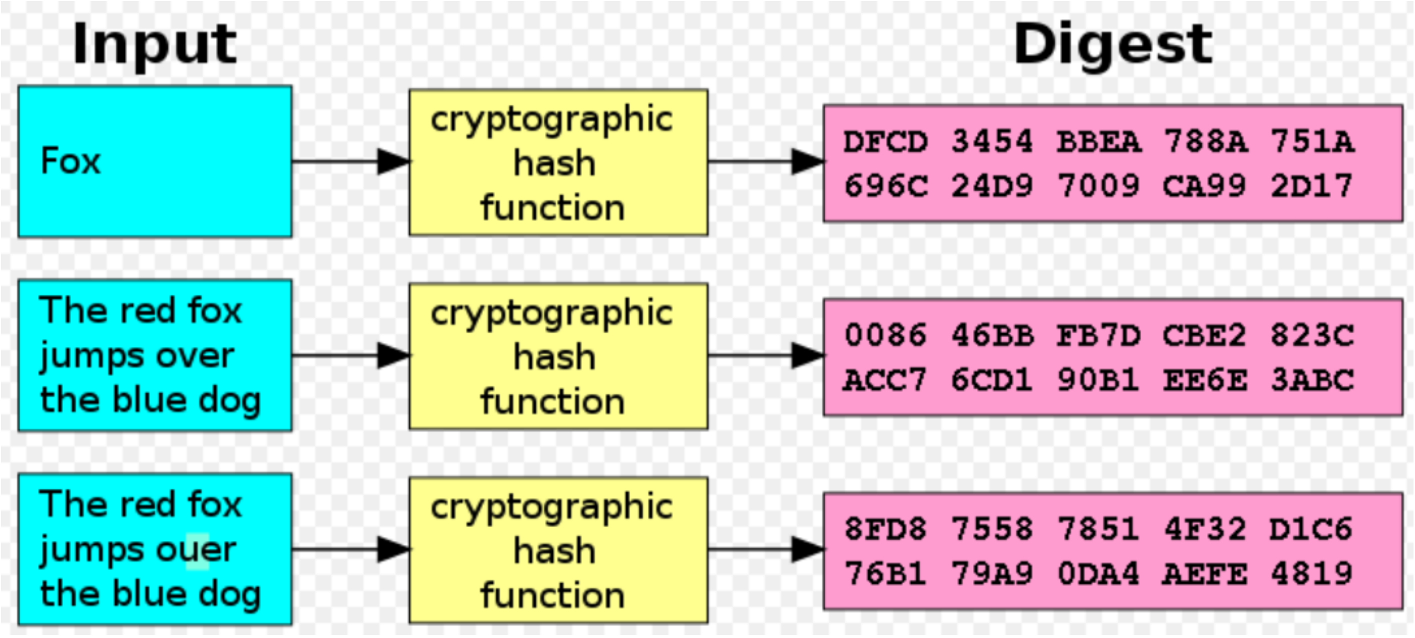

Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

对称vs.非对称

- 对称加密保证了数据的保密性(confidentiality)但是并不保证数据的不可否认性(non-repudiation)
- 非对称加密依赖于使用两个不用的密钥，称为私钥和公钥。
  - 用自己的私钥加密给对方，对方用公钥解开
    - 真实性、不可否认性和完整性保护（不提供保密性）
  - 用公钥加密送给私钥拥有者
    - 保证了保密性（不提供完整性、真实性的保护）

§10.2 哈希 Hashing

- 哈希(Hashing)
  - 用来获得消息的哈希代码或消息摘要(message digest)，通常是固定的长度，小于原始的消息大小。
  - 单向的、不可逆转的数据保护。



Input

Digest

Fox → cryptographic hash function → DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17

The red fox jumps over the blue dog → cryptographic hash function → 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC

The red fox jumps ouer the blue dog → cryptographic hash function → 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819

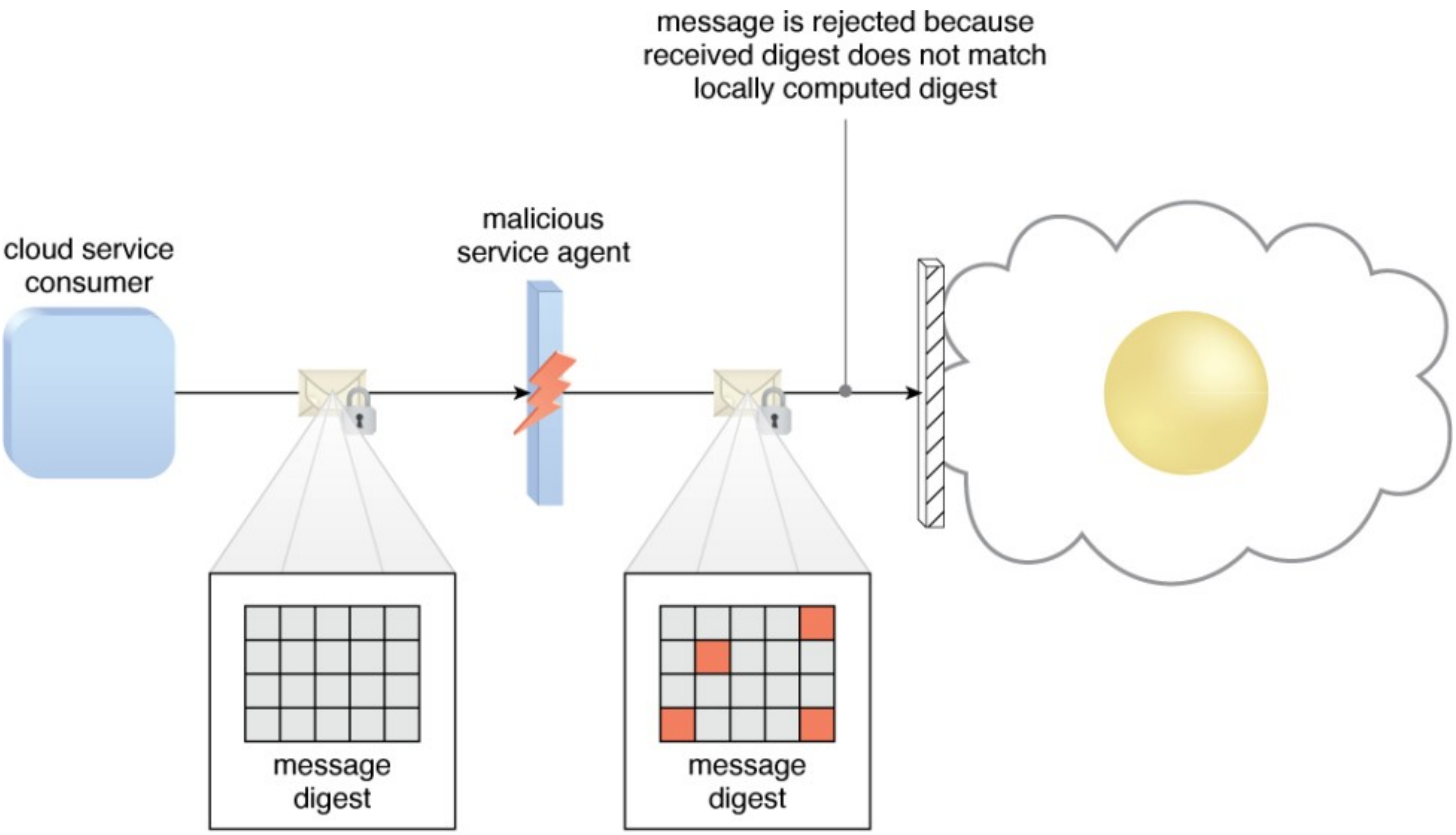
哈希算法

哈希函数的主要属性：
计算简单、不可逆、不重复

- MD5
  - Computes 128-bit hash value
  - Widely used for file integrity checking
- SHA-1（新版本为SHA-2）
  - Computes 160-bit hash value
  - NIST approved message digest algorithm
- HAVAL
  - Computes between 128 and 256 bit hash
  - Between 3 and 5 rounds
- RIPEMD-160
  - Developed in Europe published in 1996
  - Patent-free

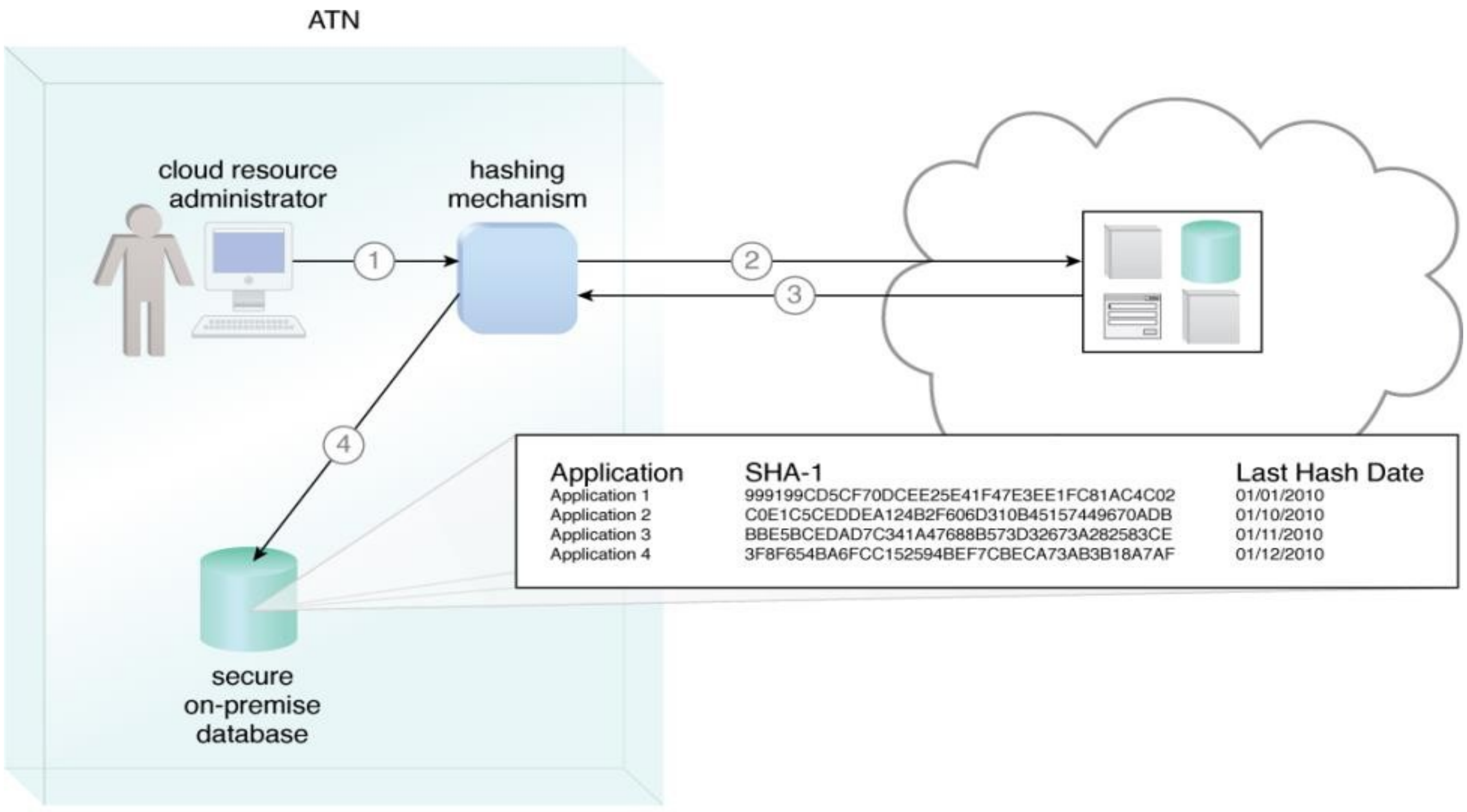
哈希的典型应用

- 数据保密
  - 如密码哈希（Password verification）
- 恶意媒介和授权不足
  - Verifying the integrity of files or messages
- 服务滥用（如DoS）
  - Proof-of-work，要求服务请求者产生能生成特种Hash值的消息
- 文件标识
  - P2P文件系统、软件版本管理工具等


message is rejected because received digest does not match locally computed digest
malicious service agent
cloud service consumer
message digest
message digest

Copyright © Arcitura Education

- *Figure 10.3 – A hashing function is applied to protect the integrity of a message that is intercepted and altered by a malicious service agent, before it is forwarded. The firewall can be configured to determine that the message has been altered, thereby enabling it to reject the message before it can proceed to the cloud service.*

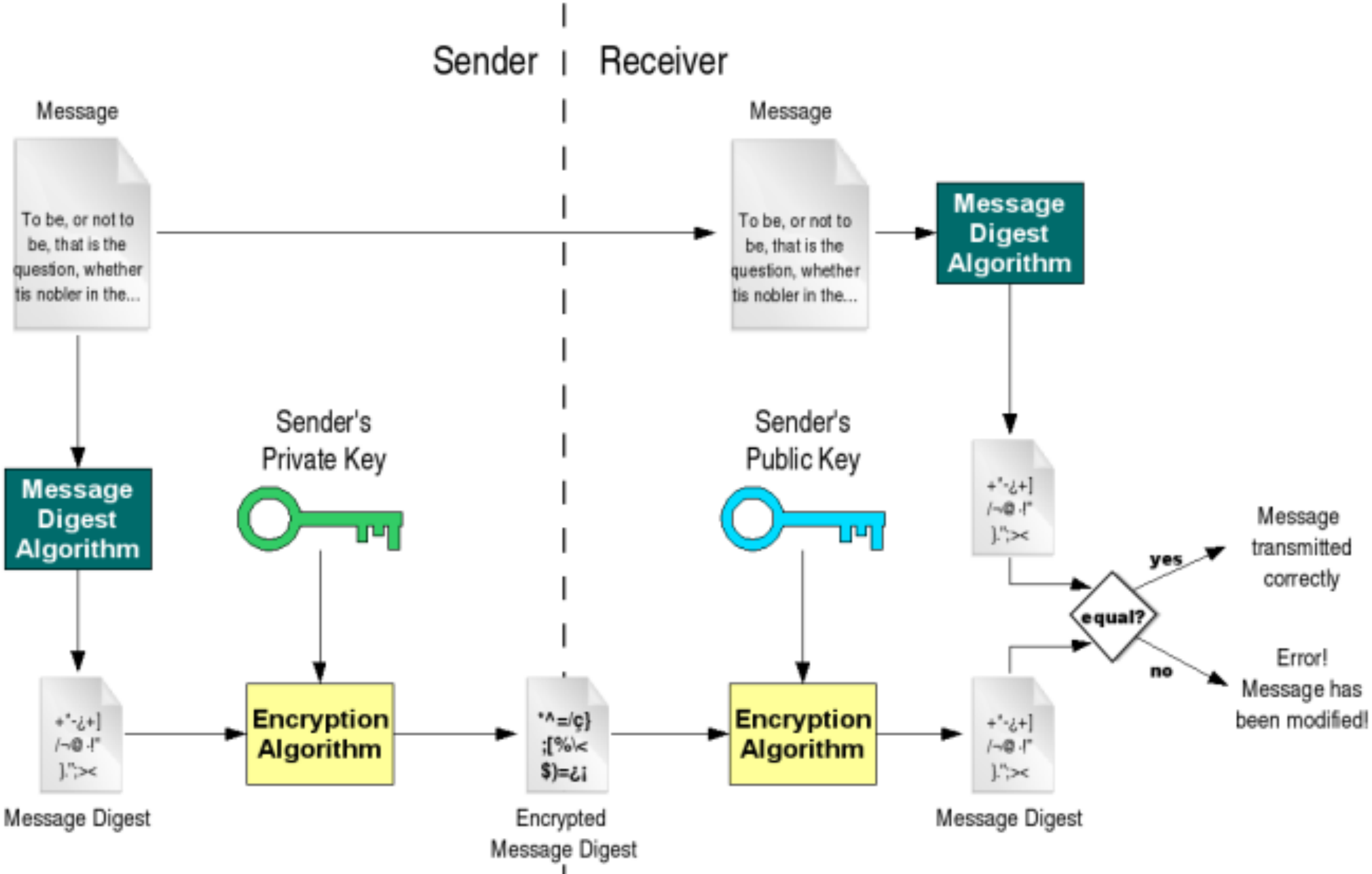


Application	SHA-1	Last Hash Date
Application 1	999199CD5CF70DCEE25E41F47E3EE1FC81AC4C02	01/01/2010
Application 2	C0E1C5CEDDEA124B2F606D310B45157449670ADB	01/10/2010
Application 3	BBE5BCEDAD7C341A47688B573D32673A282583CE	01/11/2010
Application 4	3F8F654BA6FCC152594BEF7CBECA73AB3B18A7AF	01/12/2010

图 10.4哈希摘要用于保障应用程序的完整性。A hashing procedure is invoked when the PaaS environment is accessed (1). The applications that were ported to this environment are checked (2) and their message digests are calculated (3). The message digests are stored in a secure on-premise database (4), and a notification is issued if any of their values are not identical to the ones in storage.

§10.3 数字签名

- 数字签名(digital signature)
  - 将消息进行哈希，然后用私钥进行加密。



数字签名

- 作用：
  - 提供不可否认性、数据真实性和数据完整性。
  - 类似于日常生活中的“签名”。
- 算法：
  - RSA是最常用的签名算法。
- 扩展应用：
  - 数字证书：个人安全邮件证书
  - 智能卡：将数字签名放入便携物理存储介质

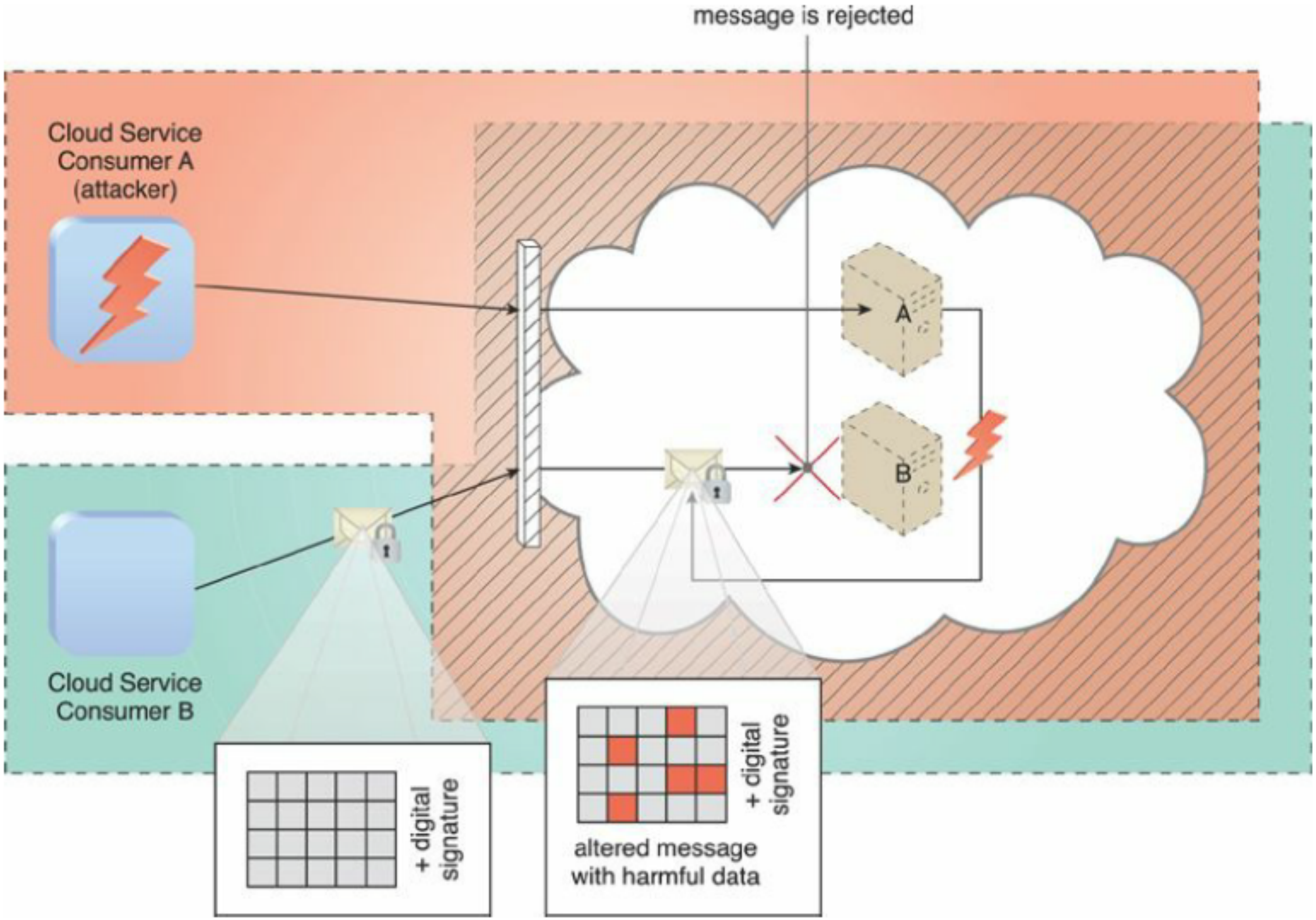


Figure 10.5. Cloud Service Consumer B sends a message that was digitally signed but was altered by trusted attacker Cloud Service Consumer A. Virtual Server B is configured to verify digital signatures before processing incoming messages even if they are within its trust boundary. The message is revealed as illegitimate due to its invalid digital signature, and is therefore rejected by Virtual Server B.

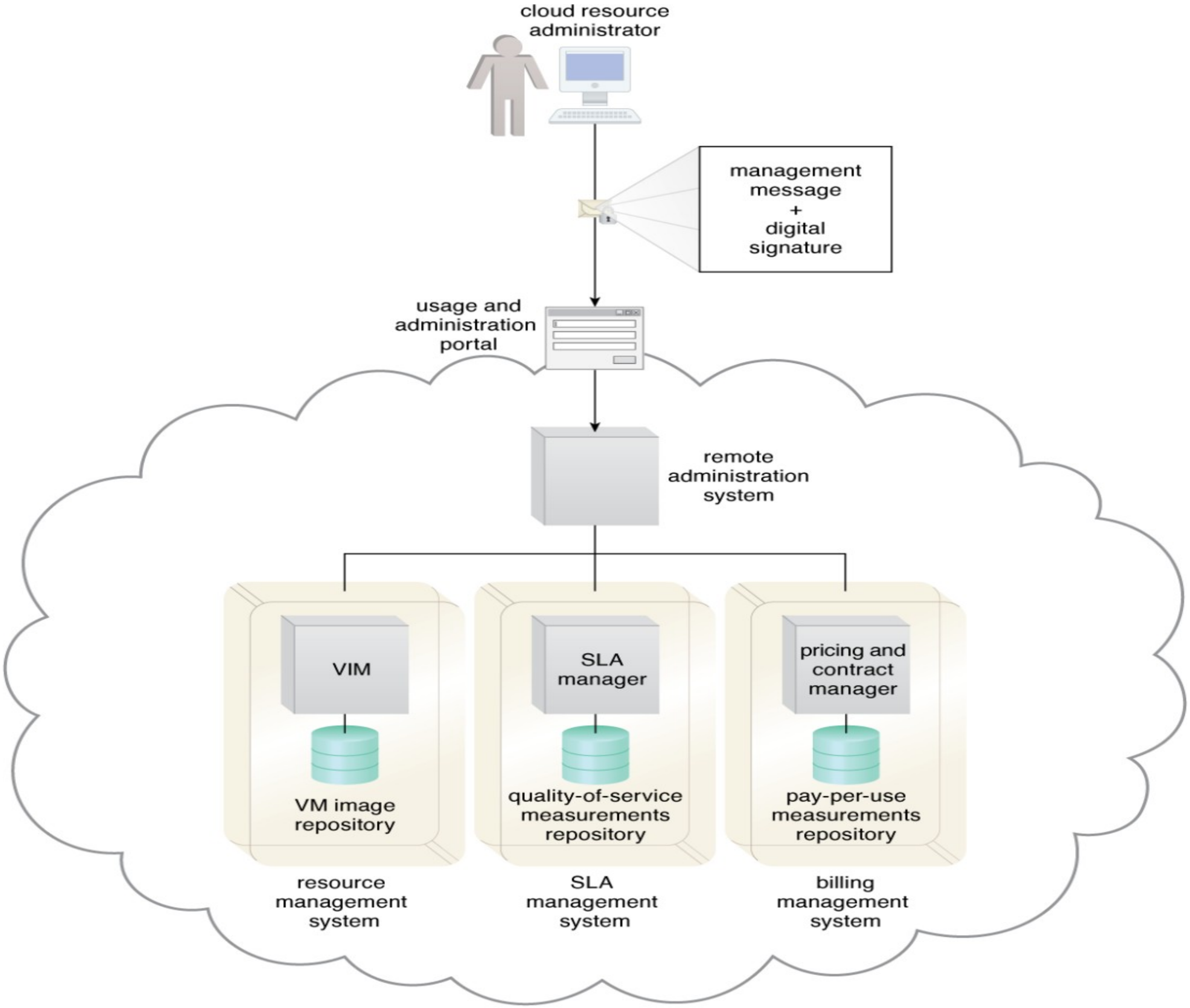
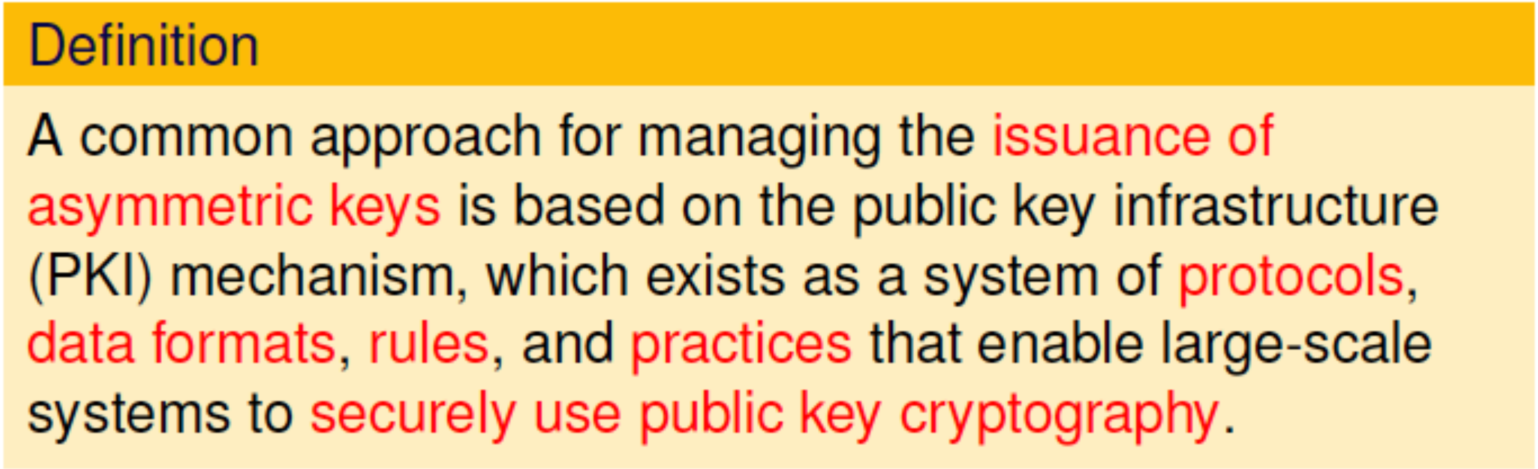

cloud resource administrator
management message + digital signature
usage and administration portal
remote administration system
VIM
VM image repository
resource management system
SLA manager
quality-of-service measurements repository
SLA management system
pricing and contract manager
pay-per-use measurements repository
billing management system

Figure 10.6. Whenever a cloud consumer performs a management action that is related to IT resources, the cloud service consumer program must include a digital signature in the message request to prove the legitimacy of its user.

§10.4 公钥基础设施

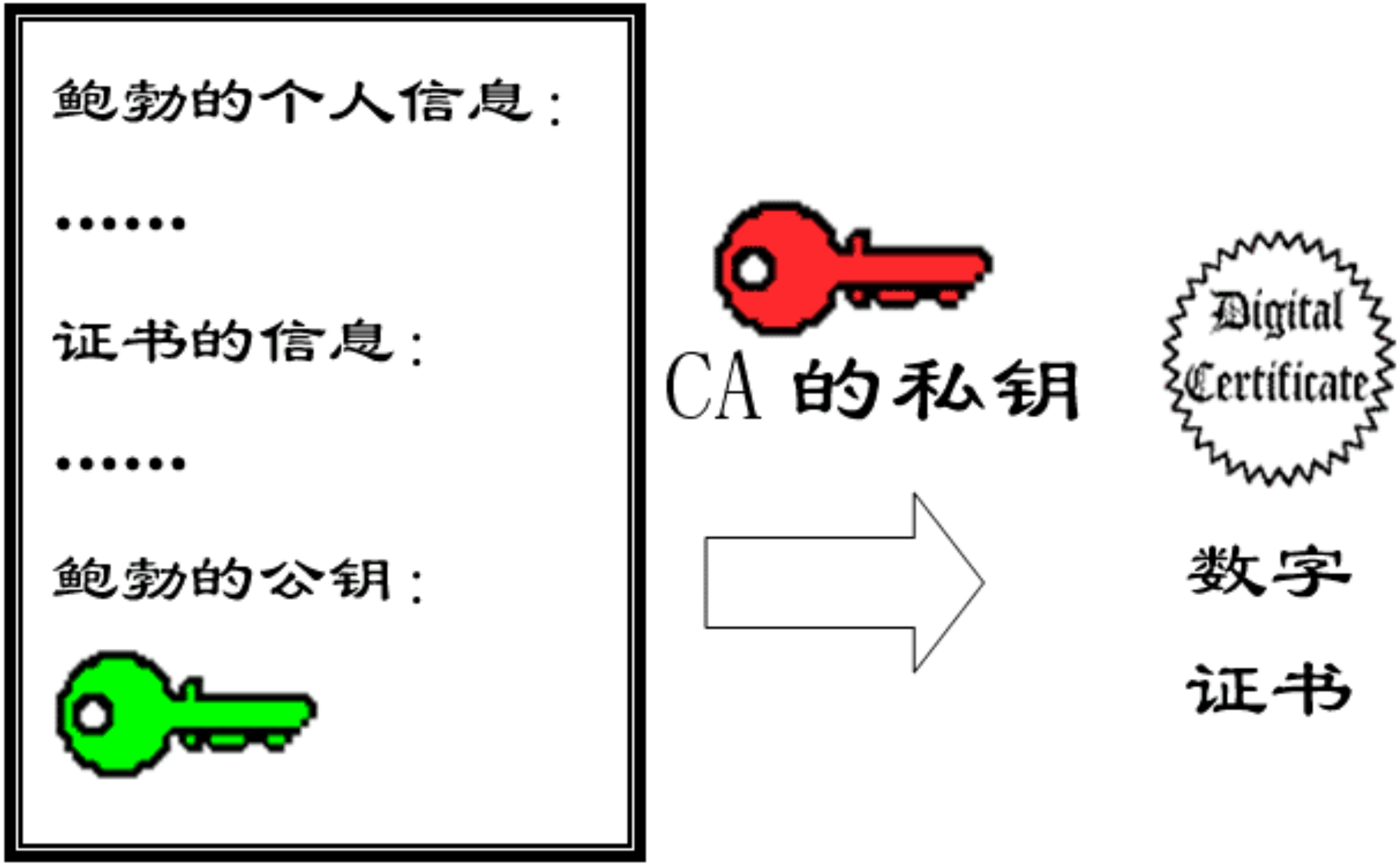
- 公钥基础设施(The public key infrastructure, PKI)
  - 是一个由协议、数据格式、规则和实施组成的系统
  - 是用于大规模、公共系统的公钥管理技术
- 数字证书：
  - 带数字签名的数据结构，验证证书拥有者身份以及相关信息（如名称、Email、身份证号）。
  - 通常是由第三方证书颁发机构(Certificate Authority, CA)签发的，比如和VeriSign 和 Comodo



Definition

A common approach for managing the issuance of asymmetric keys is based on the public key infrastructure (PKI) mechanism, which exists as a system of protocols, data formats, rules, and practices that enable large-scale systems to securely use public key cryptography.

数字证书



鲍勃的个人信息：

……

证书的信息：

……

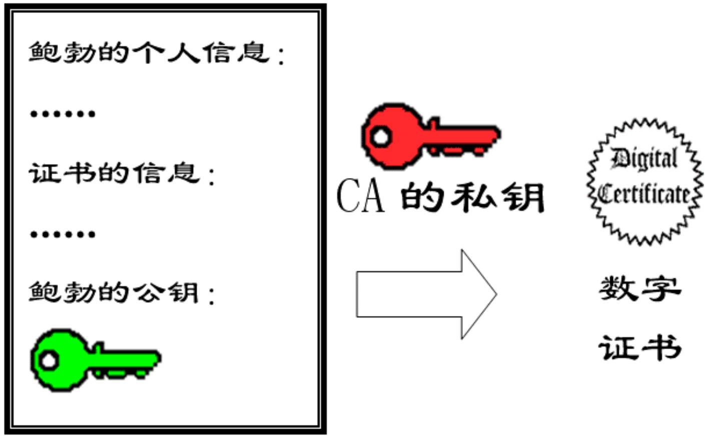
鲍勃的公钥：

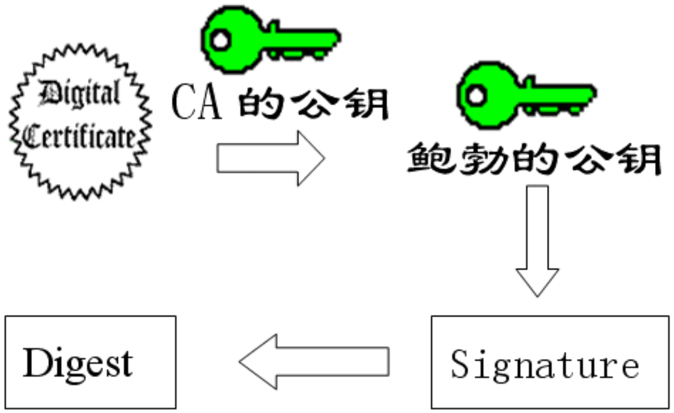
CA 的私钥

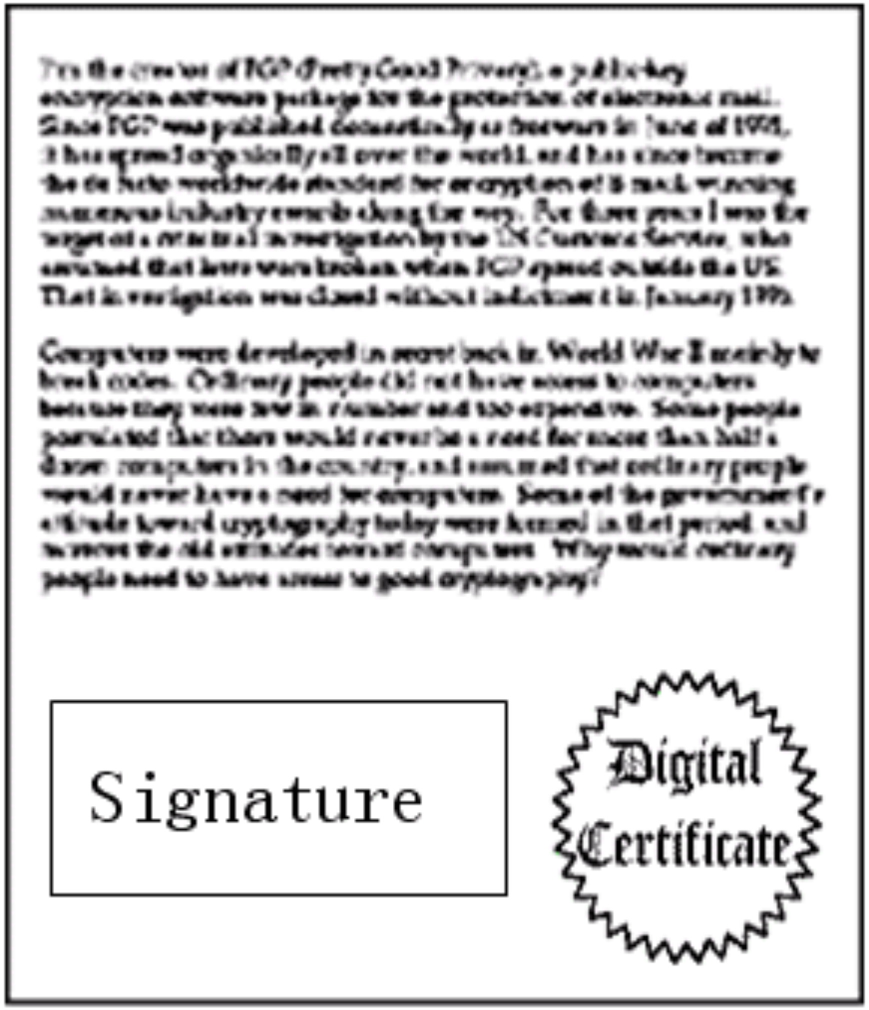
数字证书

数字证书

证书：安全传送发送者的公钥；
签名：确认数据是发送者发送并且未被篡改。



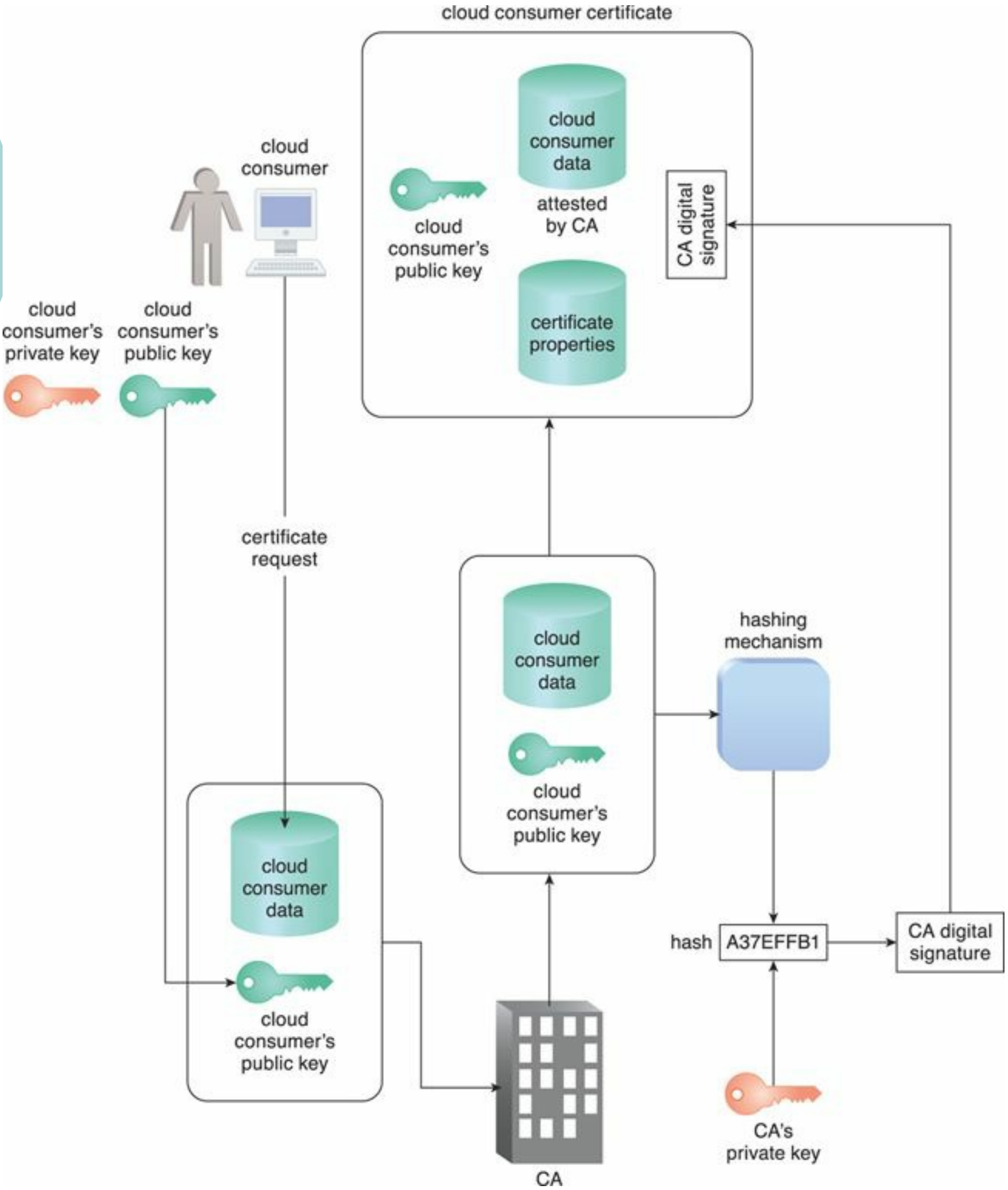


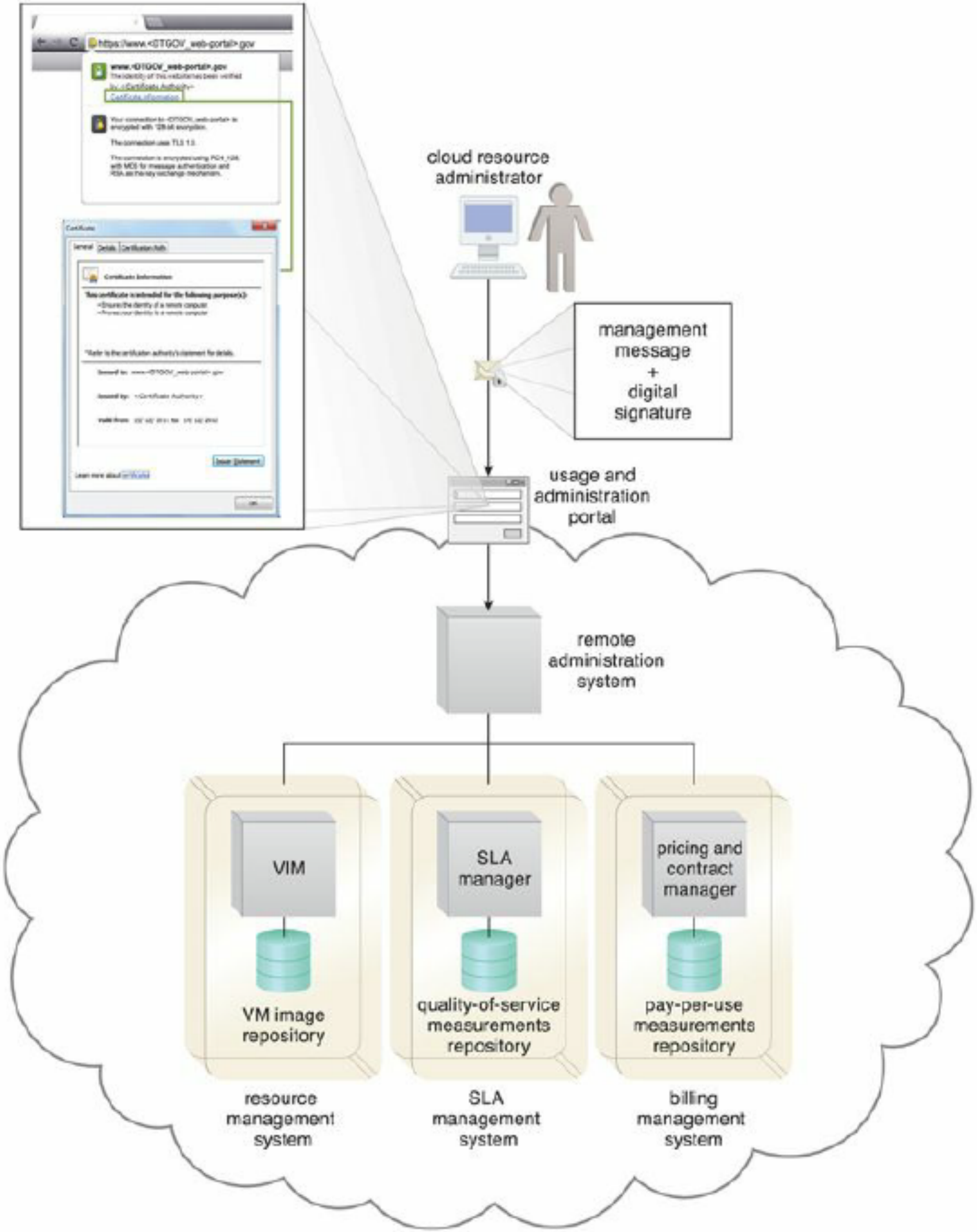


I'm the creator of PGP (Pretty Good Privacy), a public key encryption software package for the protection of electronic mail. Since PGP was published domestically as freeware in June of 1991, it has spread organically all over the world, and has since become the de facto worldwide standard for encryption of E-mail, winning numerous industry awards along the way. For three years I was the target of a criminal investigation by the US Customs Service, who assumed that laws were broken when PGP spread outside the US. That investigation was closed without indictment in January 1996.

Computers were developed in secret back in World War II mainly to break codes. Ordinary people did not have access to computers because they were few in number and too expensive. Some people postulated that there would never be a need for more than half a dozen computers in the country, and assumed that ordinary people would never have a need for computers. Some of the government's attitude toward cryptography today were formed in that period, and mirrors the old attitudes toward computers. Why would ordinary people need to have access to good cryptography?

数字证书签发流程


cloud consumer certificate
cloud consumer data
attested by CA
cloud consumer's public key
certificate properties
CA digital signature
cloud consumer
cloud consumer's private key
cloud consumer's public key
certificate request
cloud consumer data
cloud consumer's public key
hashing mechanism
cloud consumer data
cloud consumer's public key
hash
A37EFFB1
CA digital signature
CA
CA's private key



https://www.<DTGOV_web-portal>.gov

www.<DTGOV_web-portal>.gov

The identity of this website has been verified by <Certificate Authority>

Certificate information

Your connection to <DTGOV_web-portal> is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using RC4_128, with MD5 for message authentication and RSA as the key exchange mechanism.

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

*Refer to the certification authority's statement for details.

Issued to: www.<DTGOV_web-portal>.gov

Issued by: <Certificate Authority>

Valid from: [illegible]

Issuer Statement

Learn more about certificates

OK

cloud resource administrator
management message
+
digital signature
usage and administration portal
remote administration system
VIM
VM image repository
SLA manager
quality-of-service measurements repository
pricing and contract manager
pay-per-use measurements repository
resource management system
SLA management system
billing management system

Figure 10.8. An external cloud resource administrator uses a digital certificate to access the Web-based management environment. DTGOV's digital certificate is used in the HTTPS connection and then signed by a trusted CA.

PKI与云计算

- 实现非对称加密
- 管理云用户和云提供者身份信息
- 防御恶意媒介和授权不足威胁

Q&A：PKI如何防御恶意媒介和授权不足威胁？

授权不足(Insufficient Authorization)攻击是指错误地授予了攻击者访问权限或是授权太宽泛，导致攻击者能够访问到本应该受保护的IT资源。

§10.5 身份与访问管理 IAM

- 身份与访问管理(identity and access management)
  - 控制和追踪用户身份以及
  - IT资源、环境、系统访问特权
- 四部分组成
  - 认证(Authentication)
  - 授权 (Authorization)
  - 用户管理(User Management)
  - 证书管理(Credential Management)

身份与访问管理

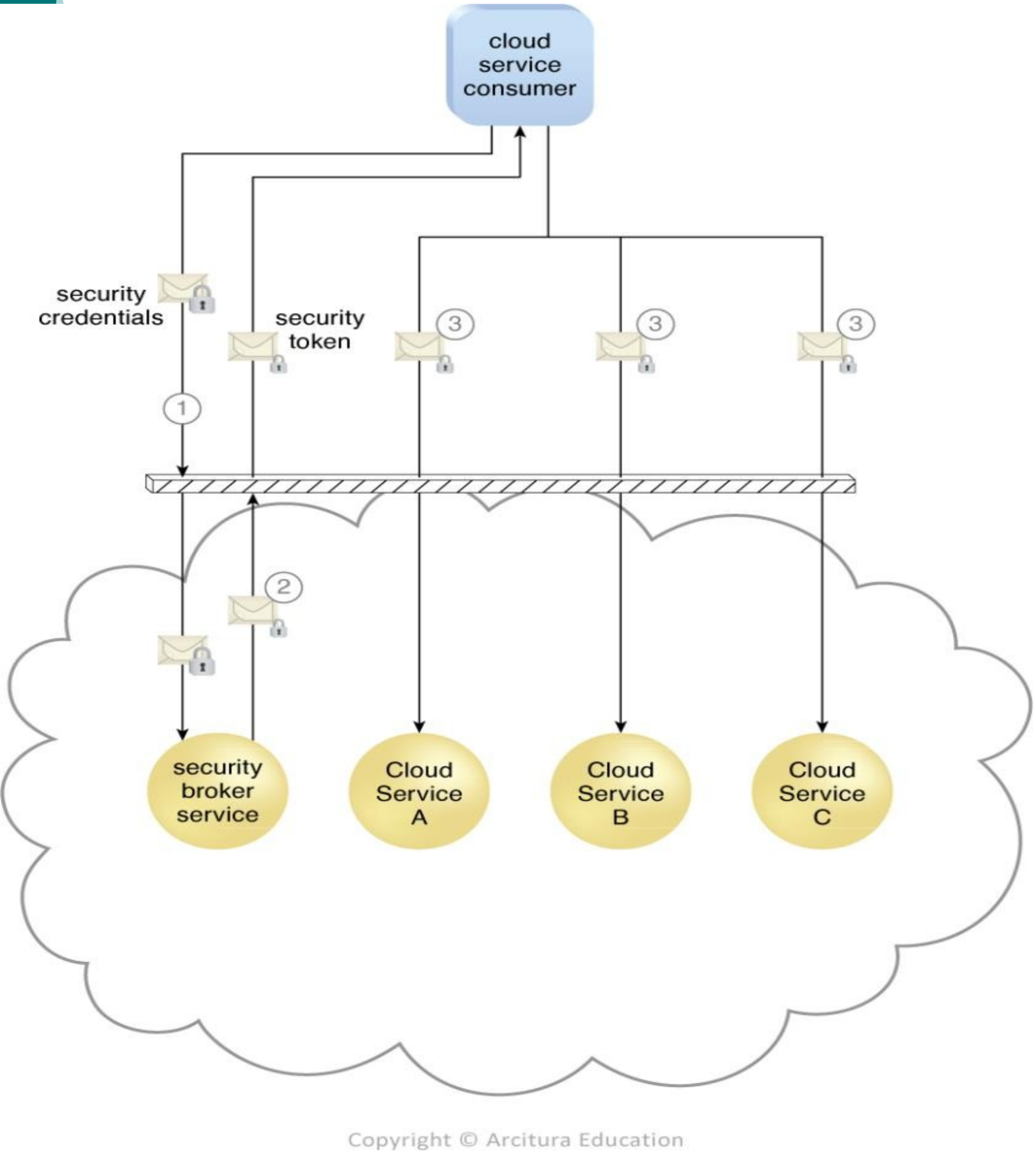
- IAM机制功能：
  - 分配用户特权等级
  - 访问控制和策略
- IAM机制的用途：
  - 对抗授权不足、拒绝服务攻击和信任边界重叠等威胁
  - 比PKI机制要更全面，但是侧重点不同

  - Q&A：IAM是如何对抗授权不足、拒绝服务攻击和信任边界重叠？

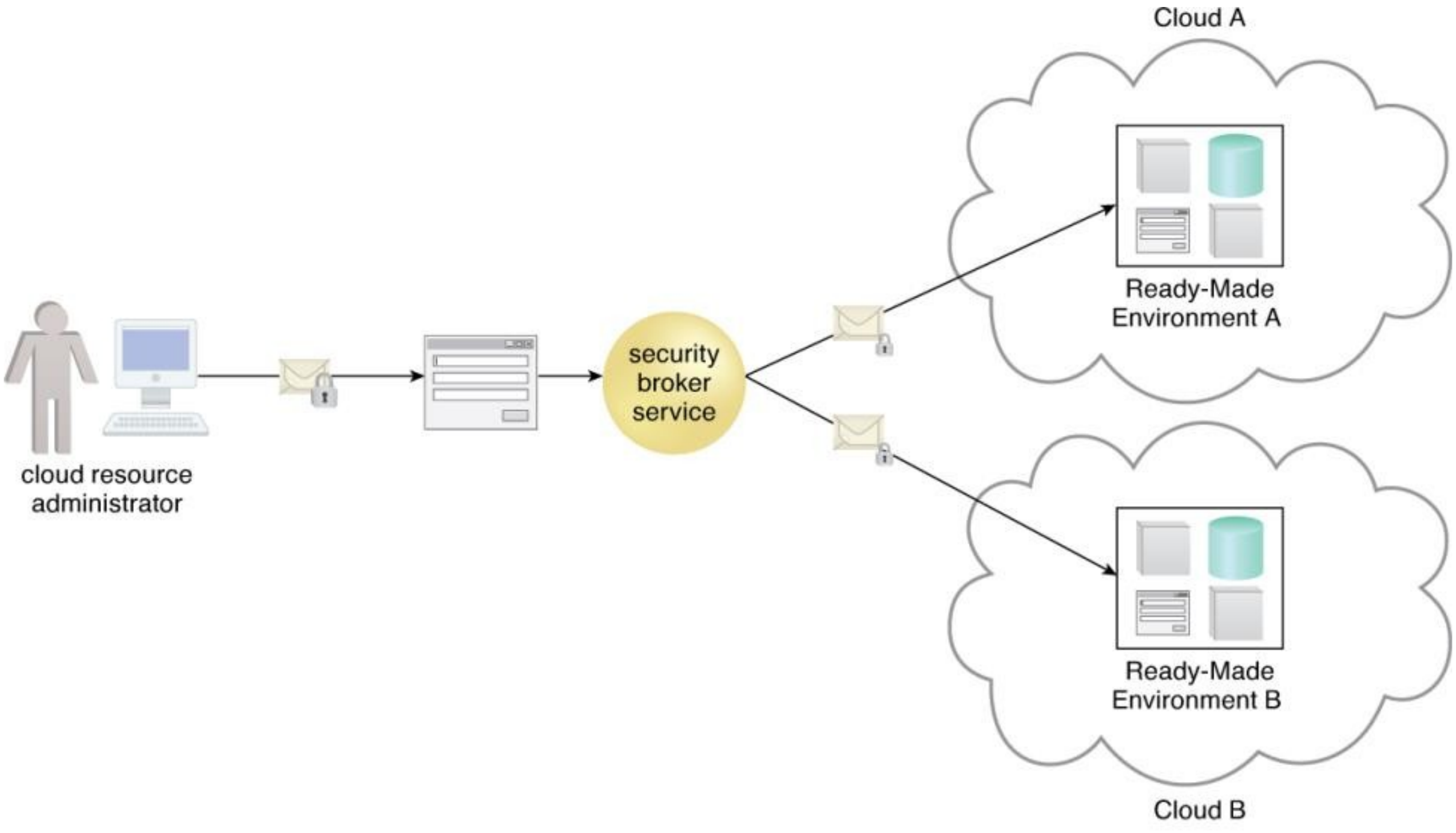
§10.6 单一登录

- 单一登录(single sign-on, SSO)机制
  - 使得一个云服务用户能够被一个安全代理认证并建立起一个安全上下文
  - 当云用户要访问其他云服务或资源的时候，这个上下文会被持久化。
- 实现跨云服务的用户认证和授权

SSO基本示例



- *A cloud service consumer provides the security broker with login credentials (1).*
- *The security broker responds with an authentication token (message with small lock symbol) upon successful authentication, which contains cloud service consumer identity information (2) that is used to automatically authenticate the cloud service consumer for Cloud Services A, B, and C (3).*



- *Figure 10.10 – The credentials received by the security broker are propagated to ready-made environments across two different clouds. The security broker is responsible for selecting the appropriate security procedure with which to contact each cloud.*

单一登录

- SSO机制实际上允许互相独立的云服务和IT资源产生并流通运行时认证和授权证书。
- SSO机制实际上并不直接对抗任何一个云安全威胁。
- SSO增强了基于云的环境的访问并管理分布式IT资源和解决方案。

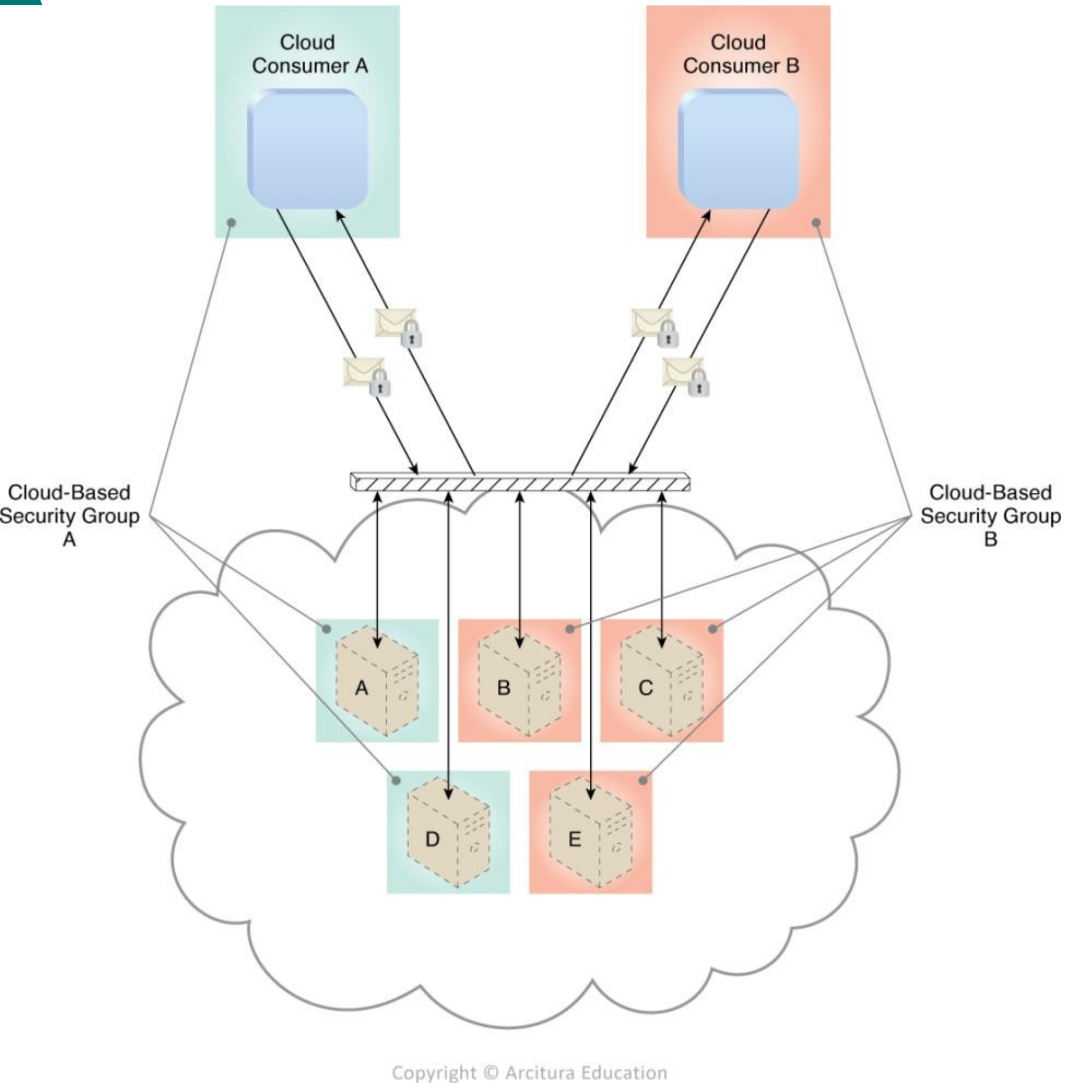
§10.7 基于云的安全组

- 云资源分割(segmentation)
  - 为不同用户和组创建各自的物理和虚拟IT环境的过程。
  - 云资源分割是虚拟化的基础
- 基于云的安全组(cloud-based security group)
  - 基于云的资源分割，网络被分成逻辑的基于云的安全组，形成逻辑网络边界。

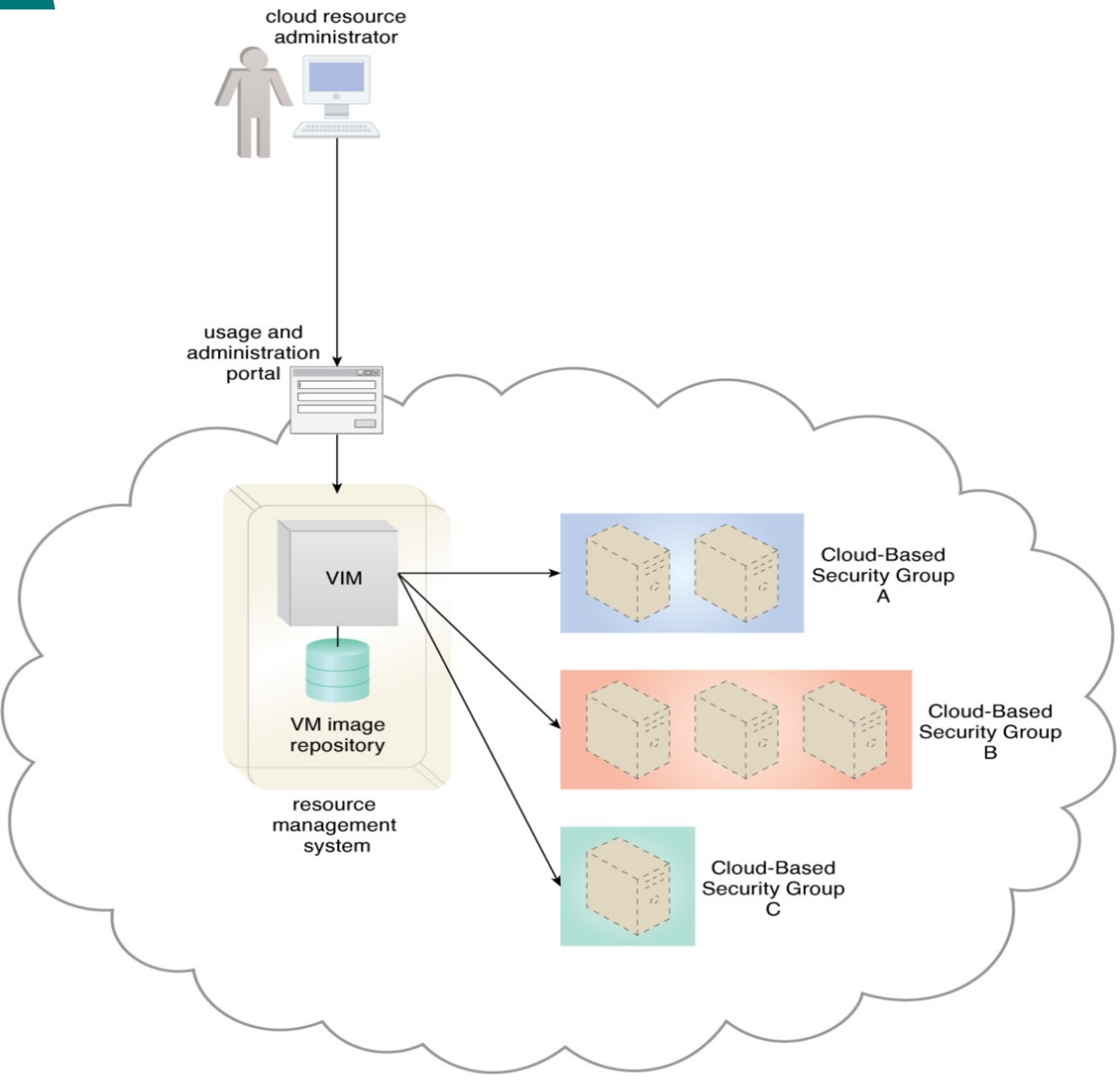
基于云的安全组

- 运行在同一个物理服务器上的多个虚拟服务器逻辑上可以是隶属于不同的基于云的安全组的成员。
- 基于云的安全组能限制对资源的未被授权的访问。
- 用来对抗
  - 拒绝服务、授权不足和信任边界重叠等威胁

Q&A：基于云的安全组是如何对抗拒绝服务、授权不足和信任边界重叠等威胁？


Cloud Consumer A
Cloud Consumer B
Cloud-Based Security Group A
Cloud-Based Security Group B
A
B
C
D
E
Copyright © Arcitura Education

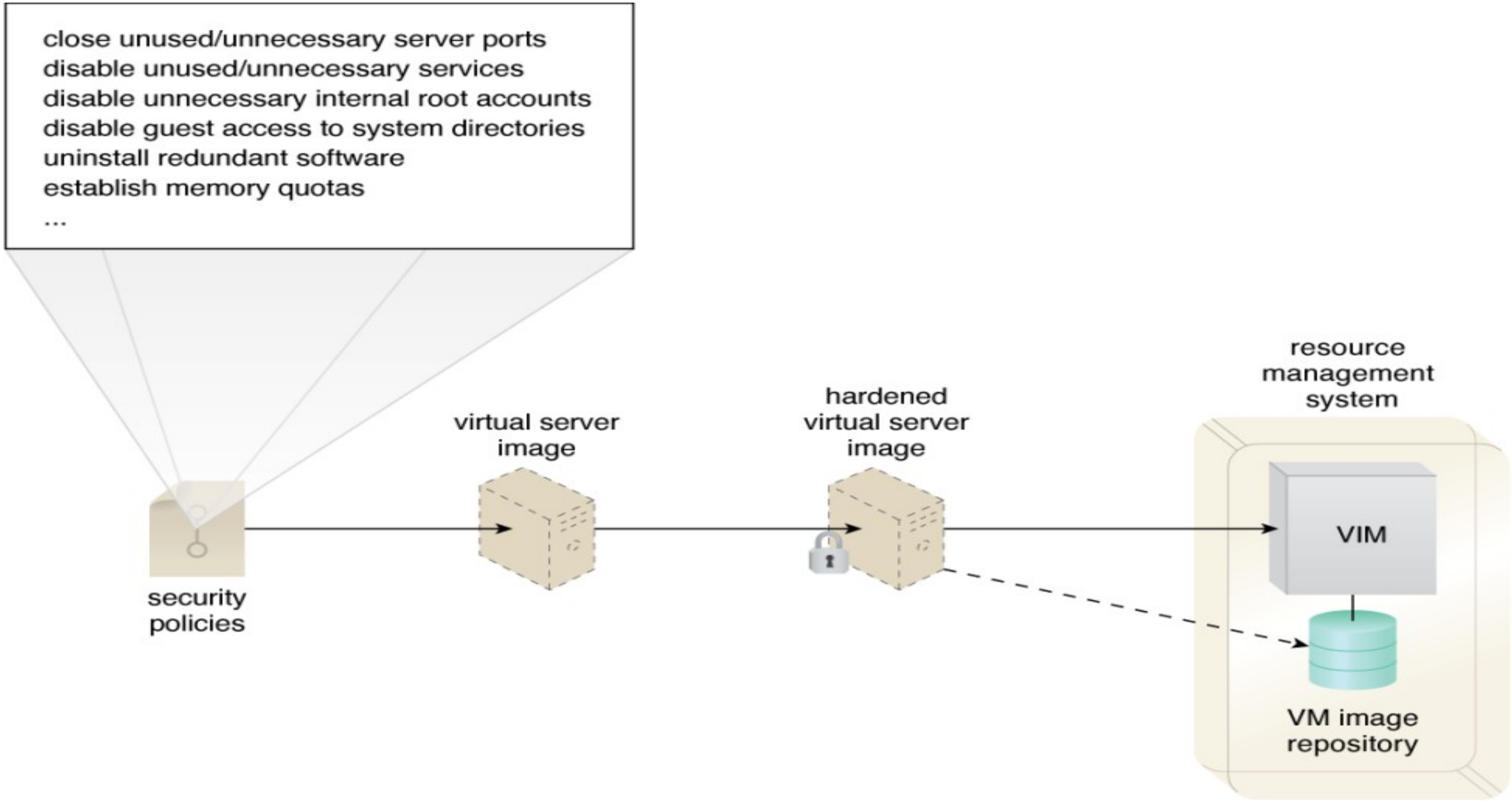
- Figure 10.11 – A logical cloud-based security group, Group A, is comprised of Virtual Servers A and D and assigned to Cloud Consumer A, while Group B is comprised of Virtual Servers B, C, and E and assigned to Cloud Consumer B. If Cloud Service Consumer A's user account is compromised, the attacker would only be able to damage the servers in Security Group A, thereby protecting Virtual Servers B, C, and E.


cloud resource administrator
usage and administration portal
VIM
VM image repository
resource management system
Cloud-Based Security Group A
Cloud-Based Security Group B
Cloud-Based Security Group C

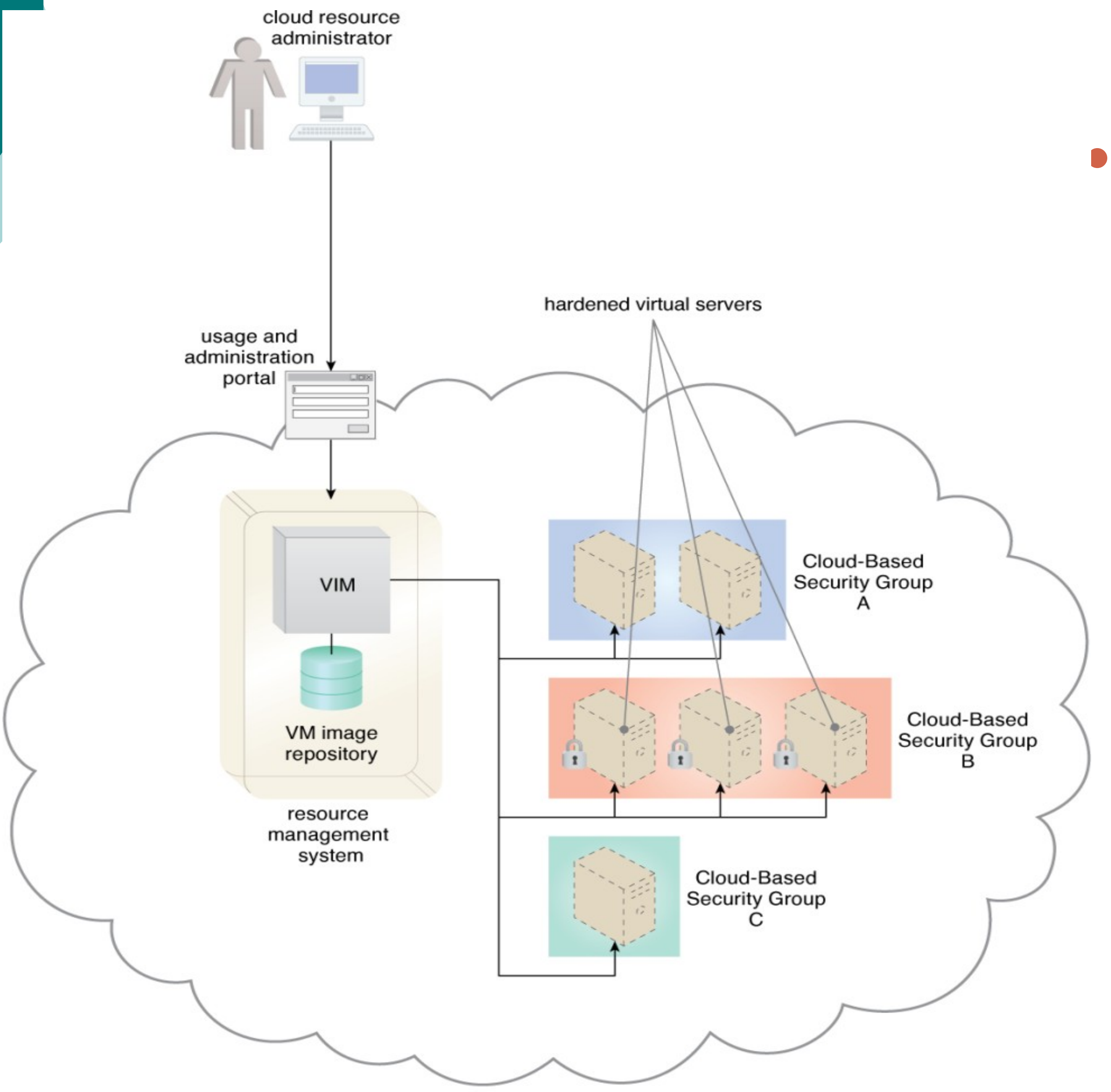
- Figure 10.12 – When an external cloud resource administrator accesses the web portal to allocate a virtual server, the requested security controls are assessed and mapped to an internal security policy that assigns a corresponding cloud-based security group to the new virtual server.

§10.8 强化的虚拟服务器映像

- 虚拟服务器镜像(VM image)
  - 一个从模板配置创建的虚拟服务器镜像
  - 比原始标准映像更加安全的虚拟服务器模板
- 强化(Hardening)
  - 把不必要的软件从系统中剥离出来，限制可能被攻击者利用的潜在漏洞的过程。
  - 去除冗余的程序，关闭不必要的服务器端口，关闭不使用的服务，内部root用户和guest访问等。
- 对抗拒绝服务、授权不足和信任边界重叠等威胁。


close unused/unnecessary server ports
disable unused/unnecessary services
disable unnecessary internal root accounts
disable guest access to system directories
uninstall redundant software
establish memory quotas
...
security policies
virtual server image
hardened virtual server image
resource management system
VIM
VM image repository

- *Figure 10.13 – A cloud provider applies its security policies to harden its standard virtual server images. The hardened image template is saved in the VM images repository as part of a resource management system.*


cloud resource administrator
usage and administration portal
hardened virtual servers
VIM
VM image repository
resource management system
Cloud-Based Security Group A
Cloud-Based Security Group B
Cloud-Based Security Group C

- Figure 10.14 – The cloud resource administrator chooses the hardened virtual server image option for the virtual servers provisioned for Cloud-Based Security Group B.

本章小结

- 云安全的基本措施和技术
  - 加密、哈希、签名、PKI
- 云安全的相关机制
  - 身份认证与访问控制
  - 单一登录
  - 安全组
  - 虚拟服务器强化

课后题

无。