DALHOUSIE UNIVERSITY

Inspiring Minds

CLOUD SECURITY MECHANISMS

CSCI 5408:

Data Management, Warehousing, and Analytics

Prepared By: Suhaib Qaiser (suhaibqaiser@dal.ca)

Symmetric and Asymmetric Encryption

Hashing

Digital Signature

Public Key Infrastructure (PKI)

Identity Access Management

Single Sign-On

Security Groups

Firewalls

Security Groups

Recap on last lecture …

Q1. What are the three components of Remote Administration System on Cloud Provider?

Q2. Name 6 advantages of Version Control System?

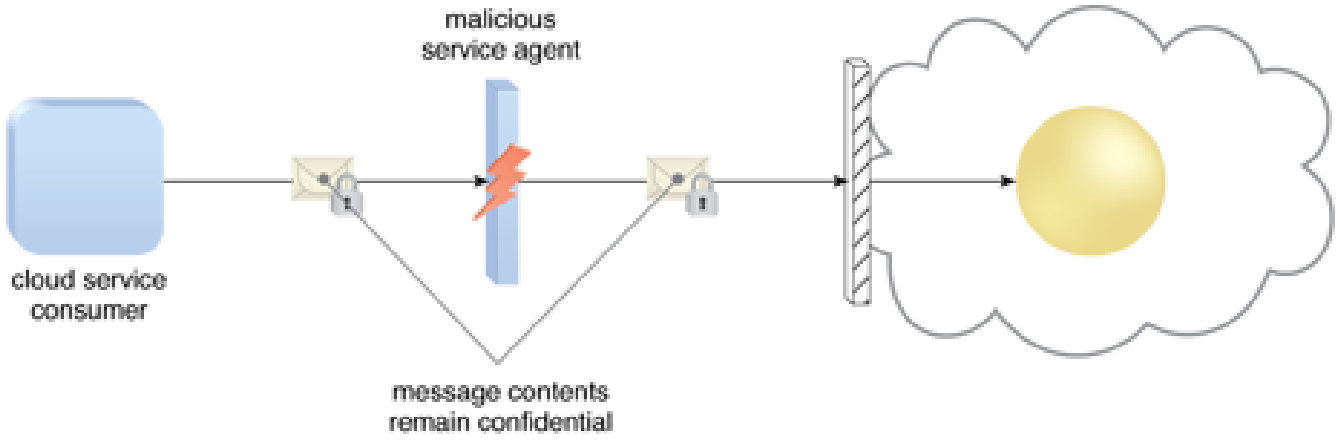
Q3. What is the main benefit of using Distributed Version Control System?

Q4. State three differences between analytical information provided by Salesforce and Heroku

Q5. Difference between guest machine and host machine?

Q6. What are the roles of a hypervisor in private cloud versus public cloud?

Encryption



Encryption mechanism commonly relies on a standard algorithm called a cipher to transform original plain text into cipher text

Access to cipher text does not expose original data. It is always hidden from general public

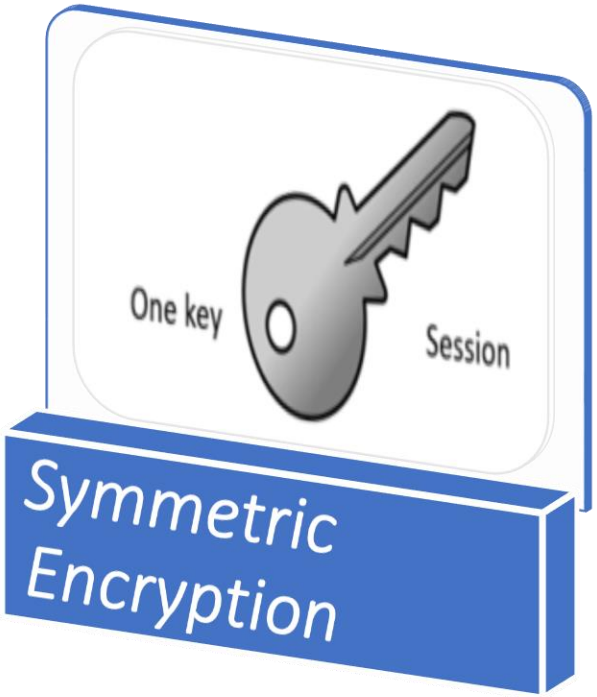
An encryption key is used to encrypt data and decrypt it

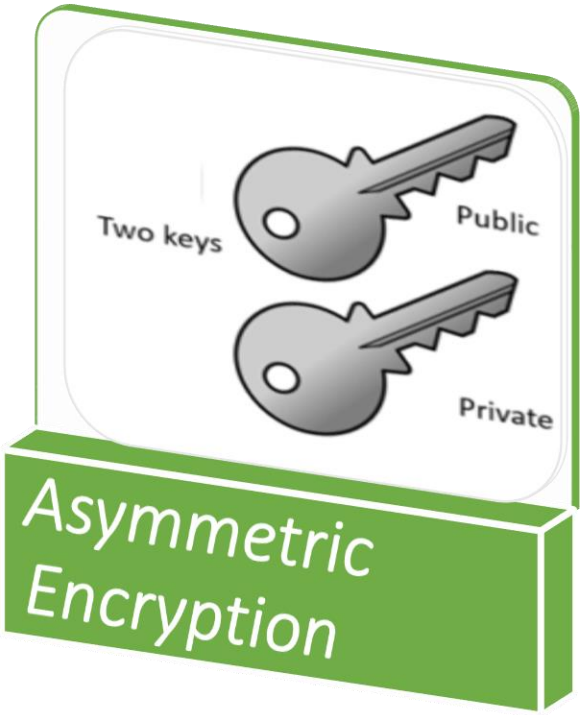
The encryption mechanism is a digital coding system dedicated to preserving the confidentiality and integrity of data

The encryption mechanism can help counter the traffic eavesdropping, malicious intermediary, insufficient authorization, and overlapping trust boundaries security treats

Source: http://servicetechbooks.com/cloud/figures

Symmetric and Asymmetric Encryption





Overview of Symmetric and Asymmetric Encryption

Encryption provides confidentiality and prevents unauthorized disclosure of data

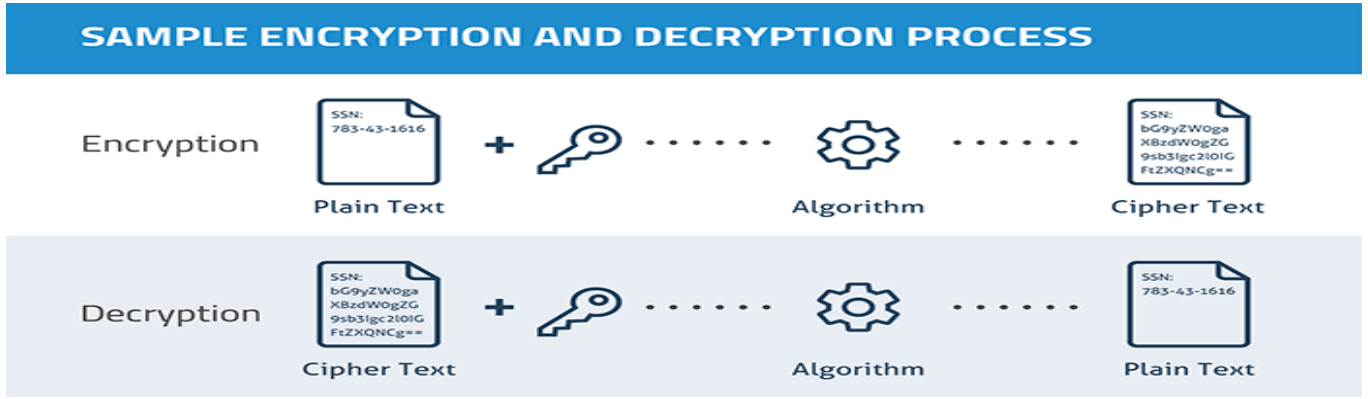
Encrypted data is in a ciphertext format that is unreadable

Attackers can't read encrypted traffic sent over a network or encrypted data stored on a system

In contrast, if data is sent in clear text, an attacker can capture and read the data using a protocol analyzer

Encryption scrambles, or ciphers, data to make it unreadable if intercepted

Encryption normally includes an algorithm and a key



References:

- http://blogs.getcertifiedgetahead.com/symmetric-and-asymmetric-encryption/,
- http://www.slideshare.net/RituparnaNag/cloud-encryption-52204838 ,
- https://www3.skyhighnetworks.com/cloud-security- university/tokenization-vs-encryption/

Overview of Symmetric and Asymmetric Encryption

Encryption scrambles, or ciphers, data to make it unreadable if intercepted. Encryption normally includes an algorithm and a key.

Symmetric encryption uses the same key to encrypt and decrypt data.

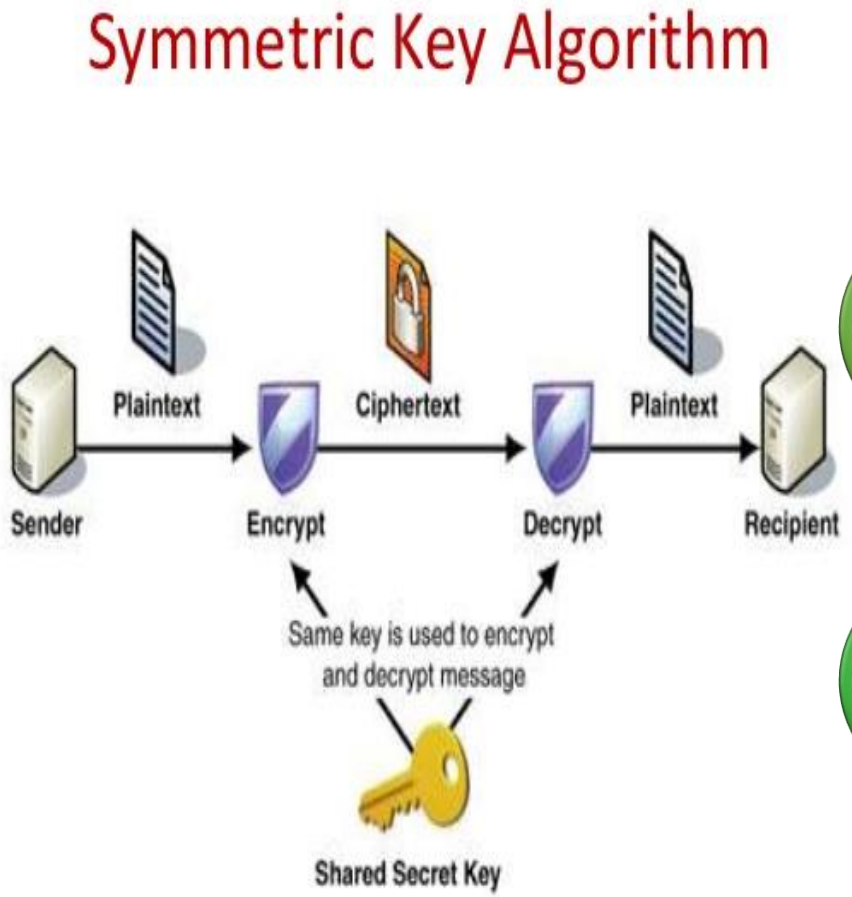
Asymmetric encryption uses two keys (public and private) created as a matched pair.

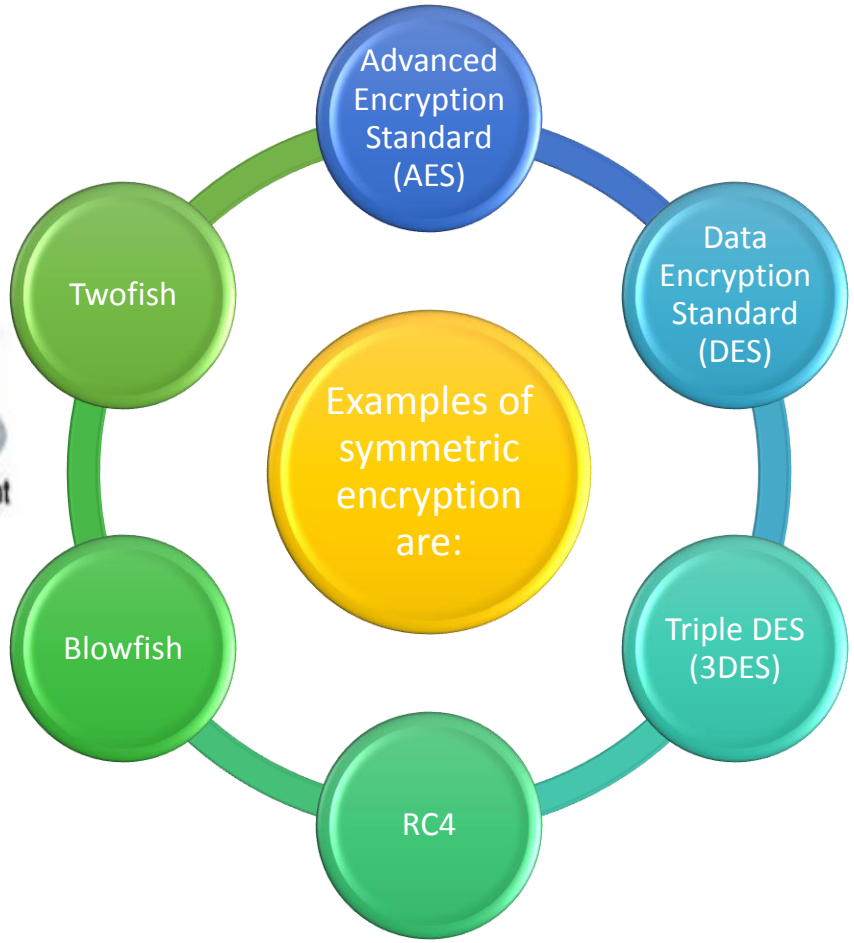
- Anything encrypted with the public key can only be decrypted with the matching private key.
- Anything encrypted with the private key can only be decrypted with the matching public key.

http://blogs.getcertifiedgetahead.com/symmetric-and-asymmetric-encryption/

Symmetric Encryption

Symmetric encryption uses the same key to encrypt and decrypt data. In other words, if you encrypt data with a key of three, you decrypt it with the same key of three. Symmetric encryption is also called secret-key encryption or session-key encryption





http://blogs.getcertifiedgetahead.com/symmetric-and-asymmetric-encryption/

Symmetric Encryption (OPTIONAL READING)

RC4 - Weak, but fast; implemented in the minimal protection of WEP (Wired Equivalent Privacy); small RAM requirement makes it usable for mobile devices; implemented in @50 lines of code. Poor implementation yields minimal protection

DES - *Data Encryption Standard* / a single **56-bit key** algorithm and process developed by IBM in 1974 for NIST & later adopted as both an ANSI and ISO standard used by general public

- **64-bit block cipher** (encrypts 64 bits at a time) with ***substitution & transposition*** thru 16 cycles or iterations of activity
- vulnerable to exhaustive key search by modern computers (2^{56} possibilities)
- 1997, consolidated attack via 3500 computers inferred a key in 4 months
- 1998, cracker machine found key in 4 days

3DES - DES applied for 3 cycles (=112 bit with 3 keys) to strengthen the aging DES method & keep it viable; slow processing (= expensive $) & too slow for personal computers; encrypt/decrypt/encrypt cycle, each with a different key; adopted to strengthen original DES implementation without requiring major programming changes.

AES - Advanced Encryption Standard - 2001 - latest standard; implemented via @350 lines of code but efficient enough to run on mobile devices; strong mathematical foundation

- fast & efficient algorithm, with 4-step process, variable key-length (128, 192, 256 bit); longer keys may be added
- 128 bit block size, variable factors & repetition add complexity, number of cycles is variable
- combines byte substitution, transposition, XoR, row shifts, mixed column phase, multiple matrices, subkeys
- implemented in 802.11, IPsec, S/MIME, TLS

Source: http://itm455.itmbsu.net/Notes/L6_Elements_of_Cryptography.htm

Asymmetric Encryption

Asymmetric (public key) - a **pair** of mathematically related keys, **public and private**, is used for specialized encryption tasks that justify the processing overhead (up to 10k times slower than symmetric). Each user has his/her own key pair, and shares their public key only

The **private key is always kept private**, and **never shared.**

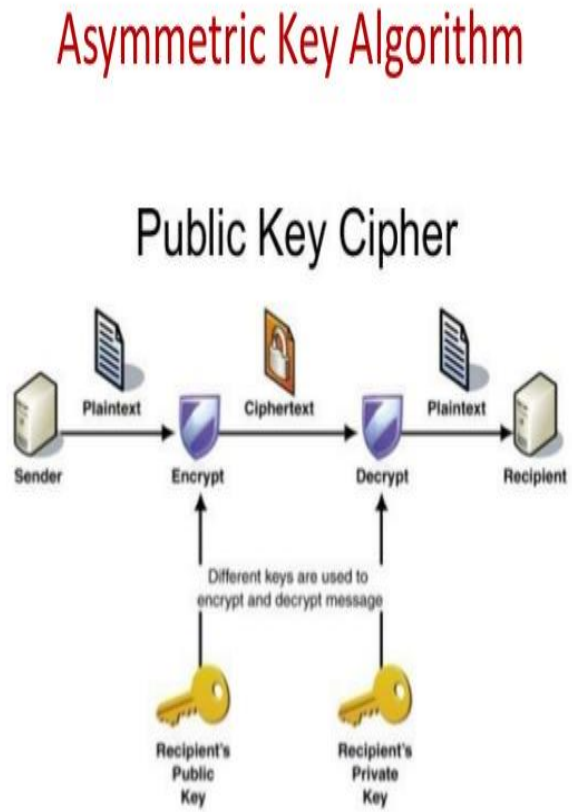
when a message is encrypted with a private key, it can only be decrypted with the paired public key. A message encrypted with a public key can only be decrypted with its paired private key

Asymmetric encryption is considered "reversible," as there is an option as to which key is used for encryption & they accomplish different things

Implemented in SSL & TLS transactions

Hash - one-way functions that build a unique message representation without a key; verifies integrity & authentication; not reversible, but repeatable, also called message digests; a message fingerprint

Utilized ECC - elliptical curve cryptography; strong even with shorter keys, fast & efficient



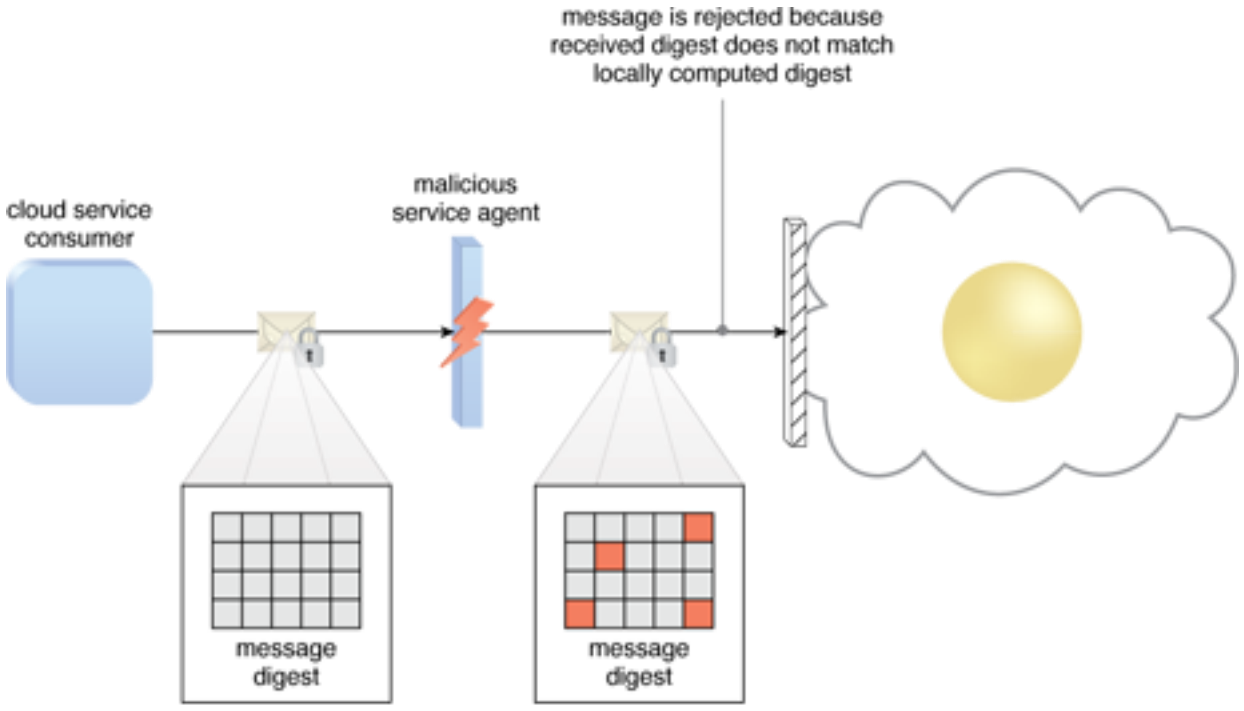
Source: http://itm455.itmbsu.net/Notes/L6_Elements_of_Cryptography.htm

Encryption Algorithms Types

SYMMETRIC	ASYMMETRIC
AES (AES-128, AES-192, AES-256)	Diffie-Hellman key exchange
Blowfish	RSA asymmetric algorithm
Twofish	SHA-224
DES	SHA-256
3DES	SHA-386
RC4	SHA-512
	SHA-3 (emerging standard)

http://searchsecurity.techtarget.com/answer/What-are-the-differences-between-symmetric-and-asymmetric-encryption-algorithms

Hashing



The hashing mechanism is used when one-way, non-reversible form of data protection is required

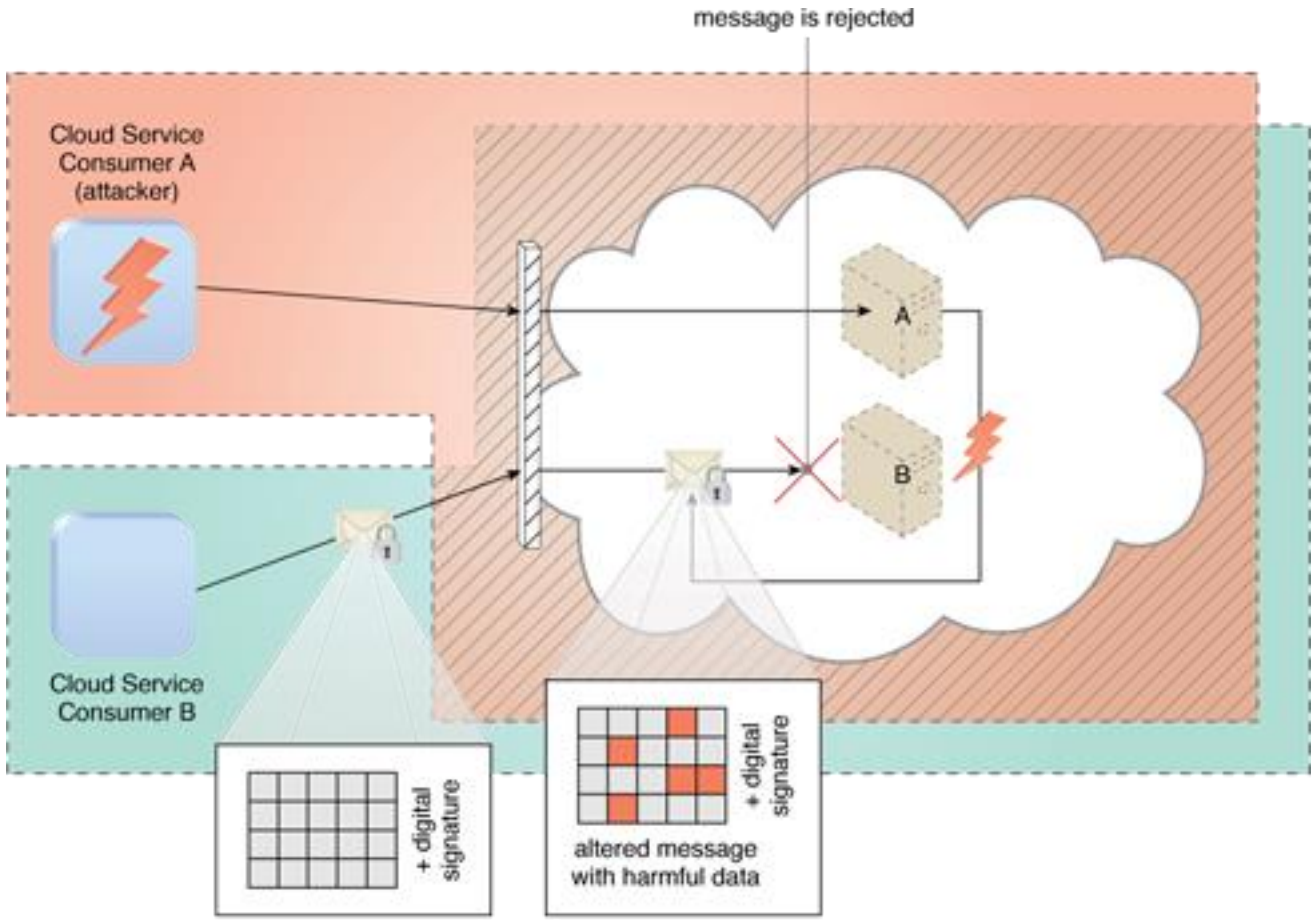
It is locked and no key is provided for the message to be unlocked

A common application of this mechanism is the storage of passwords

Hashing can be used to derive a message digest from original message

The recipient applies the same mechanism to the message and compare message digest with sender's digest to verify the authenticity of the message

Digital Signature

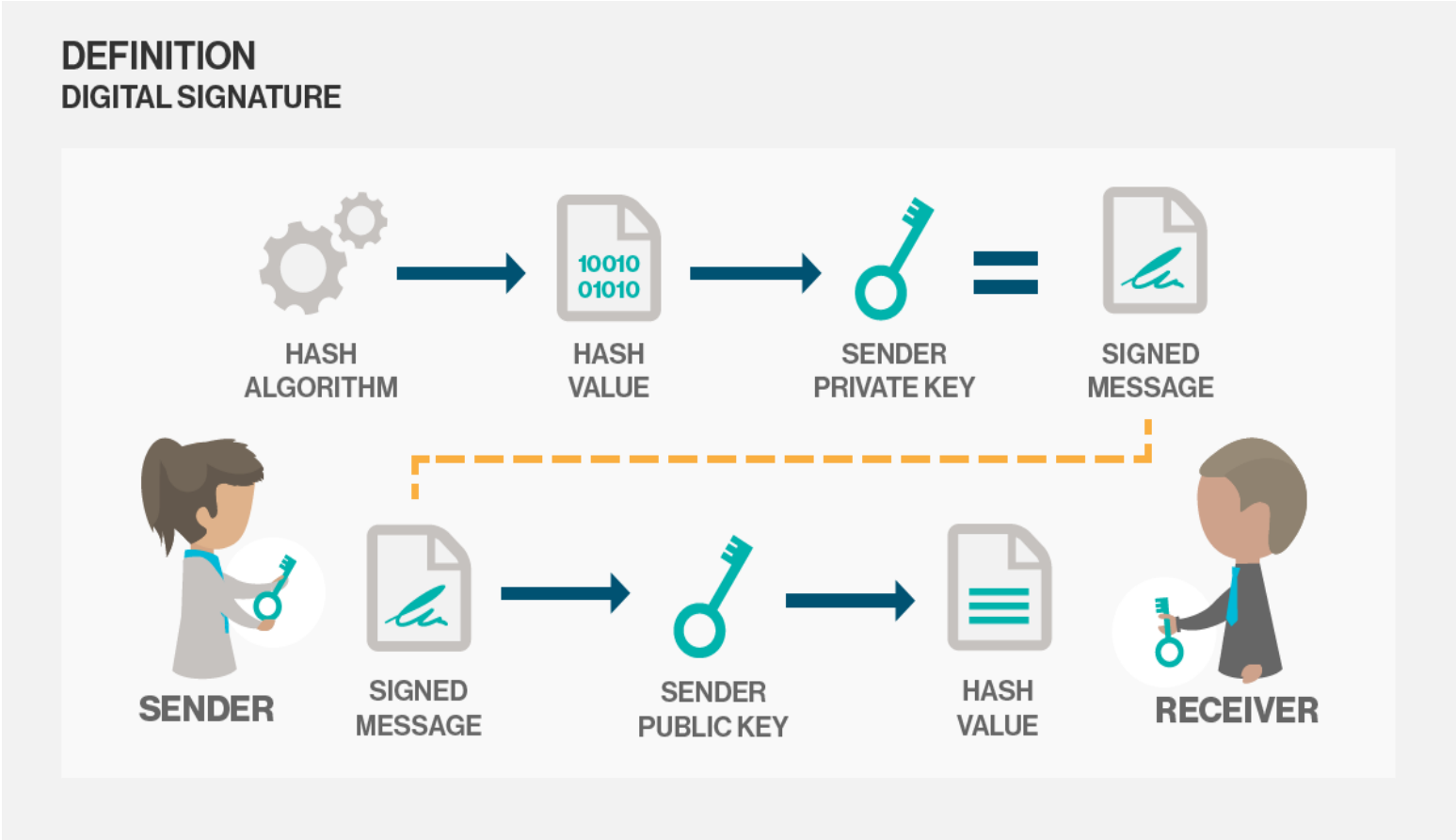


Digital Signature mechanism is a means of providing data authenticity and integrity through authentication and non-repudiation.

A message is assigned a digital signature prior to the transmission of message, which is then rendered invalid if message is changed or altered during transmission to receiver. Receiver has a way of identifying message authenticity through digital signature

You should sign the message with senders name appended and then encrypt it instead of vice versa

Digital Signature



Source: http://searchsecurity.techtarget.com/definition/digital-signature

Public Key Infrastructure (PKI)

A public key infrastructure (PKI) supports the distribution and identification of public encryption Keys,

Enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.

Without PKI, sensitive information can still be encrypted (ensuring confidentiality) and exchanged, but there would be no assurance of the identity (authentication) of the other party.

Any form of sensitive data exchanged over the Internet is reliant on PKI for security

Public Key Infrastructure (PKI)

A typical PKI consists

To manage the creation, administration, distribution and revocation of keys and Digital Certificates

A typical PKI includes the following key elements

1:Certificate authority (CA):A trusted party, called a certificate authority (CA), acts as the root of trust and provides services that authenticate the identity of individuals, computers and other entities

2:Registration authority: A registration authority, often called a subordinate CA, certified by a root CA to issue certificates for specific uses permitted by the root

3:Certificate database : A certificate database, which stores certificate requests and issues and revokes certificates

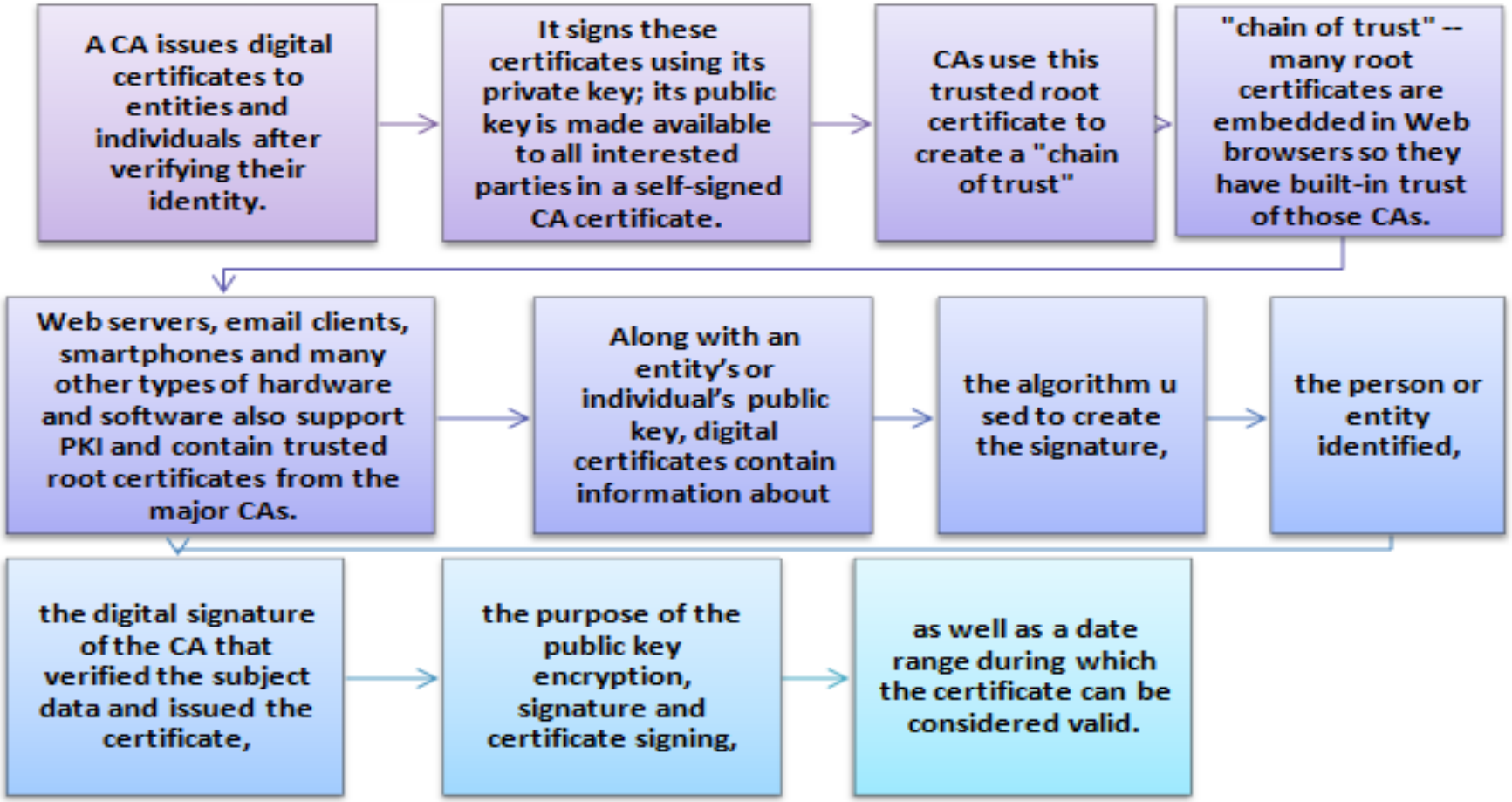
4:Certificate store : A certificate store, which resides on a local computer as a place to store issued certificates and private keys

Public Key Infrastructure (PKI)

DIGITAL CERTIFICATES

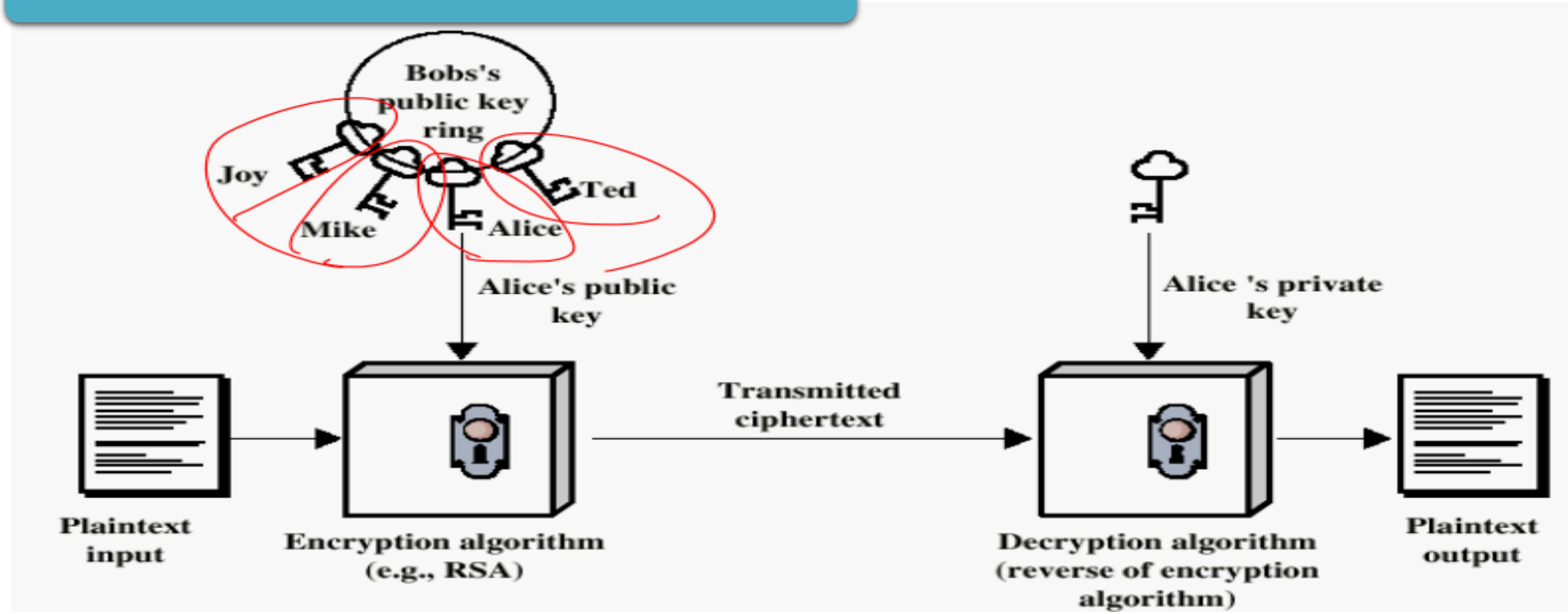
Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate

HOW IT WORKS



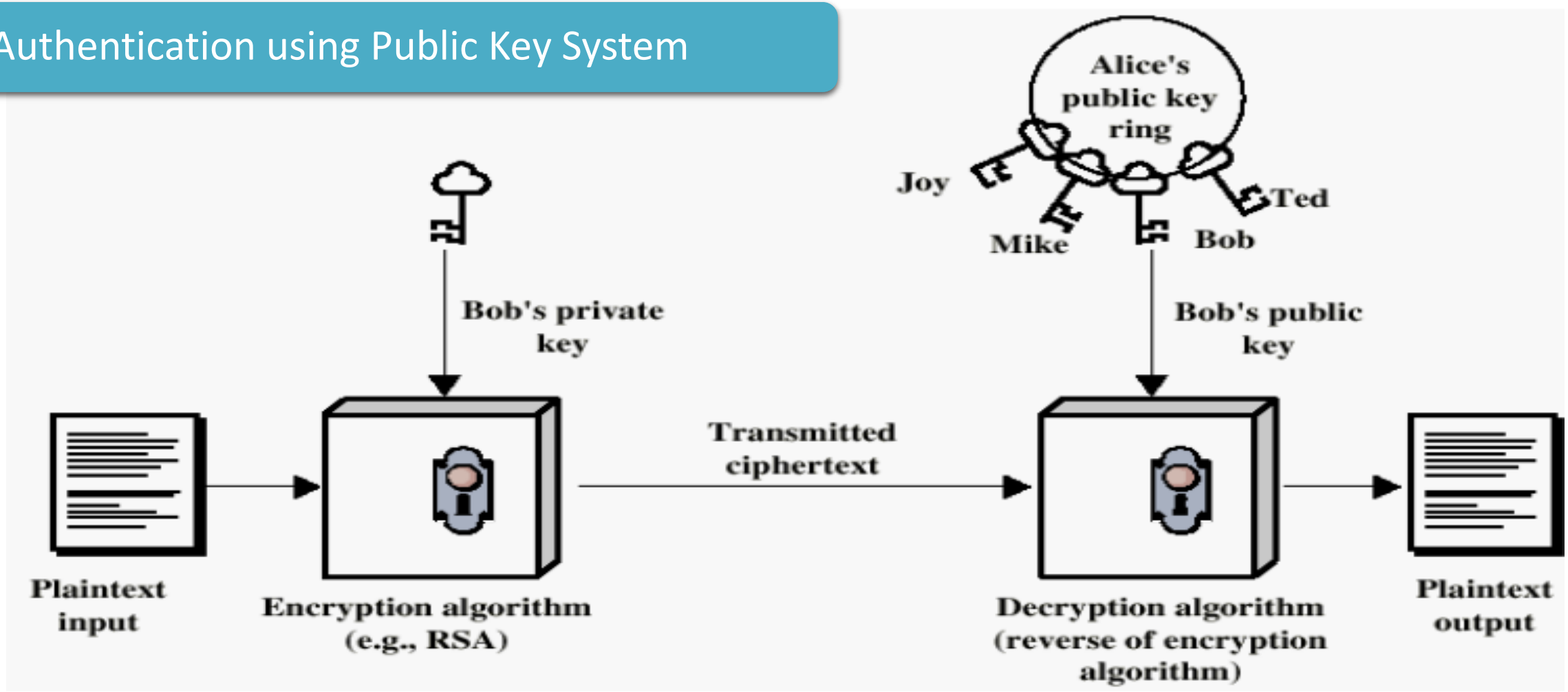
Public Key Infrastructure (PKI)

Encryption using Public-Key system



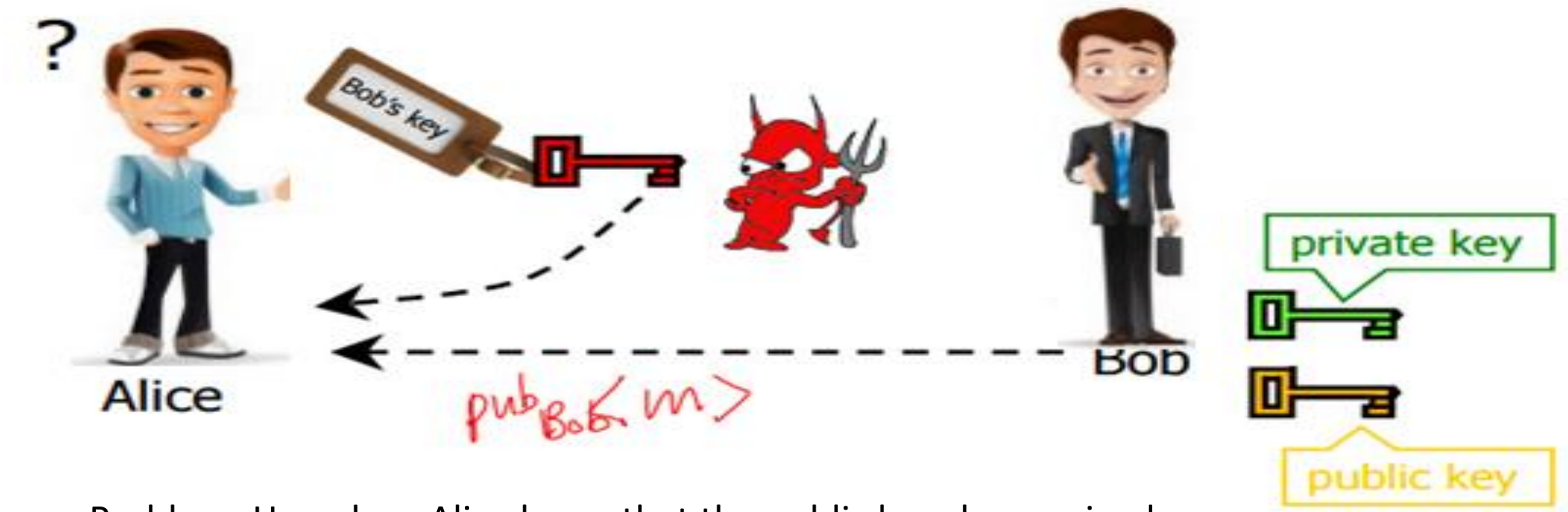
Public Key Infrastructure (PKI)

Authentication using Public Key System



Public Key Infrastructure (PKI)

Authenticity of Public Keys



Problem: How does Alice know that the public key she received is really Bob's public key?

Public Key Infrastructure (PKI)

Distribution of Public Keys !

Public announcement or public directory

- Risks: forgery and tampering !

Public-key certificate

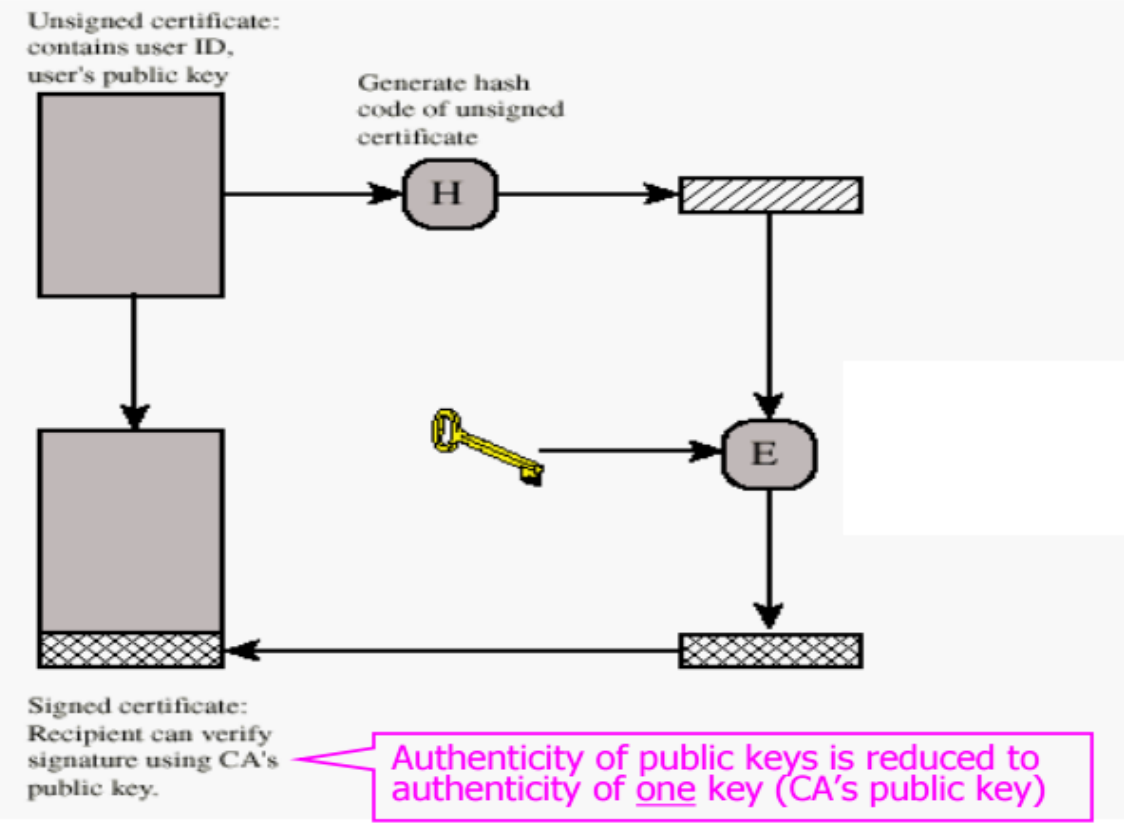
- Signed statement specifying the key and identity – sigAlice("Bob", PKB) !

Common approach: certificate authority (CA)

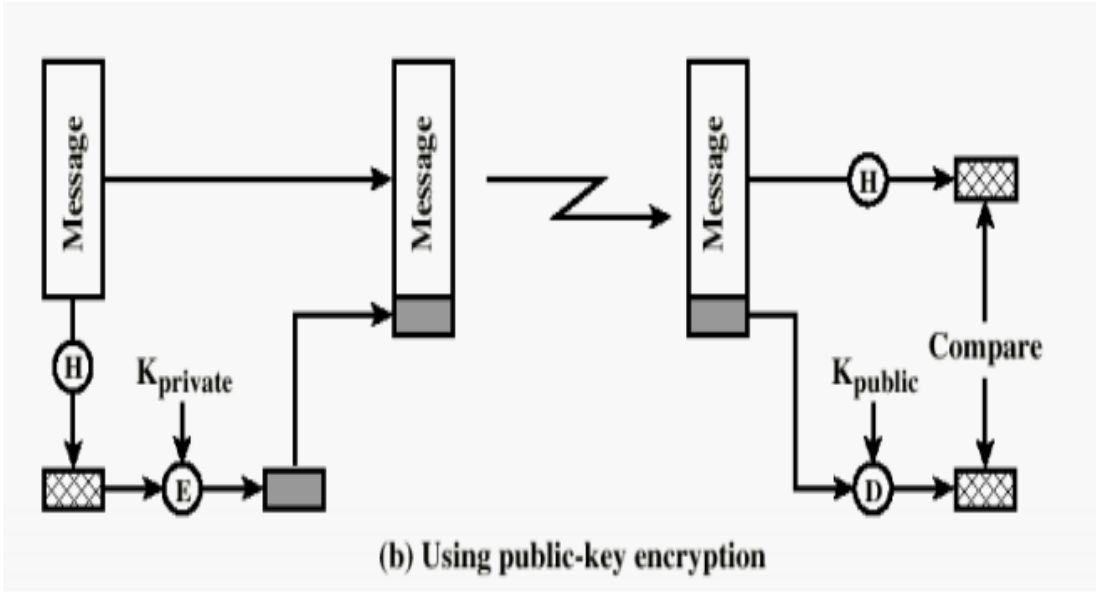
- Single agency responsible for certifying public keys
- After generating a private/public key pair, user proves his identity and knowledge of the private key to obtain CA's certificate for the public key (offline)

Public Key Infrastructure (PKI)

Using Public-Key Certificates



Typical Digital Signature Approach



(b) Using public-key encryption

Henric Johnson

Public Key Infrastructure (PKI)

Hierarchical Approach

Single CA certifying every public key is impractical !

Instead, use a trusted root authority

- For example, Verisign
- Everybody must know the public key for verifying root authority's signatures !

Root authority signs certificates for lower-level authorities, lower-level authorities sign certificates for individual networks, and so on

- Instead of a single certificate, use a certificate chain – sigVerisign("UI", PKUI), sigUI ("EJ Jung", PKE)
- What happens if root authority is ever compromised?

Revocation of Certificates

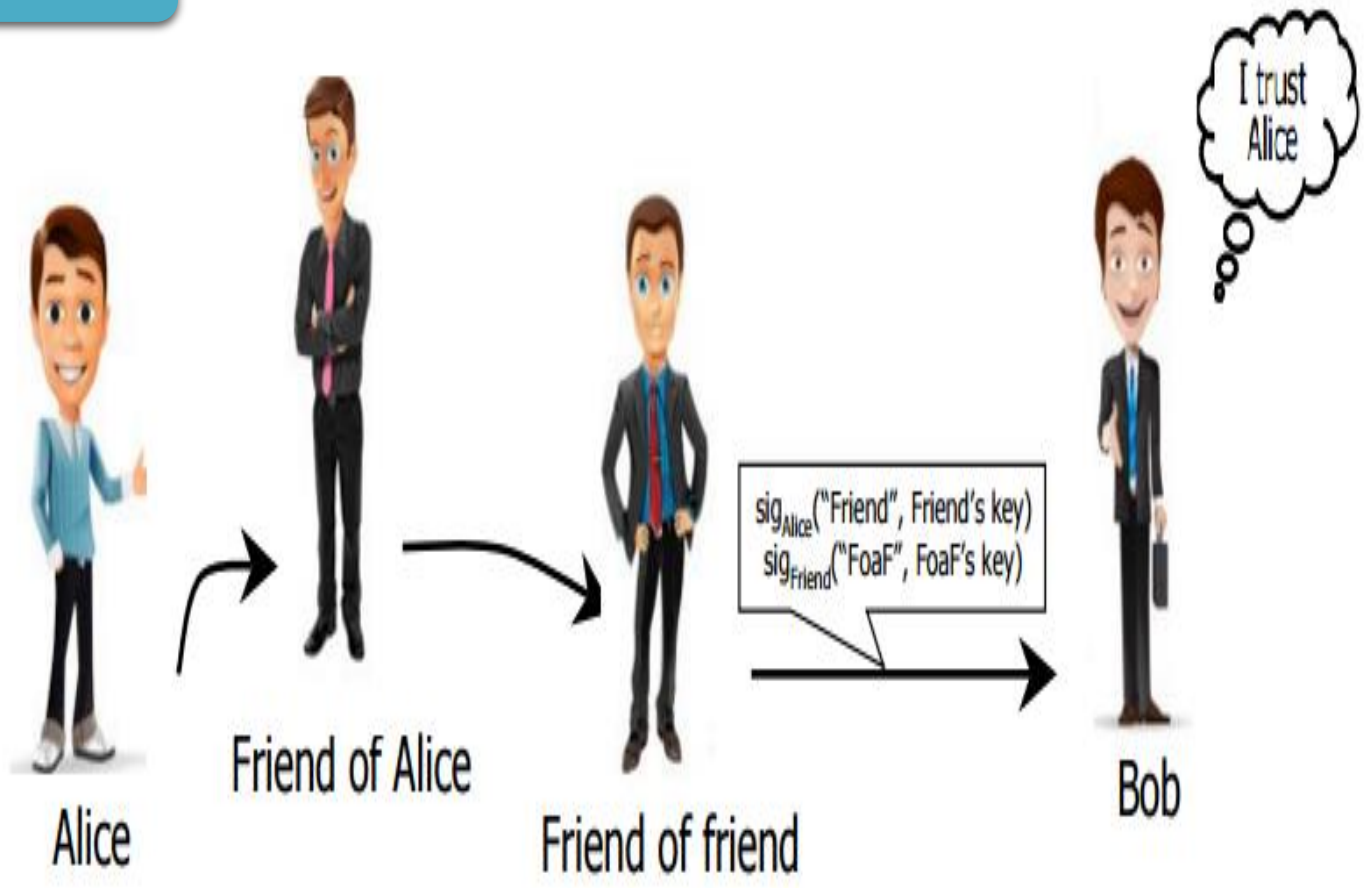
Reasons for revocation:

- The users secret key is assumed to be compromised.
- The user is no longer certified by this CA.
- The CA's certificate is assumed to be compromised

Public Key Infrastructure (PKI)

Alternative: "Web of Trust" !

- Used in PGP (Pretty Good Privacy) !
- Instead of a single root certificate authority, each person has a set of keys they "trust"
- If public-key certificate is signed by one of the "trusted" keys, the public key contained in it will be deemed valid
- Trust can be transitive
- Can use certified keys for further certification



Identity Access Management

DEFINITION

An identity management access (IAM) system is a framework for business processes that facilitates the management of electronic identities. The framework includes the technology needed to support

Identity Management Interface such as Ethernet

DEFINITION

In computer security, **identity** and **access management** (IAM) is the security and business discipline that "enables the right individuals to **access** the right resources at the right times and for the right reasons".
Source: Identity management - Wikipedia

DEFINITION

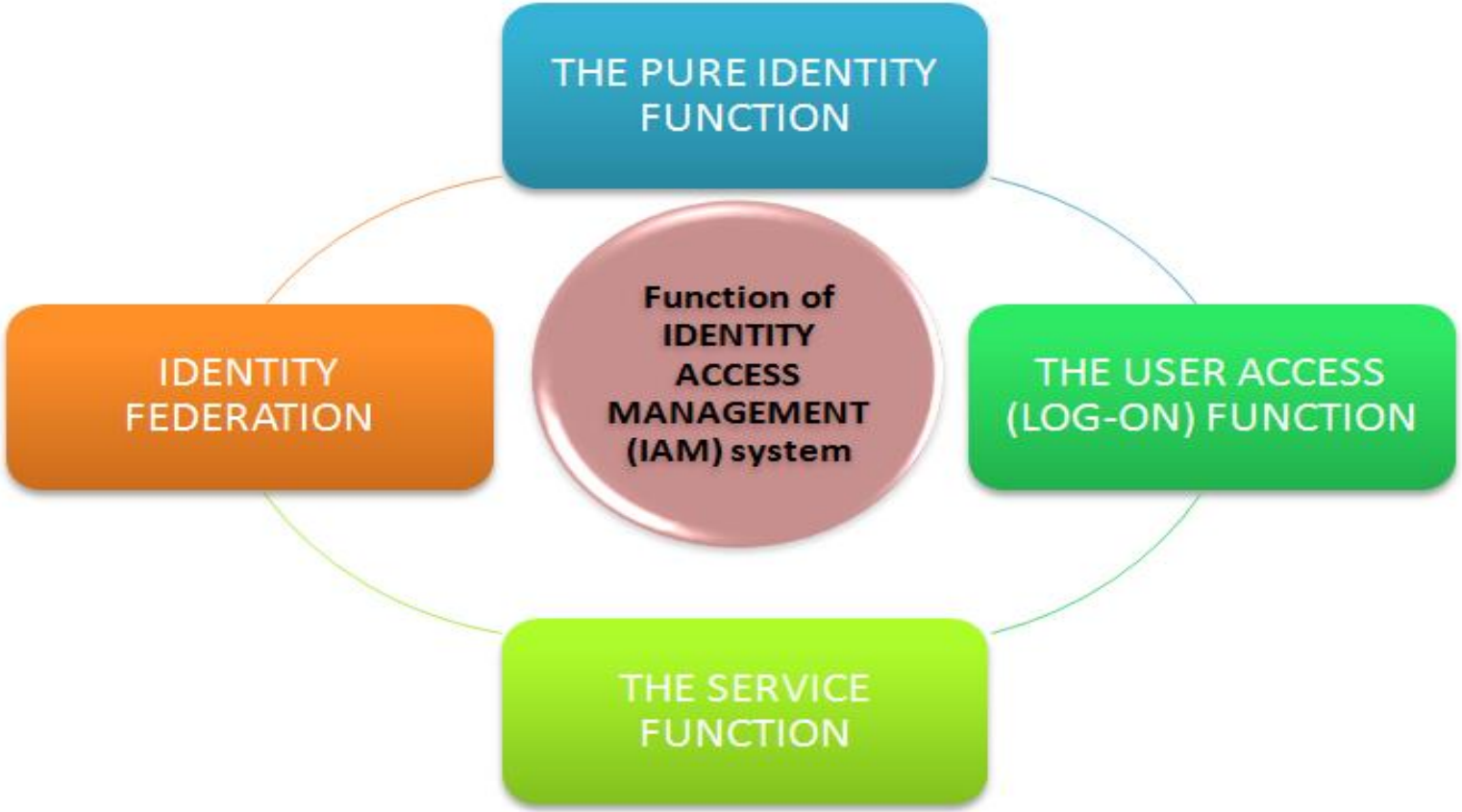
Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.

Source: http://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system
https://en.wikipedia.org/wiki/**Identity_management**

Identity Access Management

Function of identity access management (IAM) system

In the real-world context of engineering online systems, identity management can involve four basic functions:



https://en.wikipedia.org/wiki/Identity_management#User_access

Identity Access Management

System capabilities: OF IDENTITY ACCESS MANAGEMENT (IAM) system

Authentication : Verification that an entity is who/what it claims to be using a password, biometrics such as a fingerprint, or distinctive behavior such as a gesture pattern on a touchscreen.

Authorization : Managing authorization information that defines what operations an entity can perform in the context of a specific application. For example, one user might be authorized to enter a sales order, while a different user is authorized to approve the credit request for that order.

Roles : Roles are groups of operations and/or other roles. Users are granted roles often related to a particular job or job function. For example, a user administrator role might be authorized to reset a user's password, while a system administrator role might have the ability to assign a user to a specific server.

Delegation : Delegation allows local administrators or supervisors to perform system modifications without a global administrator or for one user to allow another to perform actions on their behalf. For example, a user could delegate the right to manage office-related information.

Interchange : The SAML protocol is a prominent means used to exchange identity information between two identity domains.[7] For non-SAML enabled devices there exist tools, like the SMRTe, which can be used to exchange identity information

https://en.wikipedia.org/wiki/Identity_management#User_access

Identity Access Management

Function OF IDENTITY ACCESS MANAGEMENT (IAM) system

THE PURE IDENTITY FUNCTION

Creation, management and deletion of identities without regard to access or entitlements

A general model of identity can be constructed from a small set of axioms, for example that all identities in a given namespace are unique, or that such identities bear a specific relationship to corresponding entities in the real world.Such an axiomatic model expresses "pure identity" in the sense that the model is not constrained by a specific application context

In general, an entity (real or virtual) can have multiple identities and each identity can encompass multiple attributes, some of which are unique within a given name space

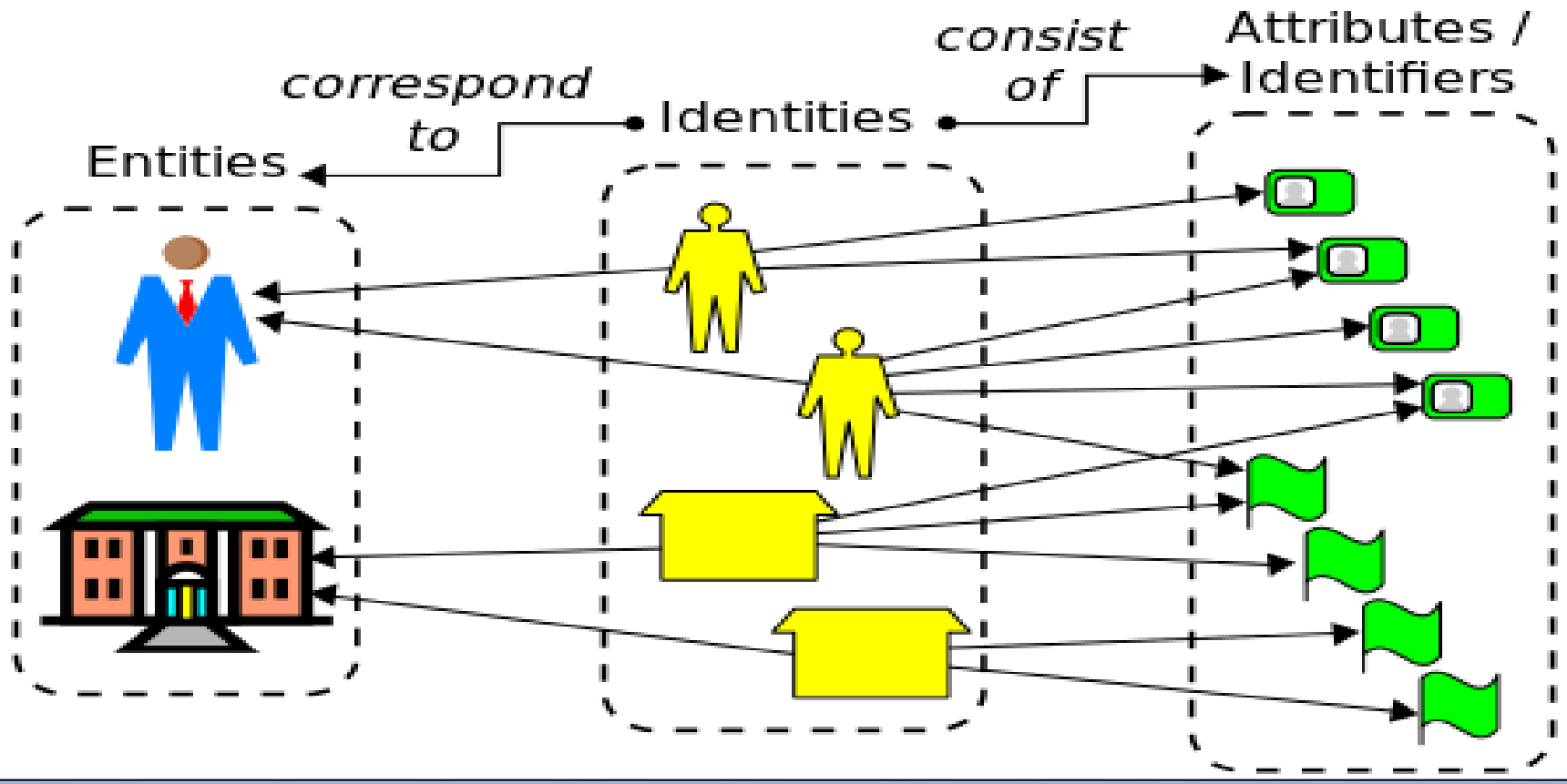
https://en.wikipedia.org/wiki/Identity_management#User_access

Identity Access Management

Function OF IDENTITY ACCESS MANAGEMENT (IAM) system

THE PURE IDENTITY FUNCTION

The diagram below illustrates the conceptual relationship between identities and entities, as well as between identities and their attributes.



https://en.wikipedia.org/wiki/Identity_management#User_access

Identity Access Management

Function OF IDENTITY ACCESS MANAGEMENT (IAM) system

THE USER ACCESS (LOG-ON) FUNCTION

A SMART CARD and its associated data used by a customer to log on to a service or services (a traditional view);

User access enables users to assume a specific digital identity across applications, which enables access controls to be assigned and evaluated against this identity. The use of a single identity for a given user across multiple systems eases tasks for administrators and users. It simplifies access monitoring and verification and allows the organization to minimize excessive privileges granted to one user. User access can be tracked from initiation to termination of user access

When organizations deploy an identity management process or system, their motivation is normally not primarily to manage a set of identities, but rather to grant appropriate access rights to those entities via their identities. In other words, access management is normally the motivation for identity management and the two sets of processes are consequently closely related

https://en.wikipedia.org/wiki/Identity_management#User_access

Identity Access Management

Function OF IDENTITY ACCESS MANAGEMENT (IAM) system

THE SERVICE FUNCTION

A system that delivers personalized, role-based, online, on-demand, multimedia (content),presence – based-services to users and their devices.

Organizations continue to add services for both internal users and by customers. Many such services require identity management to properly provide these services. Increasingly, identity management has been partitioned from application functions so that a single identity can serve many or even all of an organization's activities.

For internal use identity management is evolving to control access to all digital assets, including devices, network equipment, servers, portals, content, applications and/or products.

Services often require access to extensive information about a user, including address books, preferences, entitlements and contact information. Since much of this information is subject to privacy and/or confidentiality requirements, controlling access to it is vital.

https://en.wikipedia.org/wiki/Identity_management#User_access

Identity Access Management

What Should IDENTITY ACCESS MANAGEMENT (IAM) system Include

https://en.wikipedia.org/wiki/Identity_management#User_access

Identity Access Management

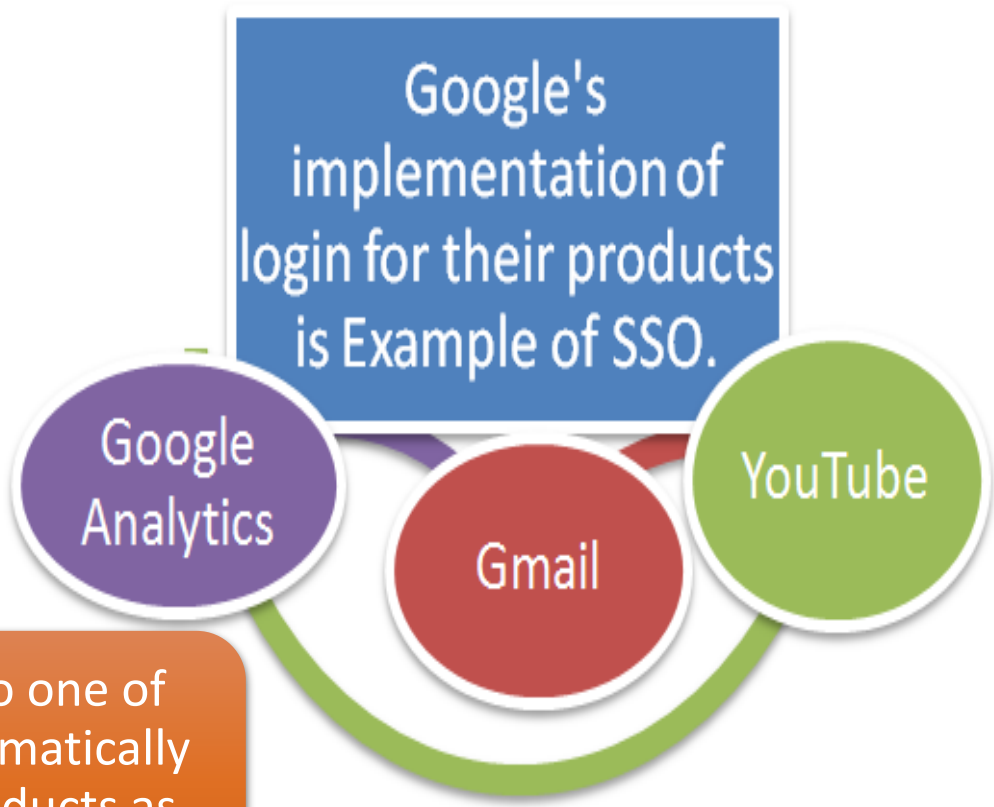
Identity and Access Management Solutions Directory

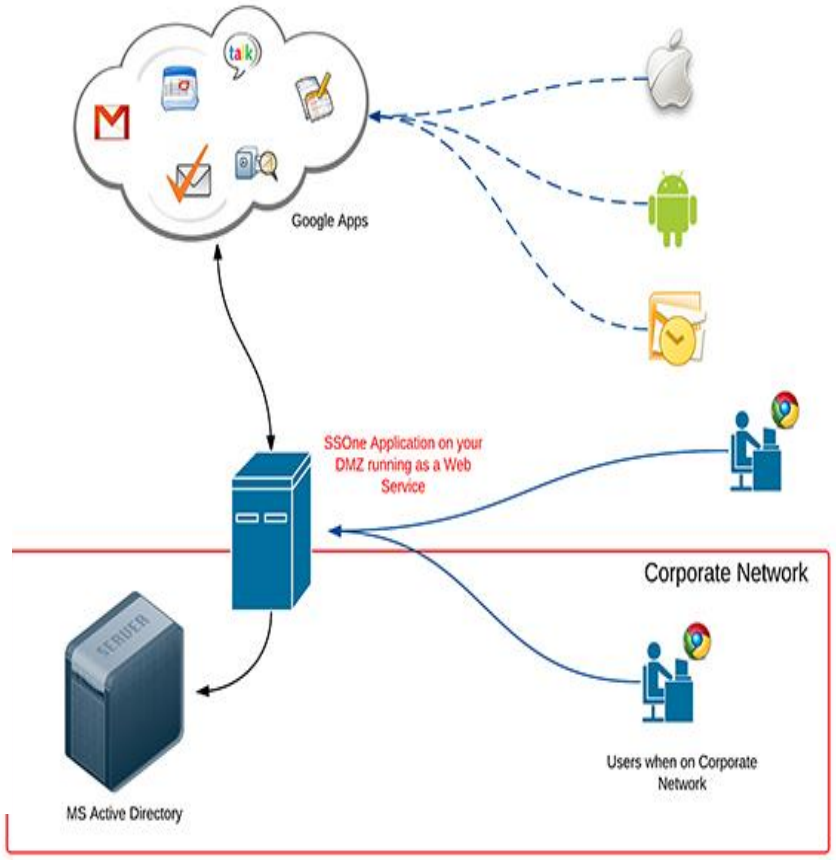
http://solutionsreview.com/identity-management/identity-management-solutions-directory/

Single Sign-On

What is SSO (Single Sign On)?

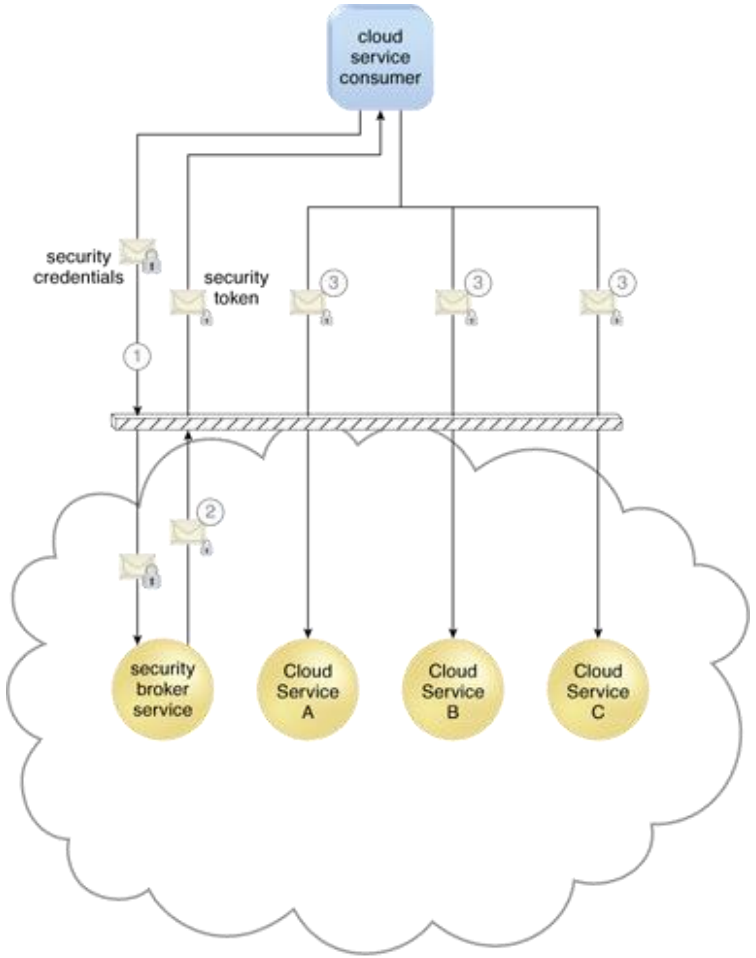
SSO (Single Sign On) occurs when a user logs in to one Client and is then signed in to other Clients automatically, regardless of the platform, technology, or domain the user is using





Any user that is logged in to one of Google's products are automatically logged in to their other products as well

Single Sign-On on Clouds



The single sign-on (SSO) mechanism enables one cloud service consumer to be authenticated by a security broker, which establishes a security context usually in form of a security token

This security token can be used between many service providers to authenticate a user

The SSO mechanism essentially enables mutually independent cloud services and IT resources to generate and circulate runtime authentication and authorization credentials

Single Sign-On

How It works

Single Sign On usually makes use of a *Central Service* which orchestrates the single sign on between multiple clients.

In the example of Google, this central service is Google Accounts.

When a user first logs in, Google Accounts creates a cookie, which persists with the user as they navigate to other Google-owned services.

https://www.oneall.com/services/single-sign-on/

Single Sign-On

The process flow is as follows:

https://auth0.com/docs/sso

Single Sign-On

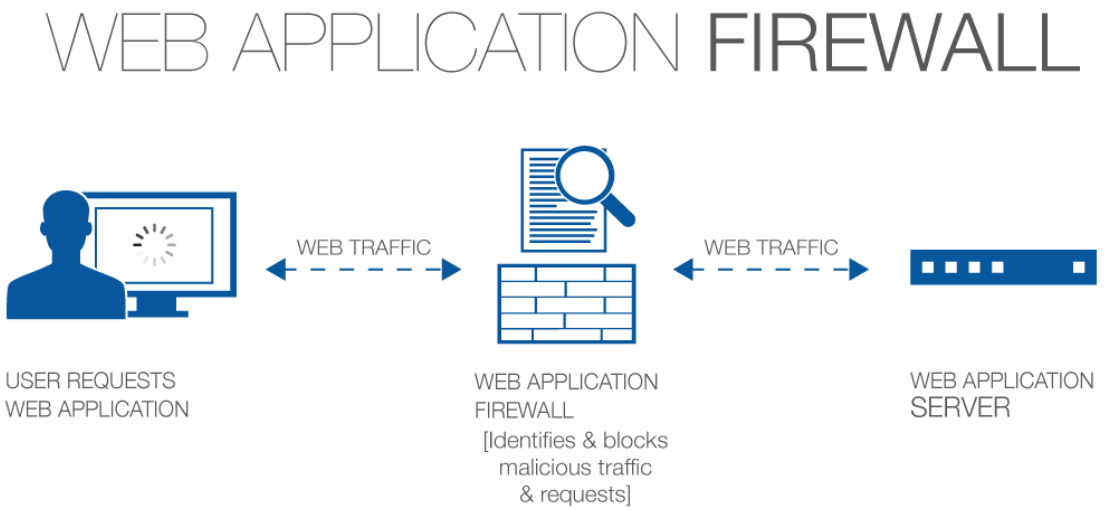
With *Single Sign-On (SSO)* you can **automatically sign in users** as they browse between multiple and independent websites in your network.

Take away the need for your users to re-enter theirs authentication credentials when they switch from one of your websites to another.

Single Sign-On can be implemented for users that login with Social Login as well as for legacy users that sign in with a username/password combination. For this purpose majority of providers offer a **durable and highly available cloud-hosted database** that allows you to store your user data and to access it from any website or server in your ecosystem.

https://www.oneall.com/services/single-sign-on/

Firewalls



Firewall is a security gateway between clients and servers to control incoming and outgoing traffic

Source: https://wpdistrict.sitelock.com/wp-content/uploads/2016/06/waf-diagram.png

Security Groups

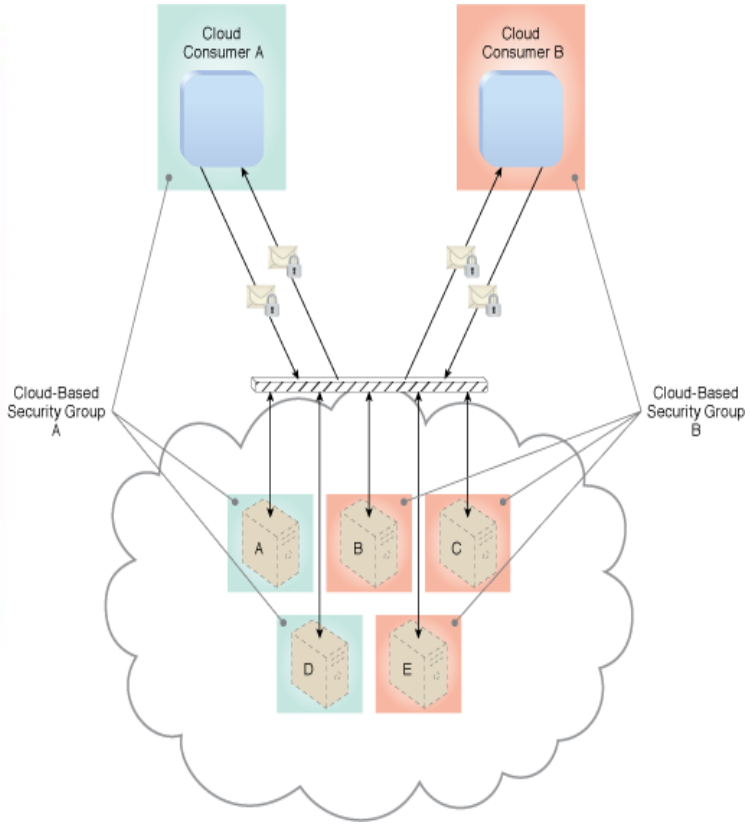
Cloud-Based Security Groups

The cloud-based resource segmentation process creates cloud-based security group mechanisms that are determined through security policies.

Networks are segmented into logical cloud-based security groups that form logical network perimeters

Each cloud-based IT resource is assigned to at least one logical cloud-based security group.

Each logical cloud-based security group is assigned specific rules that govern the communication between the security groups

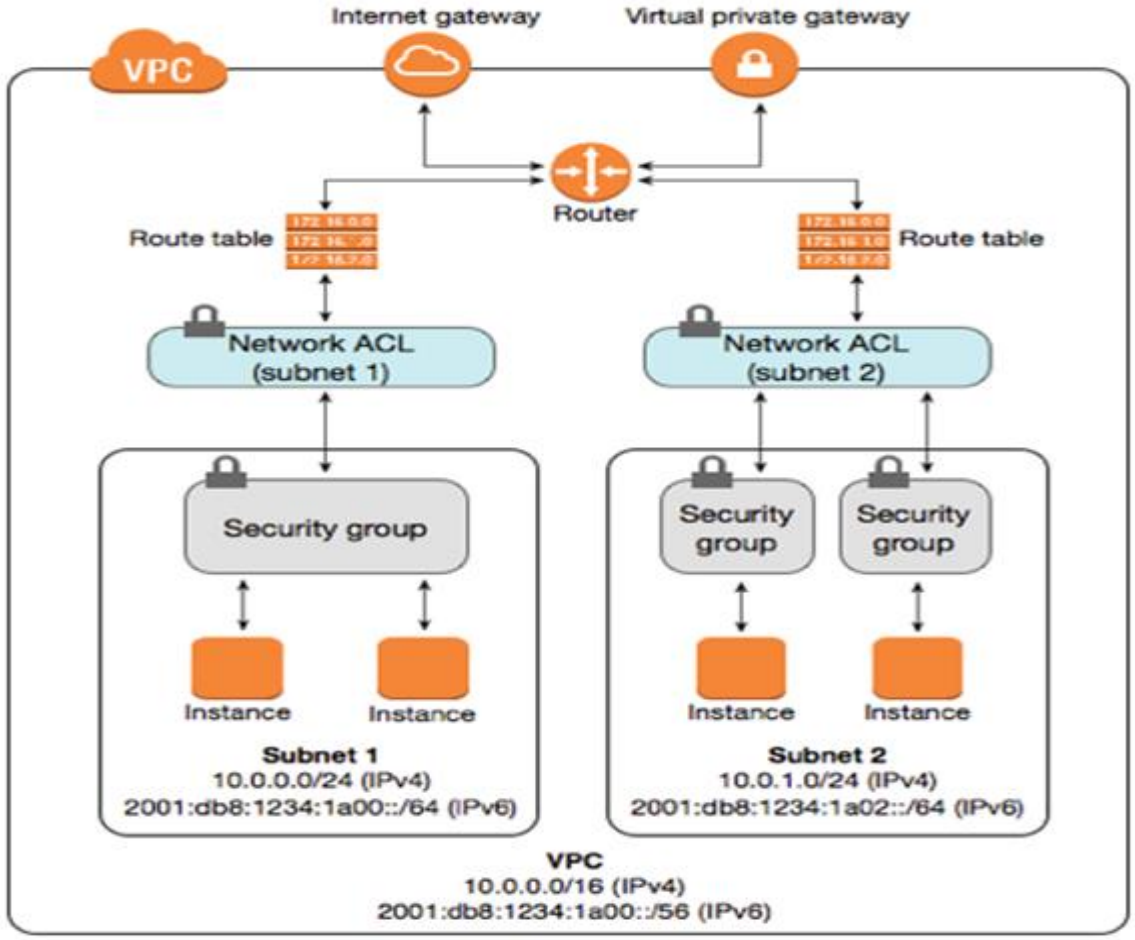


Multiple virtual servers running on the same physical server can become members of different logical cloud-based security groups (Figure)

http://cloudpatterns.org/mechanisms/cloud_based_security_groups

Security Groups

Application Security Groups (ASG)s.



http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Security.html

Quiz

Scenario # 1: A health insurance company has three portals: 1) Member Portal, 2) Provider Portal and 3) Broker Portal. They want to host all three portals on the public cloud. Company is concerned about security implications that might affect their users and patient's confidential data.

Please provide a solution to the company through which they can guarantee security and privacy of their data while keeping it in public cloud domain. Some extra requirements are:

a. Company needs to have single user authentication page but want users to be authenticated automatically on different portals

b. Each portal needs to have information transferred between other portals in terms of service calls

c. Users will be loading confidential data through HTTP on their browser. Please suggest techniques to stop eavesdropping

Reading Material

Chapter 10: Cloud Computing: Concepts, Technology & Architecture
by Zaigham Mahmood, Thomas Erl, Ricardo Puttini

URL: https://www.safaribooksonline.com/library/view/cloud-computing-concepts/9780133387568/ch10.html

OPTIONAL READING:
Cloud Computing Tutorial

URL: https://www.tutorialspoint.com/cloud_computing/cloud_computing_tutorial.pdf


ANY
QUESTIONS
?