Unit - 2

- **Basic cryptographic concepts** : cryptographic ciphers, cryptographic modes of operation,
- summarize cryptographic use cases and weaknesses, cryptographic technologies, digital certificates
- and certificate authorities, PKI management
- **Authentication controls** : authentication design concepts, knowledge-based authentication,
- authentication technologies, biometrics authentication concepts
- **Identity and account management controls** : identity and account types, account policies,
- authorization solutions, importance of personnel policies

Basic cryptographic concepts : cryptographic ciphers, cryptographic modes of operation

- Cryptography is the **science of using mathematics to encrypt (encipher) and decrypt (decipher) information**.
- Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network (like the Internet) so that it cannot be read by anyone except the intended recipient.

- Encryption is the process in which data is converted into something that seems to be random and meaningless.

- Decryption is the process in which the encoded information is converted back to its original form.

- The practice of breaking cryptographic systems is known as cryptanalysis.

Cryptographic Modes of Operation

- The use of a cipher to accomplish a security objective, such as confidentiality or integrity, is known as a mode of operation.

- modes of operation helps to implement and support security controls such as digital signatures and transport encryption.

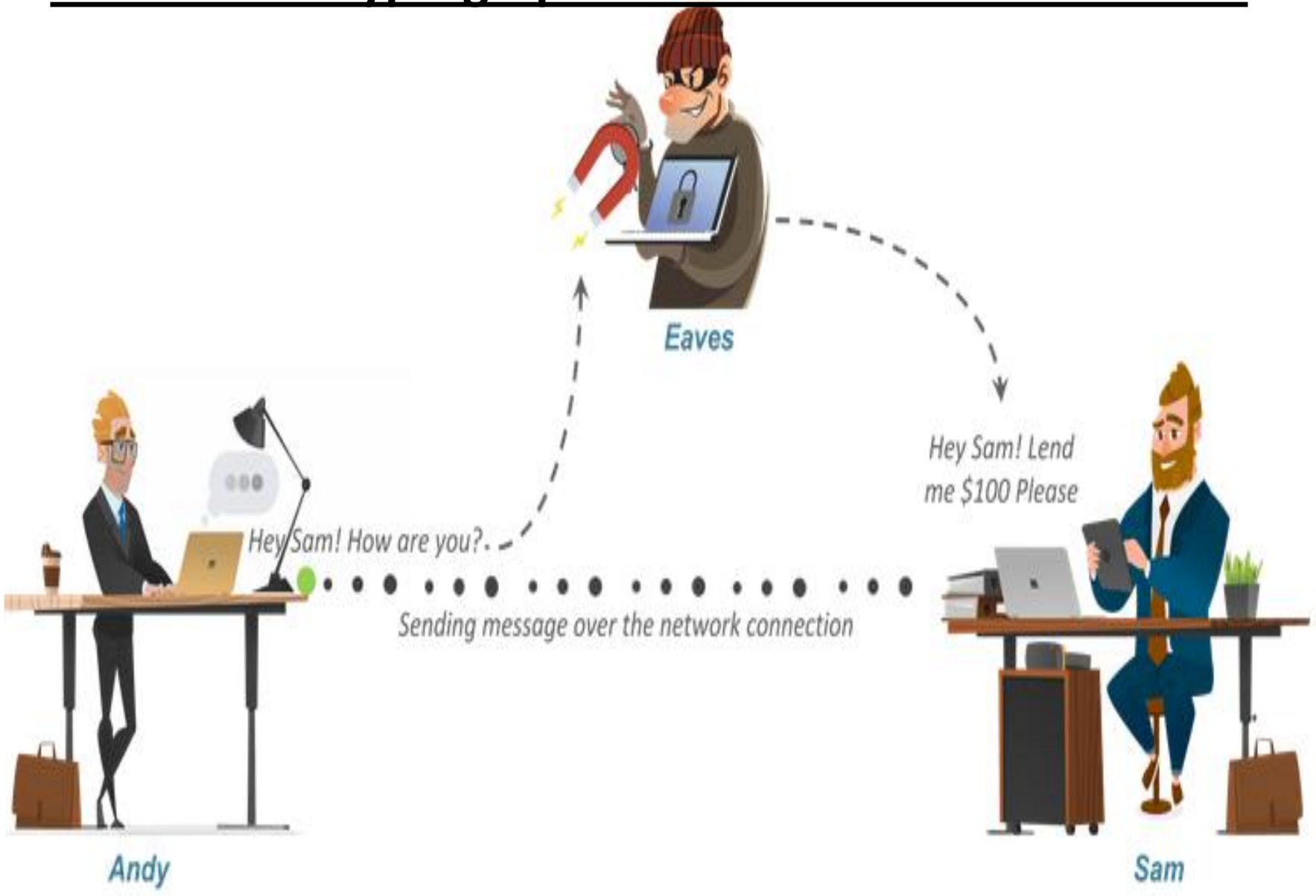
cryptographic technologies

- **Homomorphic encryption** is principally used to share privacy-sensitive data sets.
- When a company collects private data, it is responsible for keeping the data secure and
- respecting the privacy rights of individual data subjects. Companies often want to use
- third parties to perform analysis, however. Sharing unencrypted data in this scenario
- is a significant risk. Homomorphic encryption is a solution for this use case because
- it allows the receiving company to perform statistical calculations on fields within the
- data while keeping the data set as a whole encrypted.

- **Blockchain** is a concept in which an expanding list of transactional records is secured
- using cryptography. Each record is referred to as a *block* and is run through a hash
- function. The hash value of the previous block in the chain is added to the hash
- calculation of the next block in the chain. This ensures that each successive block is
- cryptographically linked. Each block validates the hash of the previous block, all the way
- through to the beginning of the chain, ensuring that each historical transaction has not
- been tampered with

- **Steganography** (literally meaning "hidden writing") is a technique for obscuring the
- presence of a message. Typically, information is embedded where you would not
- expect to find it; a message hidden in a picture, for instance. The container document
- or file is called the *covertext.* A *steganography tool* is software that either facilitates this or conversely that can be used to detect the presence of a hidden message within
- a covertext.

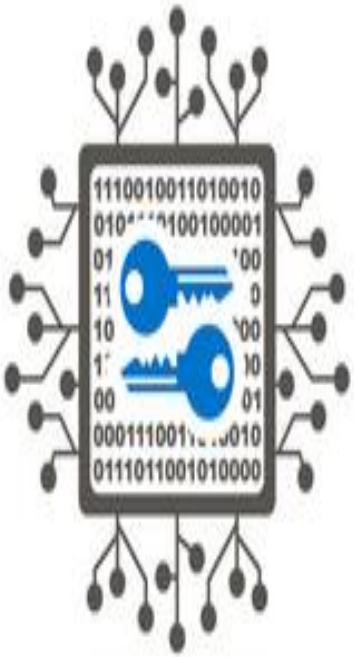
summarize cryptographic use cases and weaknesses



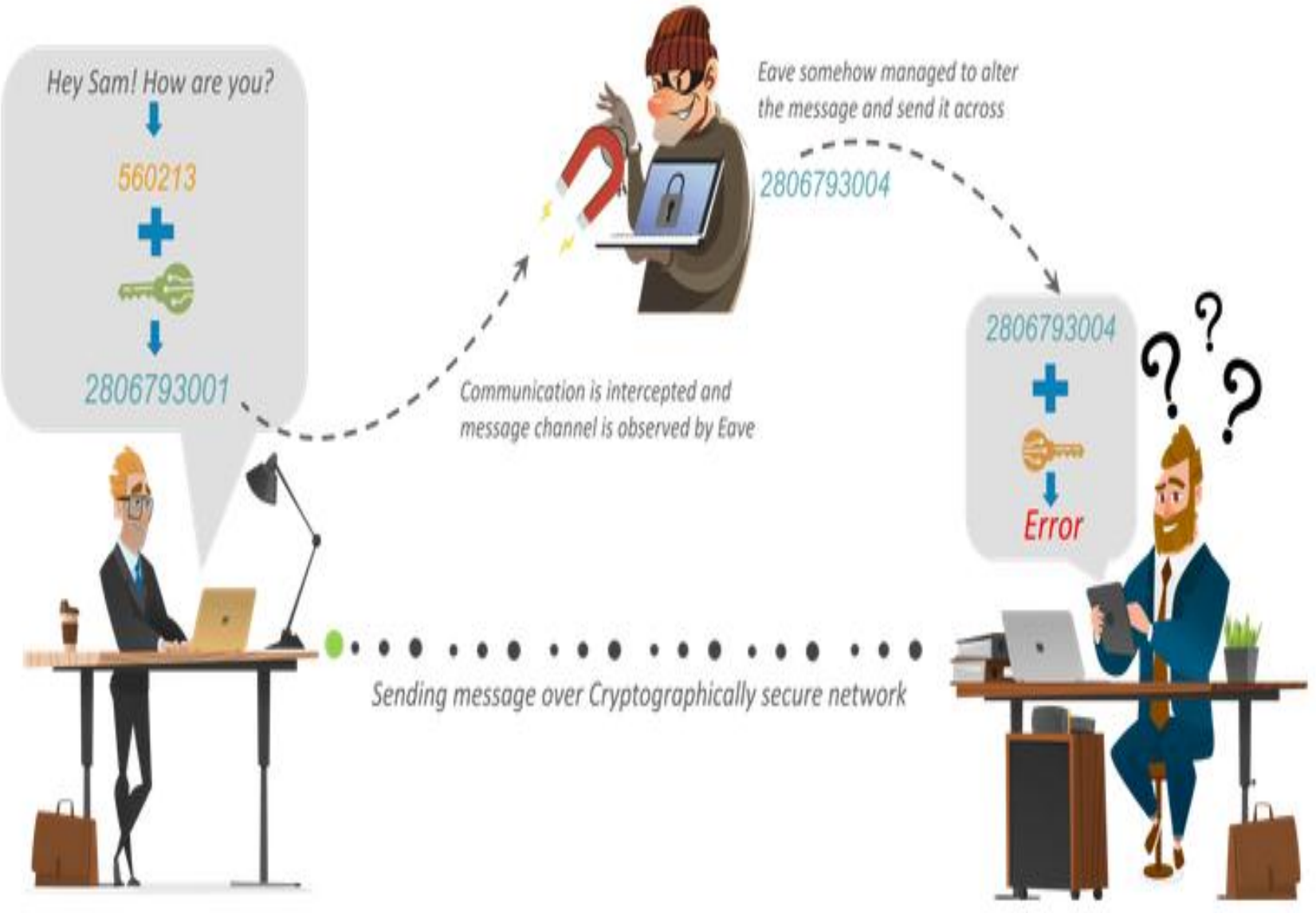
- So how can *Andy* be sure that nobody in the middle could access the message sent to *Sam*?

- That's where ***Encryption or Cryptography*** comes in.


Encryption
Decryption
Plaintext
Ciphertext
Plaintext

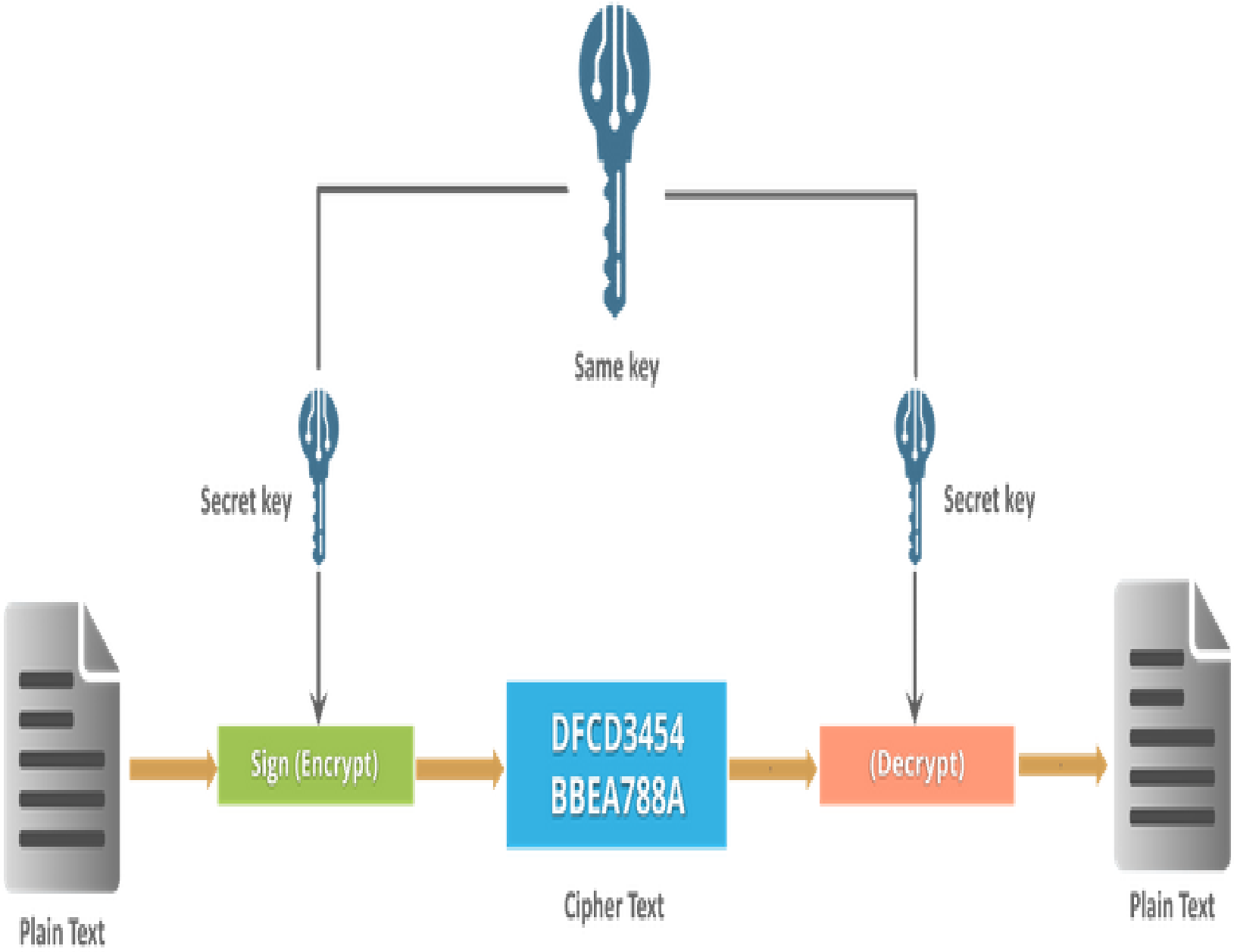


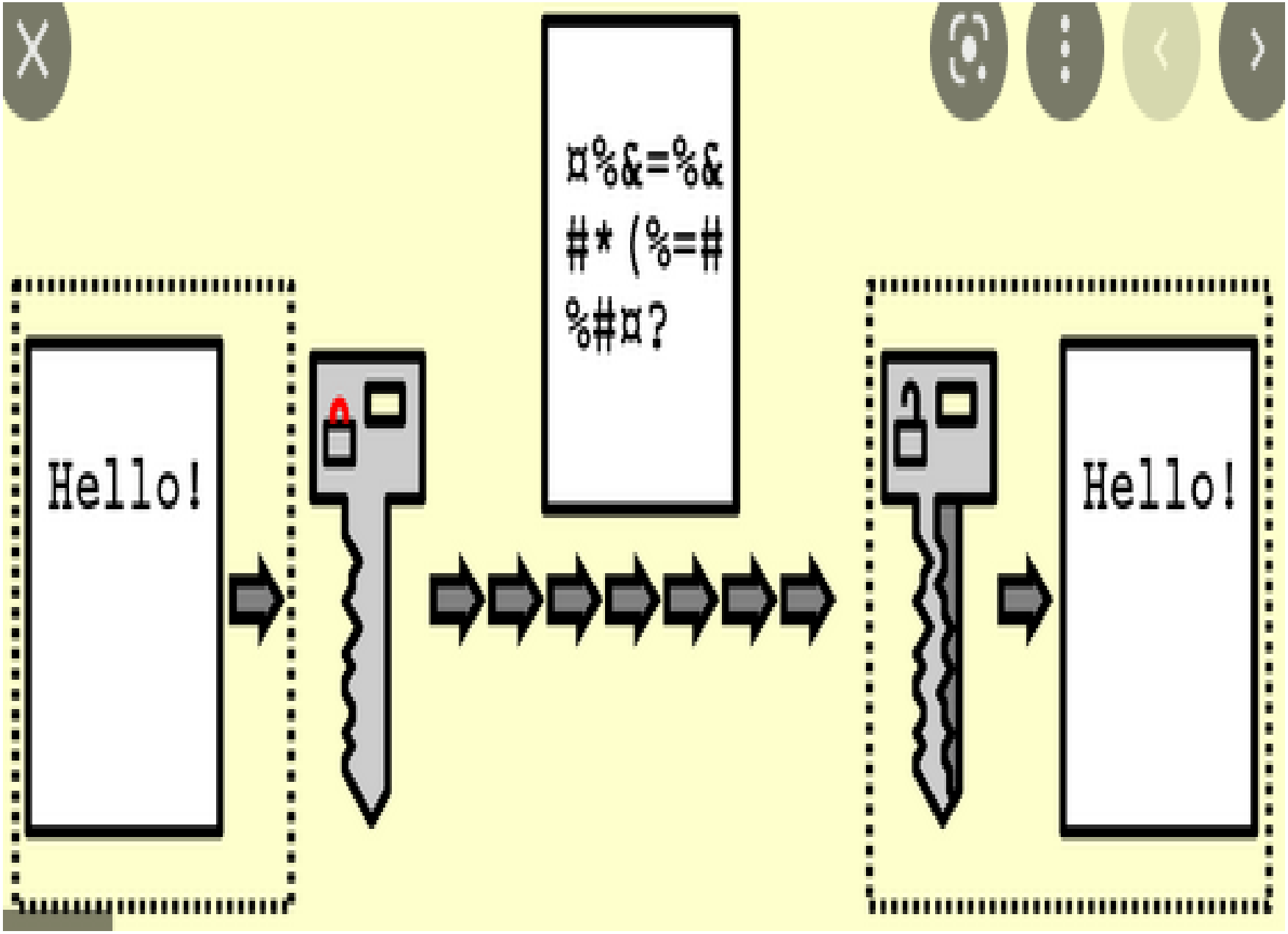

1034259
1034259
E
110340082
110340082
D
1034259 Or Error
Message

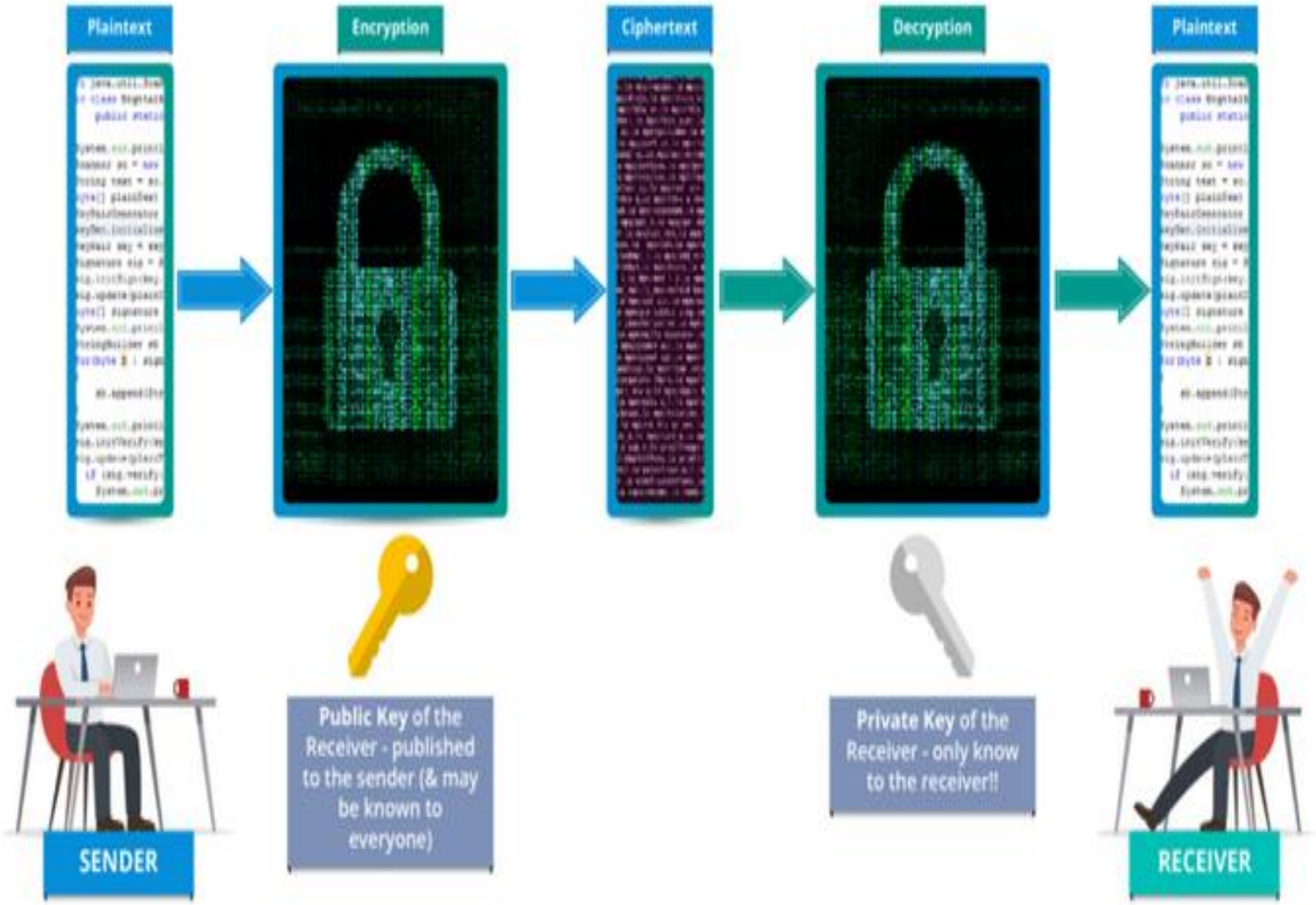


It is the way *Sam* knows that message sent by *Andy* is **not the same** as the message that he received. Thus, we can say that **encryption is important to communicate or share information** over the network.

- Now, based on the type of keys and encryption algorithms, cryptography is classified under the following categories:
- **Encryption Algorithms**
- Cryptography is broadly classified into two categories: ***Symmetric key Cryptography*** and ***Asymmetric key Cryptography*** (popularly known as public key cryptography).


Same key
Secret key
Secret key
Plain Text
Sign (Encrypt)
DFCD3454
BBEA788A
(Decrypt)
Cipher Text
Plain Text


¤%&=%&
#*(%=#
%#¤?
Hello!
Hello!


Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Public Key of the Receiver - published to the sender (& may be known to everyone)
Private Key of the Receiver - only know to the receiver!!
SENDER
RECEIVER

- **Hybrid encryption –** It is a process of encryption that blends **both** symmetric and asymmetric encryption. It takes advantage of the strengths of the two encryptions and minimizes their weakness.

- digital certificates and certificate authorities, PKI management

Public Key Infrastructure

- PKI is a system of processes, policies, authentication, and technologies that govern encryption and is ultimately what protects our text messages, emails, passwords, credit card information, etc.

- The most **popular use** of PKI is in providing *secure, encrypted communication* between web browsers (clients) and web servers (websites).

- This is done by employing the HTTPS protocol, which is implemented by installing an SSL certificate on the web server.

The “Key” Problem in Conventional Encryption

- Let’s say Alice who wants to send a confidential piece of information to Bob, her senior officer. She can’t send this information in plaintext as enemies(unauthorized access) could easily intercept and read/tamper with it. That’s why she must send this information in an unreadable form that Bob will be able to derive, but their enemies won’t. In other words, Alice will need to encrypt the information.

- But here comes a **problem**. If Alice locks (encrypts) the message using a key (some logic), ***then how will Bob decrypt it?***
- He(Bob) must have the key with him, right?
- To give the key to Bob, there's no option other than meeting with him face-to-face, which is totally impractical (to say the least) or to send it via courier and risk it being intercepted.

- Such an encryption method is problematic not only in the physical world but also in the virtual world. Every time two computers want to communicate securely, they'd have to agree on a single encryption key every single interaction. This is a mathematical process and takes time.

- And if there's a server (for example, a bank) that communicates with multiple users, then the server will have to perform a computational process for each client transaction, and that would slow it down even further. All of these things involve a variety of complex processes and agreements that must be handled at micro speed.

How PKI Changes Everything

- In addition to conventional encryption (also known as symmetric encryption) in which the same key is used for encryption and decryption, **PKI also involves the use of a *key pair*** — *a public key and a private key* — in a process that's known intuitively known as *public key encryption*. One of these keys encrypts information and the other decrypts it.

- Both these keys are **distinct**, but they're mathematically related to each other. It means that the information encrypted with one key can be decrypted only using the key associated with it.
- *The public key, as the name implies, is available publicly.*
- *The private key, on the other hand, is kept private.*

- So, if Alice and Bob are using public key infrastructure instead of the symmetric encryption method, *Alice could encrypt the secret message using Bob's public key that she has.* Bob, with his private key, is then the only person who can decrypt the message.

- This way, they could communicate securely without letting their enemies read/tamper with it. Not only that, but Bob can be sure of that the message came from Alice and not from someone else.

- PKI (**Public Key Infrastructure**), is a framework that enables the encryption of public keys and includes their affiliated crypto-mechanisms.
- The underlying purpose of any PKI setup is to manage the keys and certificates associated with it, thereby creating a highly secure network environment for use by applications and hardware.

- PKI is responsible for making online interactions more secure, and it does this by:
- *Establishing the identity of endpoints on a network*
- *Encrypting the flow of data via the network's communication channels*
- It does this by using private keys and public keys for encryption and decryption respectively, which are facilitated in turn by digital certificates.

- **Where is PKI applied?**
- Secure Browsing (via SSL/TLS)
- Securing Email (signing and encrypting messages)
- Secure Code-signing
- Network Security
- File Security (via Encrypted File Systems)
- …and so on.

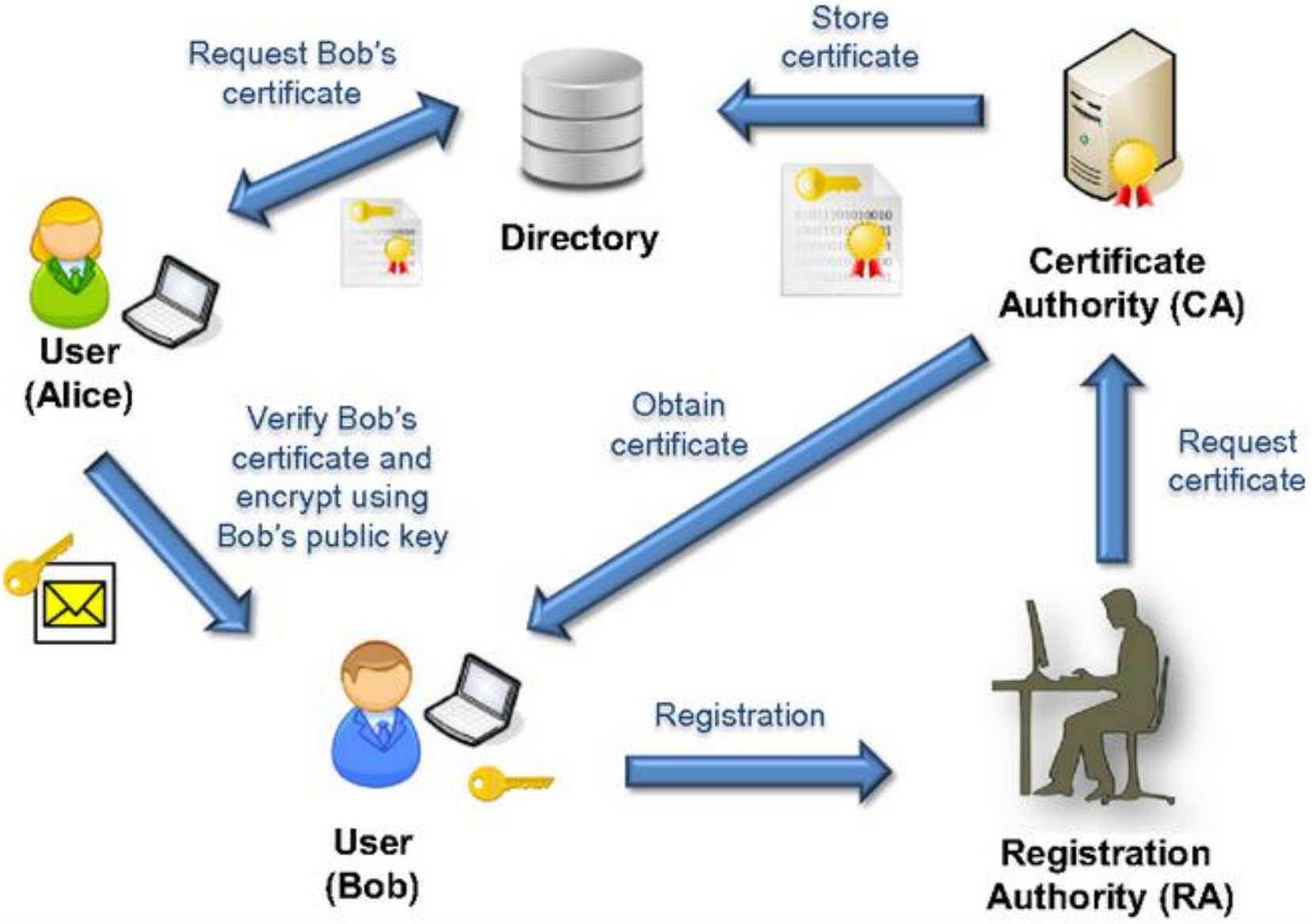
- **The Components of an Ideal PKI**
- PKI infrastructures involve the participation of some or all of the below entities:
- **Public and Private Keys:** The single most important component(s) of PKI, *public and private keys* are used to encrypt and decrypt the information transmitted over the web, ensuring that the sending and receiving party are the only ones privy to that information. Public key information is available openly online, but can only be effectively leveraged when the receiving party has an approved private key in order to decrypt a message.

- **Public Key Certificates:** Electronically signed documents that **verify ownership** of a public key. They are as important as keys, as they act as proof that a key-holder is legitimate. They are issued by Certificate Authorities(CA).

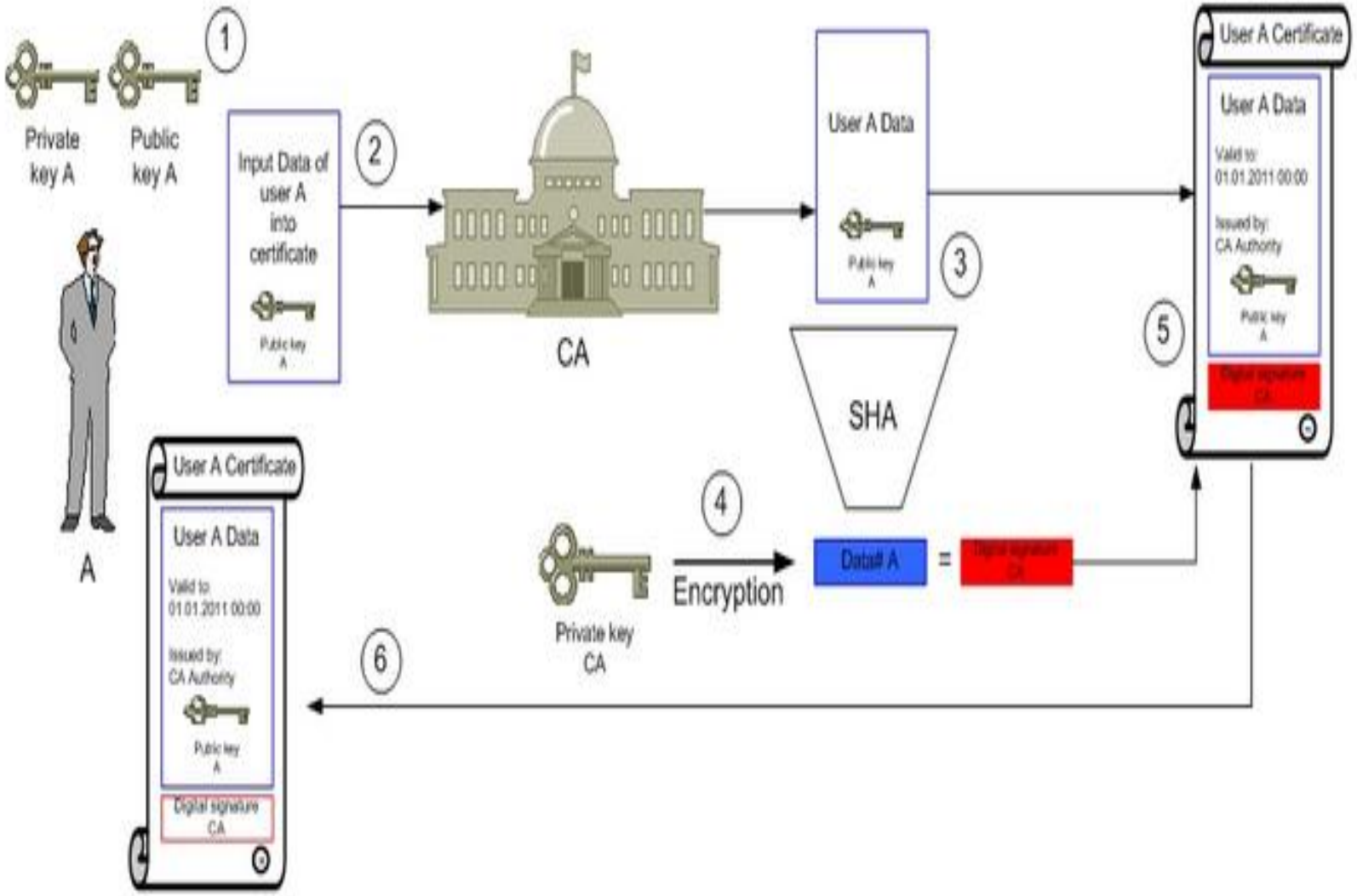
- **Certificate Repository:** An electronic, searchable **storage facility** for signed certificates with public keys that have been generated.
- It consists of important certificate information, such as *certificate validity details, revocation lists, and root certificates.* They are often equipped with LDAP (Lightweight Directory Access Protocol), an online directory service where entries are classified and indexed.

- **Certificate Authority (CA):** A trusted body which enables organizations to get themselves **verified as public key holders**. It does this by verifying a requesting organization, and generating an electronic document called a ***digital certificate*** which also holds the public key. It then signs the certificate with its own private key, which acts as a seal of approval that it is trusted by a Certificate Authority.

- **Registration Authority (RA):** Assists the PKI cycle by **verifying** that the body requesting a certificate is legitimate. Once the verification is complete, it carries out the request by allowing the request to reach the CA, who uses a certificate server to execute it.


Request Bob's certificate
Store certificate
Directory
Certificate Authority (CA)
User (Alice)
Verify Bob's certificate and encrypt using Bob's public key
Obtain certificate
Request certificate
Registration
User (Bob)
Registration Authority (RA)

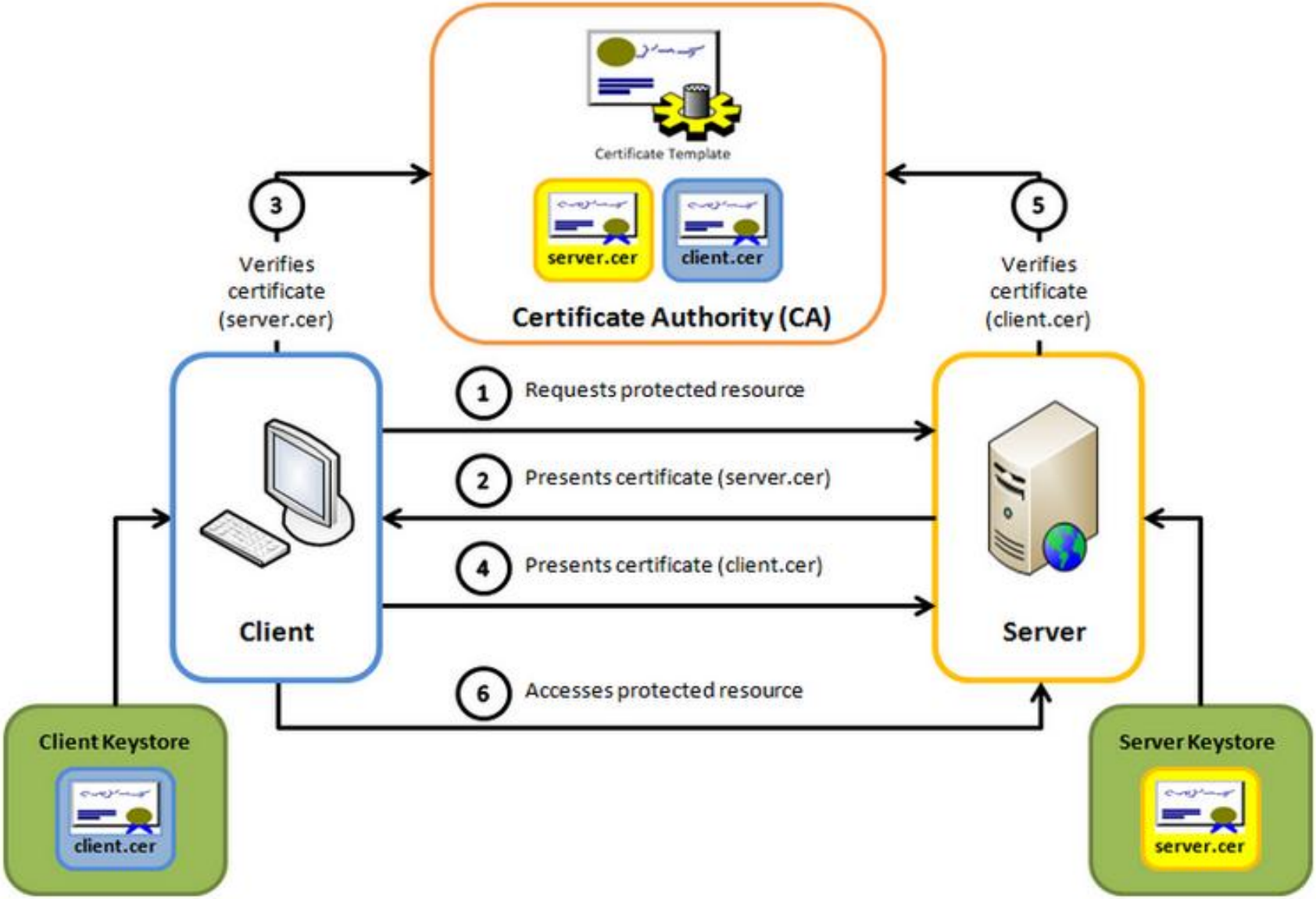
Certificate enrollment process



Certificate enrollment process

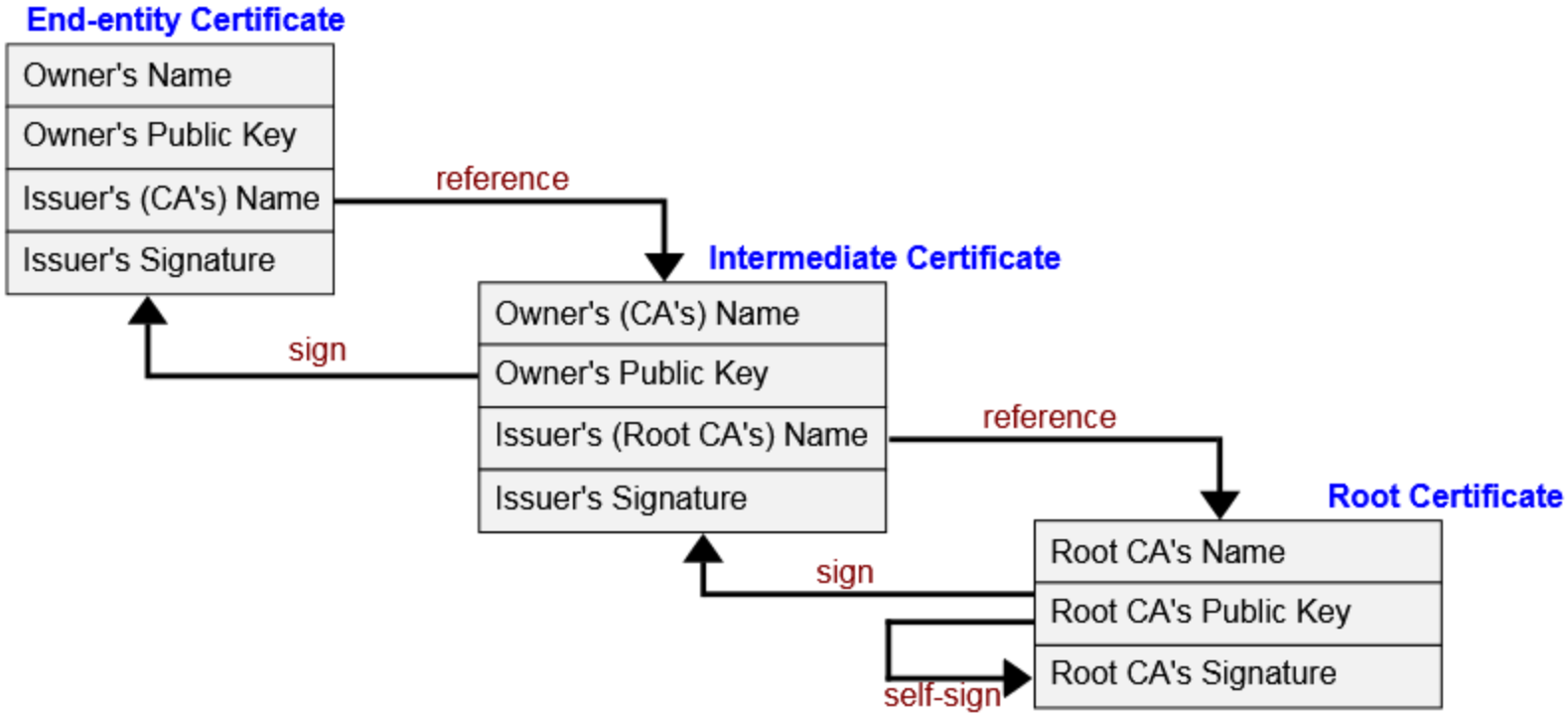
- 1. User A generates pair of keys: public key A and private key A.
  2. User A sends to the CA, own public key A with additional details that will identify user A like name, surname, department city, country, e-mail address etc.
  3. CA verifies user A data, next takes user A data and public key A as input and do SHA (or MD5) hash function – **Data# A** is output of this algorithm.

- 4. CA then uses own Private key CA and encrypts Data# A, **Digital signature of the CA** is output of this process.
  *5. User A Data, Public key of A, Digital signature of the CA, and specific details assigned by the CA like certificate serial number, issued and valid date, point of CRL distribution (and many more) creates **User A Certificates**.*
  6. Users A can get certificate and start use it to encrypt and authenticate data.


Certificate Template
server.cer
client.cer
Certificate Authority (CA)
3
Verifies certificate (server.cer)
5
Verifies certificate (client.cer)
1 Requests protected resource
2 Presents certificate (server.cer)
4 Presents certificate (client.cer)
6 Accesses protected resource
Client
Server
Client Keystore
client.cer
Server Keystore
server.cer

- Server or SSL Certificates perform a very similar role to Client Certificates, except the latter is used to identify the client/individual and the former authenticates the owner of the site.
- Server certificates typically are issued to hostnames, which could be a machine name (such as 'XYZ-SERVER-01') or domain name (such as 'www.DigiCert.com').
- A web browser reaching the server, and validates that an SSL server certificate is authentic.
- That tells the user that their interaction with the web site has no eavesdroppers and that the web site is exactly who it claims to be.
- This security is critical for electronic commerce, which is why certificates are now in such widespread use.

CERTIFICATES…



- The root certificate, also called a **trusted root**, is one of the certificates issued by a trusted Certificate Authority (CA) such as Sectigo or DigiCert.
- Nevertheless, it's a special type of **X.509 digital certificate** which is used for issuing other certificates called intermediates and further end-user SSL Certificate for avoiding the risk of getting compromised.

- Also, these end-user or leaf SSL certificates, which are installed on the website, have a validity period of two years and, the root certificates have much longer.
- For example, take a look at the validity period of DigiCert's EV root certificate.

- Issuing an **SSL/TLS Certificate** directly from the root certificate to end-users is very dangerous as well as impractical, as it could lead to managing issues and fraud.
- To overcome these issues, CAs offer *another layer of security* known as an **intermediate certificate**.
- Furthermore, these Intermediate certificates work as a "Chain of Trust" between the root certificate and an end-entity SSL/TLS certificate.


Hello, let's set up a secure SSL session
Hello, here is my certificate
Also checks that:
Certificate is valid
Signed by someone user trusts
1
2
Customer
Server
3
Here is a one time, encryption key for our session
(encrypted using Server's public key)
4
Server decrypts session key using its private key and establishes a secure session
01010010110
01010010110

How does HTTPS work: SSL explained

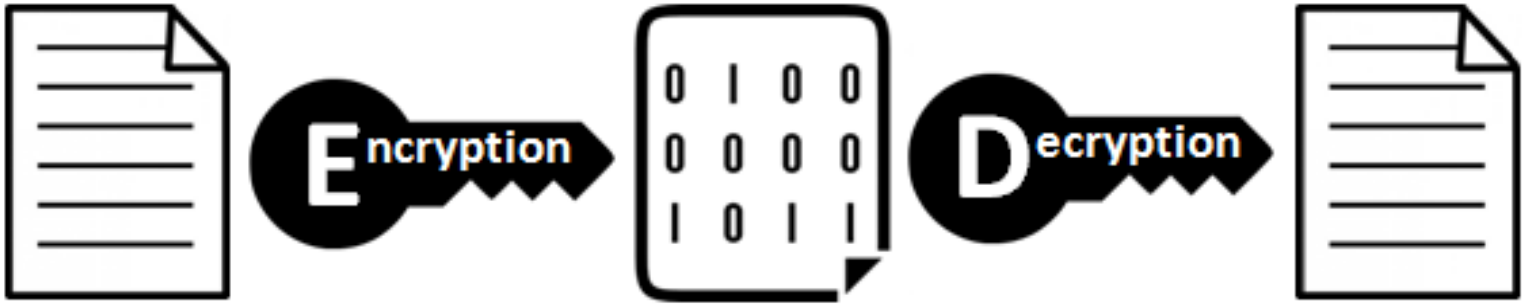
- Hashing

Hashing

- Hashing and encryption are the two most important and fundamental operations of a computer system.
- Both of these techniques change the *raw data into a **different format***.
- **Hashing on an input text provides a hash value, whereas encryption transforms the data into ciphertext**.

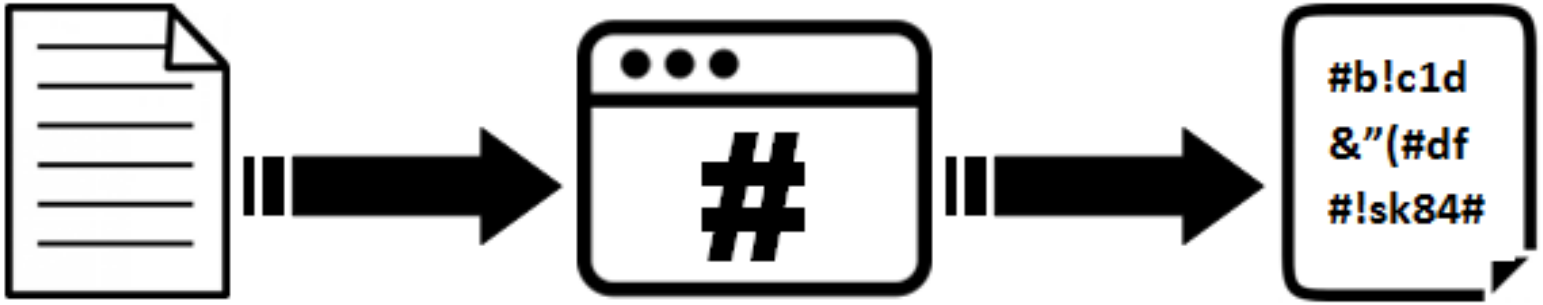
- Hash functions are mostly used for *integrity* (signatures and message digests) and password storage (*confidentiality*).

Encryption & Decryption



Plain Text | Encrypted Text | Plain Text

Hashing Algorithm



Plain Text | Hash Function | Hashed Text

- **Hashing and Encryption have different functions.**
- **Encryption includes encryption and decryption process while hashing is a one-way process that changes data into the message digest which is irreversible.**

- A hash can simply be defined as a number generated from a string of text.
- Other literature can also call it a message digest. In essence, a hash is smaller than the text that produces it.

- It can be seen that hashing is the process of producing hash values for the purpose of accessing data and for security reasons in communication systems.
- In principle, hashing will take arbitrary input and produce a string with a fixed length.

- A hash algorithm is a function that can be used to **map out** data of random size to data of fixed size.
- Hash values, hash codes and hash sums are returned by functions during hashing.
- There are different types of hashing algorithms used in computing, but some have been discarded over time.

- **In addition to assessing password values, After a file transfer, its integrity can be checked using its hash.**
- **1.** For her product, Alice runs a hash function on the setup.exe file. She uploads the digest along with a download link of file on her website.
- **2.** Bob copies the digest after downloading the setup.exe file.
- **3.** Bob applies the same hashing algorithm on the downloaded setup.exe file and contrasts the result with the Alice-published reference value. The integrity of the file can be presumed if it matches the value displayed on the website.
- **4.** Consider the possibility that Mallory could replace the download file with a malicious one. Mallory is unable to alter the reference hash, however.
- **5.** Bob computes a hash this time, but it does not match., causing him to believe the file has been **altered**.

- **MD4 –** It is a hash function created by Ronald Rivest in 1990. It has a length of 128 bits and has influenced many posterior designs like WMD5, WRIPEMD and WSHA family. The security of this algorithm has however been criticized even by the creator himself.

- **SHA algorithm** – Secure Hash Algorithm was designed by the National Security Agency to be used in their digital signature algorithm. It has a length of 160 bits. Just like the latter, security weaknesses in it means that it is no longer used SHA and SHA-1, organizations are using strong SHA-2 (256 bit) algorithm for the cryptographic purpose.

- **RIPMEND** – It is a cryptographic hash algorithm designed by Hans Dobbertin. It has a length of 160 bits. It was developed in the framework of the EU project RIPE.

- **WHIRLPOOL algorithm** – It is algorithm design by Vincent Rijmen and Paul Barreto. It has a length of 2^{256} bits and produces the 512-bit message digest.

- **TIGER algorithm –** It is a new and fast algorithm. It used by modern computers. It hashes more than 132M bits per second. It has thus far proved to be more efficient than all the hashing algorithms discussed. It has no restrictions on its usage that means it has no patents.

Purpose of hashing

- Hashing can be used to compare a large amount of data. Hash values can be created for different data, meaning that it is **easier** comparing hashes than the data itself.
- It is easy to **find** a record when the data is hashed.
- Hashing algorithms are used in cryptographic applications like a **digital signature**.

- Hashing is used to generate **random strings** to avoid duplication of data stored in databases.
- Geometric hashing – widely used in **computer graphics** to find closet pairs and proximity problems in planes. It is also called grid method and it has also been adopted in telecommunications.
- *These characteristics mean that hash can be used to store passwords. This way, it becomes difficult for someone who has the raw data to reverse them.*

- **Authentication controls** : authentication design concepts, knowledge-based authentication, authentication technologies, biometrics authentication concepts

- Each **network user and host device** must be identified with an account so that you can control their access to your organization's applications, data, and services.
- The processes that support this requirement are referred to as **identity and access management (IAM)**.
- Within IAM, authentication technologies ensure that only valid subjects (users or devices) can operate an account.

- Authentication requires the account holder to submit credentials that should only be known or held by them in order to **access** the account.
- There are many authentication technologies and it is authoritative that you be able to **compare and contrast** and to implement these security controls.

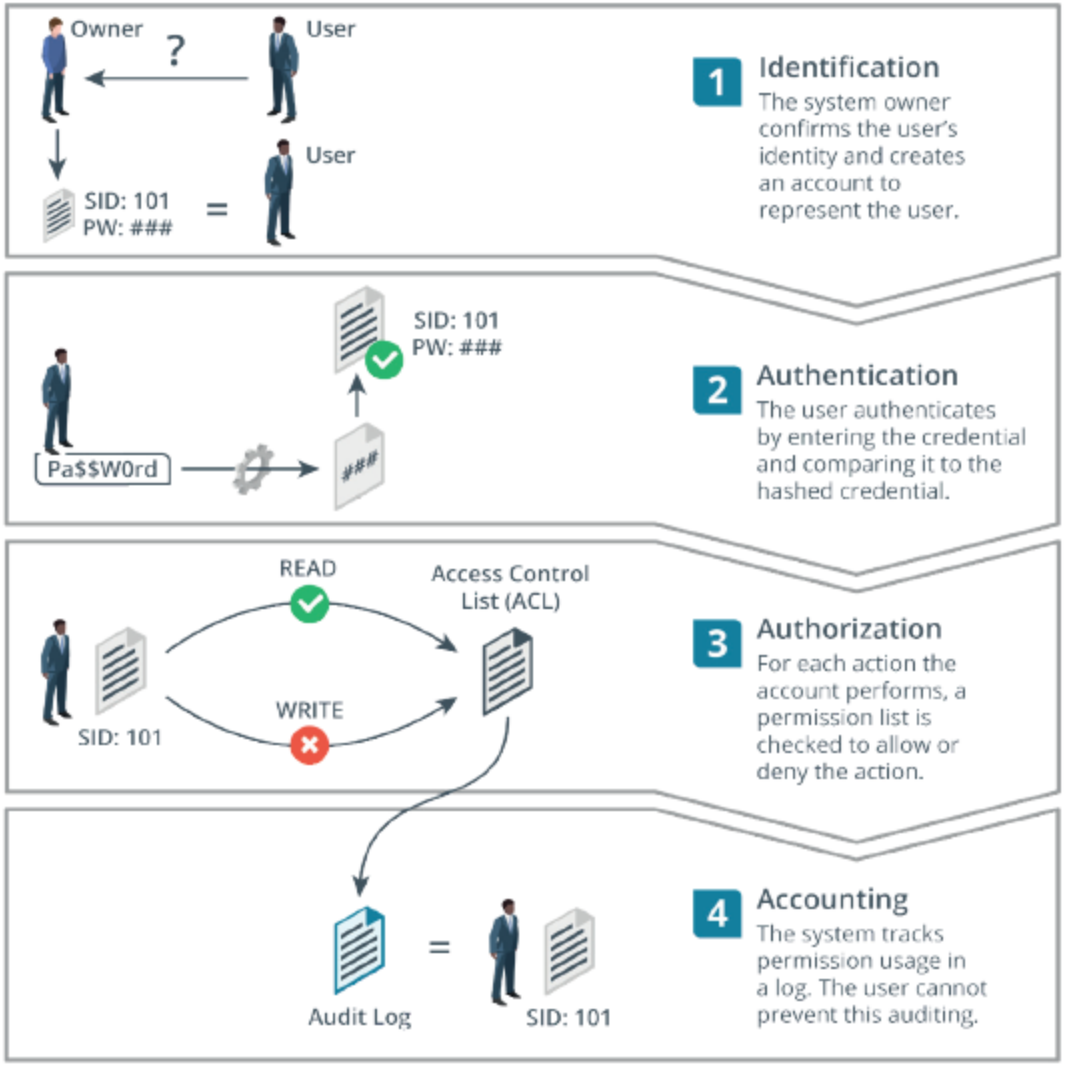
- **Strong authentication** is the first line of defense in the battle to secure network resources.
- But authentication is not a single process; there are many different methods and mechanisms, some of which can be **combined to form** more effective products.

Identity and Access Management

- An access control system is the set of technical controls that govern how subjects may interact with objects.
- **Subjects** in this sense are users, devices, or software processes, or anything else that can request and be granted access to a resource.
- **Objects** are the resources; these could be networks, servers, databases, files, and so on.

An **identity and access management (IAM)** system is usually described in terms of **four** main processes:

- **Identification**—creating an account or ID that uniquely represents the user, device, or process on the network.
- • **Authentication**—proving that a subject is who or what it claims to be when it attempts to access the resource.
- • **Authorization**—determining what rights subjects should have on each resource, and enforcing those rights.
- • **Accounting**—tracking authorized usage of a resource or use of rights by a subject and alerting when unauthorized use is detected or attempted.



Differences among identification, authentication, authorization, and accounting. (Images © 123RF.com.)

- IAM enables you to define the attributes that make up an **entity's identity**, such as its purpose, function, security clearance, and more.
- These attributes subsequently enable access management systems to make informed decisions about whether to **grant or deny** an entity access, and if granted, decide what the entity has authorization to do.

- ***For example***, an individual employee may have his or her own identity in the IAM system.
- The **employee's role** in the company factors into his or her identity, such as what department the employee is in and whether the employee is a manager.

- ***For example***, if you are setting up an e-commerce site and want to enroll users, you need to select the appropriate controls to perform each function:

- **Identification**—ensure that customers are legitimate. For example, you might need to ensure that billing and delivery addresses match and that they are not trying to use fraudulent payment methods.
- • **Authentication**—ensure that customers have unique accounts and that only they can manage their orders and billing information.
- • **Authorization**—rules to ensure customers can place orders only when they have valid payment mechanisms in place. You might operate loyalty schemes or promotions that authorize certain customers to view unique offers or content.
- • **Accounting**—the system must record the actions a customer takes (to ensure that they cannot deny placing an order, for instance).

Authentication Factors

- Something you know **Authentication**
  - The typical knowledge factor is the *logon,* composed of a username and a password.
  - Personal identification number (PIN)
  - Swipe pattern
  - Challenge questions/password reset

Screenshot used with permission from Microsoft.

- **Something You Have Authentication**
- An *ownership factor* means that the account holder possesses something that no one else does, such as a smart card, fob, or wristband programmed with a unique identity certificate or account number.
- Alternatively, they might have a USB fob that generates a unique code.
- These ownership factors can be described as hard tokens.
- A device such as a smartphone can also be used to receive a uniquely generated access code as a soft token.
- Unlike a password, these tokens are valid for only one use, typically within a brief time window.

- **Something You Are/Do Authentication**
- A *biometric factor* uses either physiological identifiers, such as a fingerprint, or behavioral identifiers, such as the way someone moves (gait).
- The identifiers are scanned and recorded as a template.
- When the user authenticates, another scan is taken and compared to the template.

Authentication Design

- *Authentication design* refers to selecting a technology that meets requirements for confidentiality, integrity, and availability:
- • *Confidentiality,* in terms of authentication, is critical, because if account credentials are leaked, threat actors can impersonate the account holder and act on the system with whatever rights they have.
- • *Integrity* means that the authentication mechanism is reliable and not easy for threat actors to bypass or trick with counterfeit credentials.
- • *Availability* means that the time taken to authenticate does not impede workflows and is easy enough for users to operate.

- **Multifactor Authentication**
- An authentication technology is **considered strong** if it combines the use of more than one type of knowledge, ownership, and biometric factor, and is called **multifactor authentication (MFA)**.

- Single-factor authentication can quite easily be **compromised**: a password could be written down or shared, a smart card could be lost or stolen, and a biometric system could be subject to high error rates or spoofing.

- *Two-Factor Authentication (2FA)* **combines** either an ownership-based smart card or biometric identifier with something you know, such as a password or PIN.

- Three-factor authentication **combines all three technologies**, or incorporates an additional attribute, such as location; for example, a smart card with integrated fingerprint reader. This means that to authenticate, the user must possess the card, the user's fingerprint must match the template stored on the card, and the user must input a PIN or password.

Authentication Attributes

- Somewhere you are Authentication
  - Geolocation via location services (geographic location)
  - IP location (logical versus geolocation)
  - Within a premises network, Switch port, virtual LAN (VLAN), or wireless network name

Something you can do Authentication

- Performing an action in a way that can be captured as a unique pattern, it can be used for contextual and continual authentication to ensure that a device continues to be operated by the owner.

Something you exhibit Authentication

- A **behavior or personality trait** that can be captured as a unique pattern, the way you use smartphone apps or web search engines might conform to a pattern of behavior that can be captured by machine learning analysis as a statistical template.
- If someone else uses the device, their behavior will be different, and this anomalous pattern could be used to lock the device and require re-authentication.

Someone you know Authentication

- Web of trust

- A someone you know authentication scheme uses a web of trust model, where new users are vouched **(assure)** for by existing users. As the user participates in the network, their identity becomes better established.

Knowledge-based authentication

- *Knowledge-based authentication* refers **primarily** to issuing users with password-based account access mechanisms.
- Configuring password-based authentication protocols and supporting users with authentication issues is an **important part** of the information security role.
- In this topic, you will learn how some common authentication protocols work and about the ways that they can be put at risk by password cracking techniques.

Local, Network, and Remote Authentication

- One of the most important features of an operating system is the **authentication provider**, which is the software architecture and code that underpins the mechanism by which the user is authenticated before starting a shell.
- This is usually described as a login (Linux) or a logon or sign-in (Microsoft).

Windows Authentication

- The following three scenarios are typical:

- **Windows local sign-in**—the Local Security Authority (LSA) compares the submitted credential to a hash stored in the Security Accounts Manager (SAM) database

- **Windows network sign-in**—the LSA can pass the credentials for authentication to a network service. The preferred system for network authentication is based on Kerberos.

- **Remote sign-in**—if the user's device is not connected to the local network, authentication can take place over some type of virtual private network (VPN) or web portal.

- To access your administrator password, you'll need to access the Windows registry.
- Navigate to Windows **Command Prompt** again.
- Type in **regedit** and hit Enter.
- The **Registry Editor** window will appear.
- Go to **HKEY_ LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Windows NT** > **CurrentVersion** > **Winlogon**
- Now, scroll down to **DefaultPassword** and double-click it.
- A window will pop up, revealing the stored password.

Linux Authentication

- In Linux, local user account names are stored in /etc/passwd.
- When a user logs in to a local interactive shell, the password is checked against a hash stored in /etc/ shadow.
- Interactive login over a network is typically accomplished using Secure Shell (SSH).
- With SSH, the user can be authenticated using cryptographic keys instead of a password.

- A **pluggable authentication module (PAM)** is a package for enabling different authentication providers, such as smart-card login.

Single Sign-On (SSO)

- A **single sign-on (SSO)** system allows the user to authenticate once to a local device and be authenticated to compatible application servers without having to enter credentials again.

Kerberos Authentication

- Kerberos is a computer network **security protocol** that authenticates service requests between two or more trusted hosts across an untrusted network, like the internet.
- It uses secret-key cryptography and a trusted third party for authenticating client-server applications and verifying users' identities.

- Kerberos is used in Active Directory.

The protocol involves:

- **Client:** The person trying to connect to a service.
- **Server:** The server that hosts the service.
- **Authentication Server (AS):** Authenticates the client. If the client is authenticated, a TGT is generated that proves the client is authentic.
- **Ticket Granting Server (TGS):** An application server that issues service tickets.
- **Key Distribution Center (KDC):** A single server that hosts the Database, Authentication Server, and the TGS.

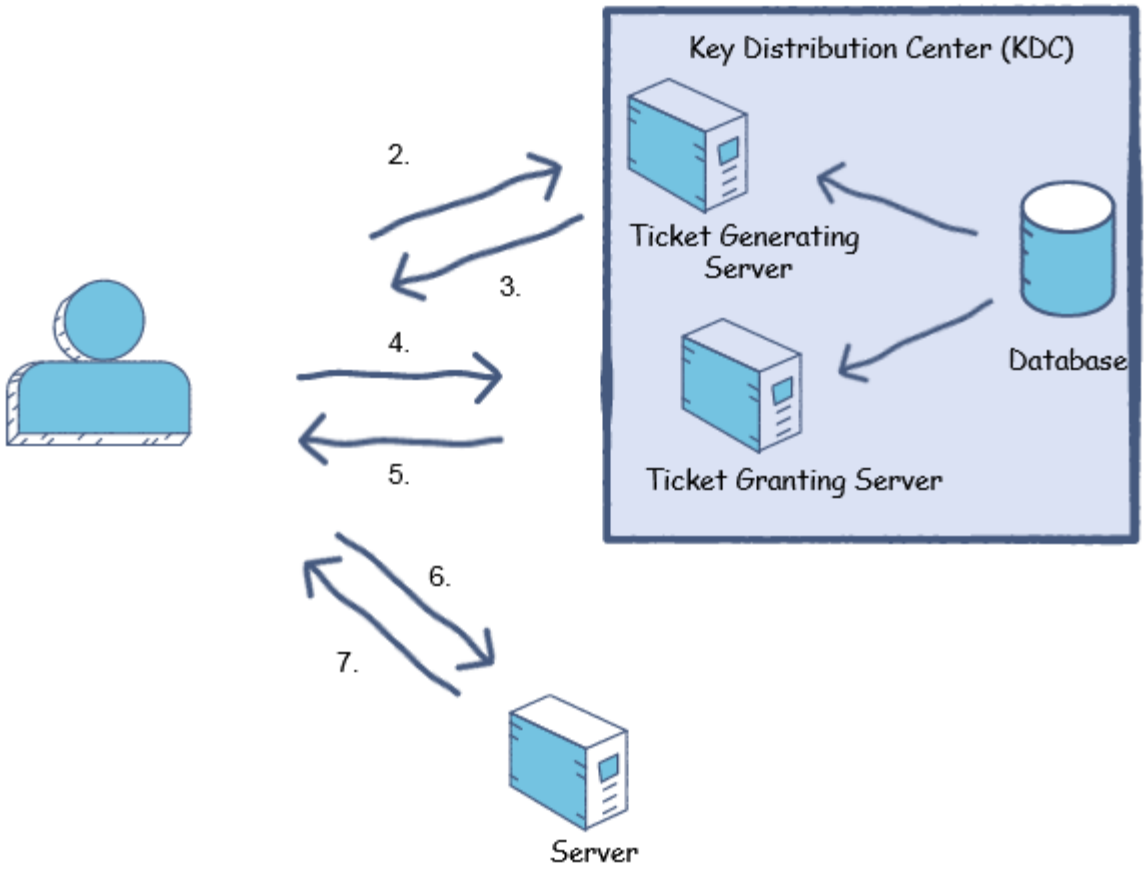
The Kerberos makes use of three types of keys:

- **Client/user secret key**
- **TGS secret key**
- **Server secret key**

Here are the steps that describe how a Kerberos protocol works:

1. The user enters the login credentials and the client secret key is generated.

2. The client asks the Authentication server for a TGT by sending the client ID.


Key Distribution Center (KDC)
Ticket Generating Server
Database
Ticket Granting Server
2.
3.
4.
5.
6.
7.
Server

3. The Authentication server checks for the availability of the client in the database. If found, the *client secret key* is generated using the user password from the database as well as a TGS secret key.

A session key (SK1) is generated and encrypted using the client secret key.

A TGT is generated containing client ID, client network address, lifetime, timestamp, and SK1. The SK1 and TGT are sent to the client.

The message, however, is encrypted using the client secret key.

- 4. The client decrypts the message using the client secret key, which is generated from the user entered password.
- An authenticator is generated that contains the client ID, client network address, and client machine timestamp, all of which is encrypted using SK1.
- The client sends the authenticator and TGT to the ticket-granting server.

5. The TGS decrypts the TGT using the TGS secret key and extracts the SK1.

The SK1 is used to decrypt the authenticator – it validates the expiration of TGT and checks if the information from TGT and the authenticator match.

Then, it creates a service session key(SK2).

A service ticket containing client ID, client network address, timestamp, and SK2 is generated.

This is encrypted with the server secret key that was obtained from the database. SK2 and service tickets are sent to the client after being encrypted with SK1.

- 6. The client decrypts the message using SK1 and extracts SK2.
- A new authenticator that contains client ID, client network address, and timestamp is generated.
- This authenticator is then encrypted with SK2.
- The authenticator and service ticket are sent to the target server.

7. The target server decrypts the service ticket with the secret key.

SK2 is extracted and used to decrypt the authenticator.

The same checks are applied, and the server sends a message that consists of a timestamp and is encrypted with SK2.

This step confirms that both the client and the server have been authenticated.

PAP, CHAP, and MS-CHAP Authentication

- Several authentication protocols have been developed to work with remote access protocols, where the connection is made over a serial link or virtual private network (VPN).

Password Authentication Protocol (PAP)

- The **Password Authentication Protocol (PAP)** is an unsophisticated authentication method developed as part of the Point-to-Point Protocol (PPP), used to transfer TCP/IP data over serial or dial-up connections. It is also used as the basic authentication mechanism in HTTP. It relies on clear text password exchange and is therefore obsolete for most purposes, except through an encrypted tunnel.

Challenge Handshake Authentication Protocol (CHAP)

- The **Challenge Handshake Authentication Protocol (CHAP)** was also developed as part of PPP as a means of authenticating users over a remote link. CHAP relies on an encrypted challenge in a system called a *three-way handshake.*

- 1. Challenge—the server challenges the client, sending a randomly generated challenge message.
- **2.** Response—the client responds with a hash calculated from the server challenge message and client password (or other shared secret).
- **3.** Verification—the server performs its own hash using the password hash stored for the client. If it matches the response, then access is granted otherwise, the connection is dropped.

- **MS-CHAPv2** is Microsoft's implementation of CHAP. Because of the way it uses vulnerable NTLM hashes, MS-CHAP should not be deployed without the protection of a secure connection tunnel so that the credentials being passed are encrypted.

Password Attacks

- **Plaintext/Unencrypted Attacks:**
- A *plaintext/unencrypted attack* exploits password storage or a network authentication protocol that does not use encryption.

- **Online Attacks:**
- An *online password attack* is where the threat actor interacts with the authentication service directly.

- **Password Spraying:**
- **Password spraying** is a horizontal brute-force online attack. This means that the attacker chooses one or more common passwords (for example, password or 123456) and tries them in conjunction with multiple usernames.

- **Offline Attacks:**
- An *offline attack* means that the attacker has managed to obtain a database of password hashes.

- **Brute-Force and Dictionary Attacks:**

- **Rainbow table** attacks refine the dictionary approach. The attacker uses a precomputed lookup table of all possible passwords and their matching hashes.

- **Hybrid Attack:**
- A **hybrid password attack** uses a combination of dictionary and brute-force attacks. It is principally targeted against naïve passwords with inadequate complexity, such as james1.

Password Crackers

- The process of recovering Secret Passwords stored in a computer system or transmitted over a network.

Authentication Management

- Users often adopt poor credential management practices that are very hard to control, such as using the same password for corporate networks and consumer websites. This makes enterprise network security vulnerable to data breaches from these websites.
- Password managers
  - Password key
  - Password vault

authentication technologies

- Authentication technologies can be used as a something you have or ownership/ possession factor.

- Many organizations are deploying multifactor authentication systems based on smart cards and USB key fobs.

Smart-Card Authentication

- **Smart-card authentication** means programming cryptographic information onto a card equipped with a secure processing chip.
- The chip stores the user's digital certificate, the private key associated with the certificate, and a personal identification number (PIN) used to activate the card.

For Kerberos authentication, smart-card logon works as follows:

- **1.** The user presents the smart card to a reader and is prompted to enter a PIN.
- **2.** Inputting the correct PIN authorizes the smart card's cryptoprocessor to use its private key to create a Ticket Granting Ticket (TGT) request, which is transmitted to the authentication server (AS).
- **3.** The AS is able to decrypt the request because it has a matching public key and trusts the user's certificate, either because it was issued by a local certification authority or by a third-party CA that is a trusted root CA.
- **4.** The AS responds with the TGT and Ticket Granting Service (TGS) session key.

Key Management Devices

- When using public key infrastructure (PKI) for smart-card authentication, the security of the private key issued to each user is critical.

- Various technologies can be used to avoid the need for an administrator to generate a private key and transmit it to the user:

- Smart card
- USB key
- Trusted Platform Module (TPM)
- Hardware security module (HSM)

Extensible Authentication Protocol/IEEE 802.1X

- The smart-card authentication process described earlier is used for Kerberos authentication where the computer is attached to the local network and the user is logging on to Windows. Authentication may also be required in other contexts:
- • When the user is accessing a wireless network and needs to authenticate with the network database.
- • When a device is connecting to a network via a switch and network policies require the user to be authenticated before the device is allowed to communicate.
- • When the user is connecting to the network over a public network via a virtual private network (VPN).

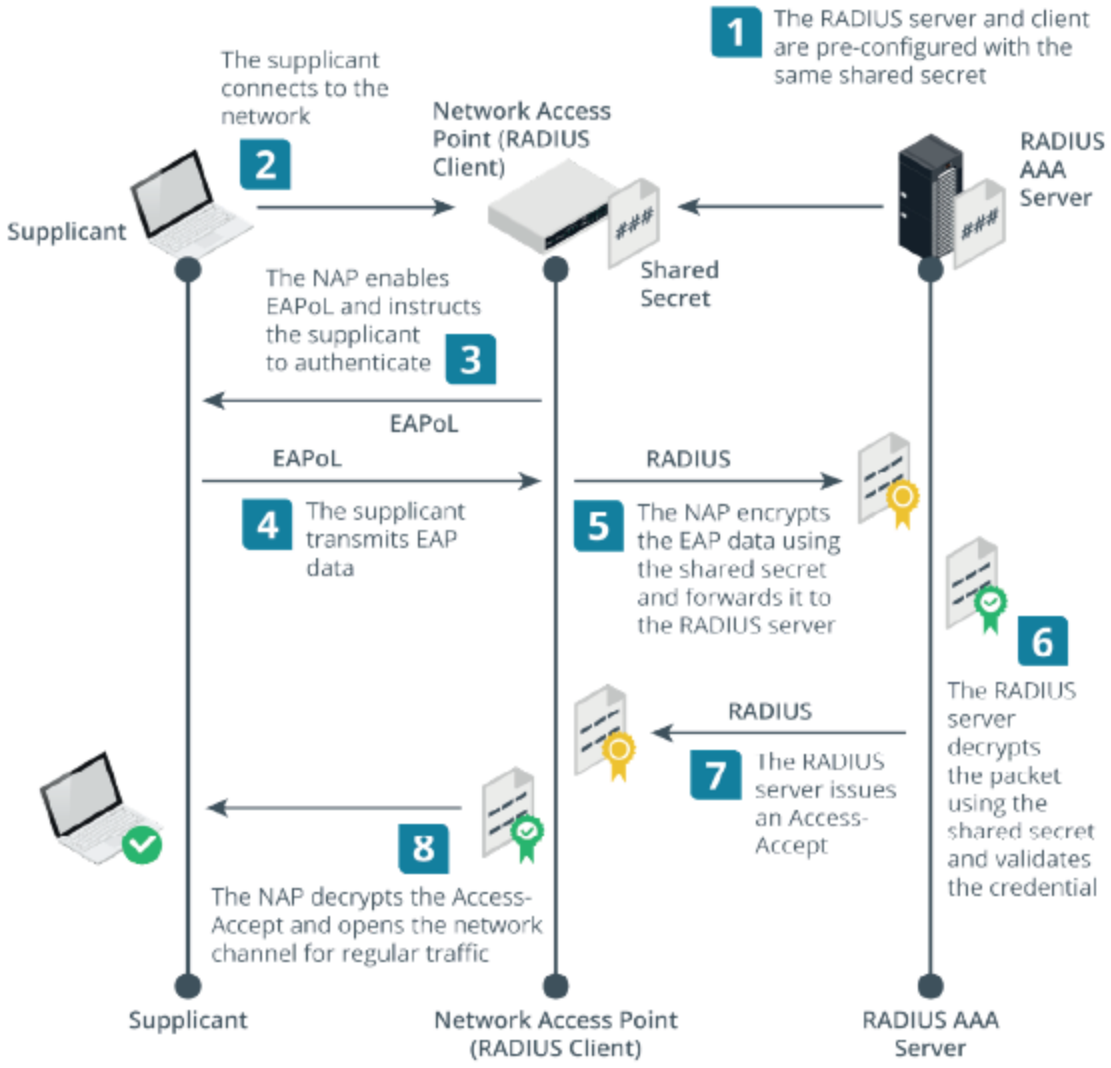
- In these scenarios, the **Extensible Authentication Protocol (EAP)** provides a framework for deploying multiple types of authentication protocols an technologies.
- EAP allows lots of different authentication methods, but many of them use digital certificate on the server and/or client machines.

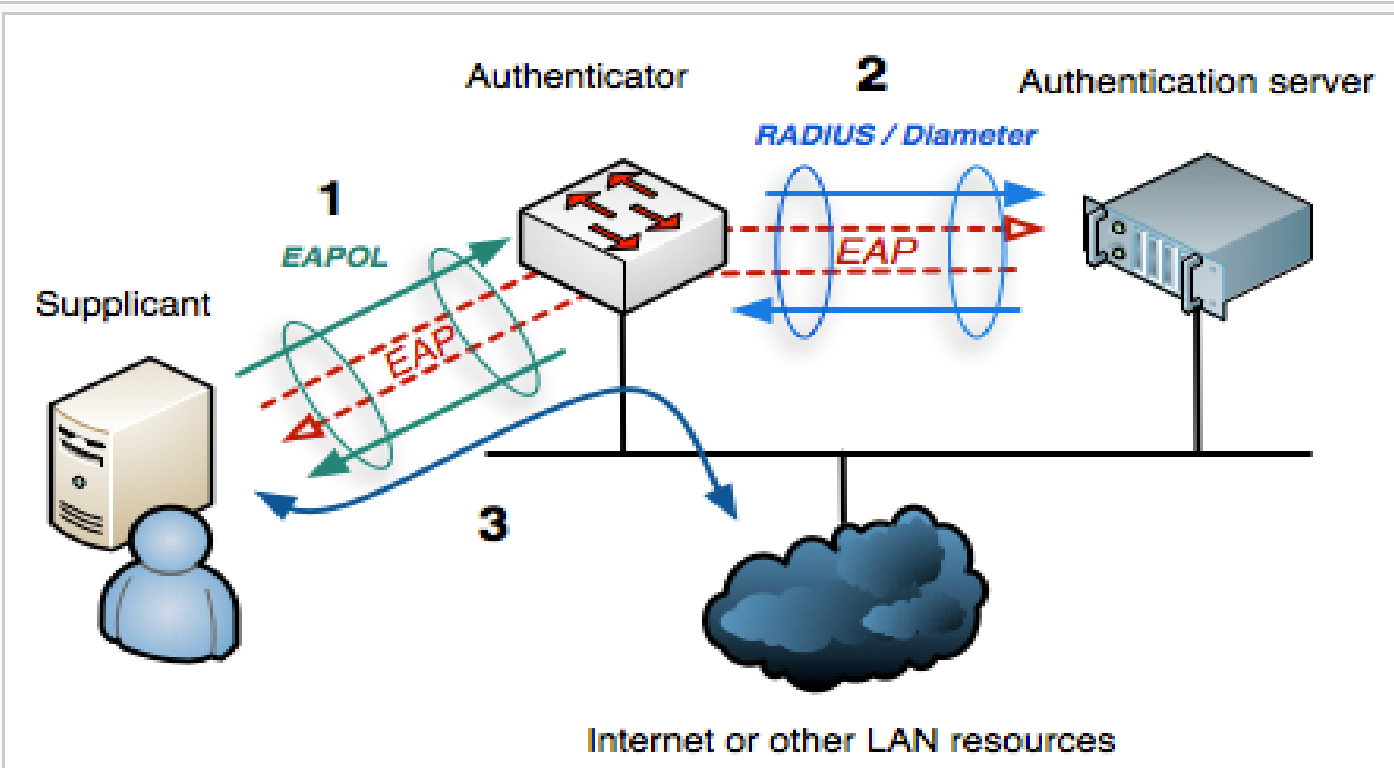
- 802.1X uses authentication, authorization, and accounting (AAA) architecture:
- • **Supplicant—**the device requesting access, such as a user's PC or laptop.
- • **Network access server (NAS)—**edge network appliances, such as switches, access points, and VPN gateways. These are also referred to as *RADIUS clients* or authenticators.
- • **AAA server—**the authentication server, positioned within the local network. With AAA, the NAS devices do not have to store any authentication credentials. They forward this data between the AAA server and the supplicant.
- There are two main types of AAA server: RADIUS and TACACS+.

RADIUS

- RADIUS stands for **Remote Authentication Dial-in User Service.**

- Communication between a network access server (NAS) and a RADIUS server is based on the User Datagram Protocol (UDP).
- Generally, the RADIUS protocol is considered a connectionless service.


1
The RADIUS server and client are pre-configured with the same shared secret
The supplicant connects to the network
2
Network Access Point (RADIUS Client)
RADIUS AAA Server
Supplicant
Shared Secret
The NAP enables EAPoL and instructs the supplicant to authenticate
3
EAPoL
EAPoL
RADIUS
4
The supplicant transmits EAP data
5
The NAP encrypts the EAP data using the shared secret and forwards it to the RADIUS server
6
The RADIUS server decrypts the packet using the shared secret and validates the credential
RADIUS
7
The RADIUS server issues an Access-Accept
8
The NAP decrypts the Access-Accept and opens the network channel for regular traffic
Supplicant
Network Access Point (RADIUS Client)
RADIUS AAA Server



EAP data is first encapsulated in EAPOL frames between the Supplicant and Authenticator, then re-encapsulated between the Authenticator and the Authentication server using RADIUS or Diameter.

Terminal Access Controller Access-Control System

- Centralizing administrative logins for network appliances
- Reliable TCP transport (over port 49)
- Data encryption
- authentication, authorization, and accounting functions

Token Keys and Static Codes

- A **one-time password (OTP)** is one that is generated automatically, rather than being chosen by a user, and used only once.

Open Authentication

- The **Initiative for Open Authentication (OATH)** is an industry body established
- with the aim of developing an open, strong authentication framework. *Open* means
- a system that any enterprise can link into to perform authentication of users and
- devices across different networks. *Strong* means that the system is based not just on
- passwords, but also on 2- or 3-factor authentication or on 2-step verification. OATH has
- developed two algorithms for implementing one time passwords (OTPs).

HMAC-Based One-Time Password Algorithm (HOTP)

- **HMAC-based One-time Password Algorithm (HOTP)** is an algorithm for token-based
- authentication. The authentication server and client token
- are configured with the same shared secret. This should be an 8-byte value generated
- by a cryptographically strong random number generator.

Time-Based One-Time Password Algorithm (TOTP)

- The **Time-based One-time Password Algorithm (TOTP)** is a refinement of the HOTP. One issue with HOTP is that tokens can be allowed to
- persist unexpired, raising the risk that an attacker might be able to obtain one and
- decrypt data in the future. In TOTP, the HMAC is built from the shared secret plus a
- value derived from the device's and server's local timestamps. TOTP automatically
- expires each token after a short window (60 seconds, for instance).

2-step verification

- *2-step verification* or *out-of-band mechanisms* generate a software token on a server and
- send it to a resource assumed to be safely controlled by the user. The token can be
- transmitted to the device in a number of ways:
- • Short Message Service (SMS)—the code is sent as a text to the registered phone
- number.
- • Phone call—the code is delivered as an automated voice call to the registered phone
- number.
- • Push notification—the code is sent to a registered authenticator app on the PC or
- smartphone.
- • Email—the code is sent to a registered email account.
- These mechanisms are sometimes also described as *2-factor authentication (2FA).*

Biometric Authentication Concepts

- Biometric authentication mechanisms allow users to access an account through a physiological feature (fingerprint or iris pattern, for instance) or behavioral pattern.

Biometric Authentication

- The first step in setting up **biometric authentication** is enrollment.
- The chosen biometric information is scanned by a biometric reader and converted to binary information.
- There are generally **two steps** in the scanning process:
  - **1.** A sensor module acquires the biometric sample from the target.
  - **2.** A feature extraction module records the features in the sample that uniquely identify the target.
- The biometric template is kept in the authentication server's database.
- When the user wants to access a resource, he or she is re-scanned, and the scan is compared to the template.
- If they match to within a defined degree of tolerance, access is granted.
- Several pattern types can be used to identify people biometrically.
- These can be categorized as physical (fingerprint, eye, and facial recognition) or behavioral (voice, signature, and typing pattern matching).

- Key metrics and considerations used to evaluate the efficacy rate of biometric pattern acquisition and matching and suitability as an authentication mechanism include the following:
  - **False Rejection Rate (FRR)**—where a legitimate user is not recognized. This is also referred to as a Type I error or false non-match rate (FNMR). FRR is measured as a percentage.

- **False Acceptance Rate (FAR)**—where an interloper is accepted (Type II error or false match rate [FMR]). FAR is measured as a percentage. False rejection cause inconvenience to users, but false acceptance can lead to security breaches, and so is usually considered the most important metric.
- **Crossover Error Rate (CER)**—the point at which FRR and FAR meet. The lower the CER, the more efficient and reliable the technology.

- Throughput (speed)—the time required to create a template for each user and the time required to authenticate. This is a major consideration for high traffic access points, such as airports or railway stations.
- Failure to Enroll Rate (FER)—incidents in which a template cannot be created and matched for a user during enrollment.

- Cost/implementation—some scanner types are more expensive, whereas others are not easy to incorporate on mobile devices.

- **Fingerprint Recognition:** Fingerprint recognition is the most widely implemented biometric authentication method.
- The technology required for scanning and recording fingerprints is relatively inexpensive and the process quite straightforward.
- A fingerprint sensor is usually implemented as a small capacitive cell that can detect the unique pattern of ridges making up the pattern.
- The technology is also non-intrusive and relatively simple to use, although moisture or dirt can prevent readings.

- **Facial Recognition:** Facial recognition records multiple indicators about the size and shape of the face, like the distance between each eye, or the width and length of the nose.

- The initial pattern must be recorded under optimum lighting conditions; depending on the technology, this can be a lengthy process.

- **Retinal scan—**an infrared light is throw into the eye to identify the pattern of blood vessels.
- The arrangement of these blood vessels is highly complex and typically does not change from birth to death, except in the event of certain diseases or injuries.
- Retinal scanning is therefore one of the most accurate forms of biometrics.
- Retinal patterns are very secure, but the equipment required is expensive and the process is relatively intrusive and complex.

- **Iris scan—**matches patterns on the surface of the eye using near-infrared imaging and so is less intrusive than retinal scanning (the subject can continue to wear glasses, for instance) and a lot quicker.
- Iris scanners offer a similar level of accuracy as retinal scanners but are much less likely to be affected by diseases.
- Iris scanning is the technology most likely to be rolled out for high-volume applications, such as airport security.
- There is a chance that an iris scanner could be fooled by a high resolution photo of someone's eye.

Behavioral Technologies

- Something you do refers to behavioral biometric pattern recognition.
- Rather than scan some attribute of your body, a template is created by **analyzing a behavior**, such as typing, writing a signature, or walking/moving.
- The variations in motion, pressure, or style are supposed to uniquely verify each individual.
- In practice, however, these methods are subject to **higher error rates**.

- Voice recognition—relatively cheap, as the hardware and software required are built into many standard PCs and mobiles.
- **Gait analysis**—produces a template from human movement (locomotion). The technologies can either be camera-based or use smartphone features, such as an accelerometer and gyroscope.

- Signature recognition—signatures are relatively easy to duplicate, but it is more difficult to fake the actual signing process. Signature matching records the user applying their signature (stroke, speed, and pressure of the stylus).
- Typing—matches the speed and pattern of a user's input of a passphrase.

- Some biometric and behavioral technologies might be used for purposes other than logon authentication:
- *Biometric identification* refers to matching people to a database, as opposed to authenticating them per se. **For example,** *if an individual crossing the floor of the data center does not produce a match for gait analysis, the system may raise a security alert.*

- *Continuous authentication* verifies that the user who logged on is still operating the device.
- **For example,** if a user successfully authenticates to a smartphone using a fingerprint, the device continues to monitor key motion and pressure statistics as the device is held and manipulated.

- If this deviates from the baseline, detection system would lock the phone.
- This sort of technology is not available on the market (at the time of writing), but it is the subject of numerous research projects.

SUMMARY

- You should be able to **assess the design and use** of authentication products for on-premises networks, web/cloud apps, and physical security in terms of meeting **confidentiality, integrity, and availability** requirements.
- Given a product-specific setup guide, you should be able to implement **protocols and technologies** such as Kerberos, smart card authentication, and EAP/RADIUS.
- You should also be able to identify signs of and risks from password attacks.

Guidelines for Implementing Authentication Controls

- Follow these guidelines when you implement authentication controls:
  - Assess the design requirements for confidentiality, integrity, and availability given the context for the authentication solution (private network, public web, VPN gateway, or physical site premises, for instance).
  - Determine whether a multifactor authentication (MFA) is required, and which hardware token or biometric technologies would meet the requirement when combined with a knowledge factor.

- Select an appropriate authentication protocol or framework.
- Assess risks from password attacks, especially when using legacy procotols (PAP and CHAP) and where hashes are exposed to capture.

- **Identity and account management controls** : identity and account types, account policies, authorization solutions, importance of personnel policies

- Identity and privilege management helps an organization to account for the actions of both regular and administrative users.

Identity Management Controls

- Certificates and smart cards
  - Public key cryptography
  - Subject identified by a public key, wrapped in digital certificate
  - Private key must be kept secure
- Tokens
  - In a single sign-on system, the user authenticates to an identity provider (IdP) and receives a cryptographic token. The user can present that token to compatible applications as proof they are authenticated, and receive authorizations from the application. With a token, there is always a risk that a malicious actor will be able to capture and replay it.
- Identity provider
  - The identity provider is the service that provisions the user account and processes authentication requests.

Background Check and Onboarding Policies

- Human resources (HR) and personnel policies
  - Recruitment (hiring): Security issues here include screening candidates and performing background checks.
  - Operation (working): HR managers devise training programs that communicate the importance of security to employees.
  - Termination/separation (firing or retiring): is a difficult process, with numerous security consequences.
- Background check
  - Employees working in high confidentiality environments or with access to high value transactions will obviously need to be subjected to greater degree of scrutiny.

- Onboarding: **Onboarding** at the HR level is the process of welcoming a ne employee to the organization.
  - **Secure transmission of credentials**: creating and sending an initial password or issuing a smart card securely.
  - Asset allocation: provision computers or mobile devices for the user or agree to the use of bring-your-own-device handsets.

  - Training/policies: schedule appropriate security awareness and role-relevant training and certification.

- **Non-disclosure Agreement (NDA):** When an employee or contractor signs an NDA, they are asserting that they will not share confidential information with a third party.

Personnel Policies for Privilege Management

- HR and IT must collaborate to ensure effective privilege management.
- These policies **aim to ensure** that the risk of ***insider*** threat is ***minimized***.

Separation of Duties

- **Standard operating procedures** (SOPs) mean that an employee has no excuse for not following protocol.

- **Shared authority** means that no one user is able to action or enable changes on his or her own authority. At least two people must authorize the change.

- **Least privilege** means that a user is granted sufficient rights to perform his or her job and no more.

- **Job rotation** (or rotation of duties) means that no one person is permitted to remain in the same job for an extended period.

- **Mandatory vacation** means that employees are forced to **take** their vacation time, during which someone else fulfills their duties.
- During that time, the corporate **audit** and security employees have time to **investigate and discover any discrepancies** in employee activity.

Offboarding Policies

- An exit interview (or **offboarding**) is the process of ensuring that an employee leaves a company **gracefully**.
- Offboarding is also used when a project using **contractors or third parties** ends.
- In terms of security, there are several processes that must be completed:

- Account management—**disable** the user account and privileges.
- Company assets—**retrieve** mobile devices, keys, smart cards, USB media, and so on.
- Personal assets—**wipe** employee-owned devices of corporate data and applications, depending on the **policies in force.**

Security Account Types and Credential Management

- Operating systems, network appliances, and network directory products use some standard account types as the basis of a privilege management system.
- These **include** standard user, administrative user, security group accounts, and service accounts.
- Standard users have ***limited privileges***, typically with access to run programs and to create and modify files belonging only to their profile.

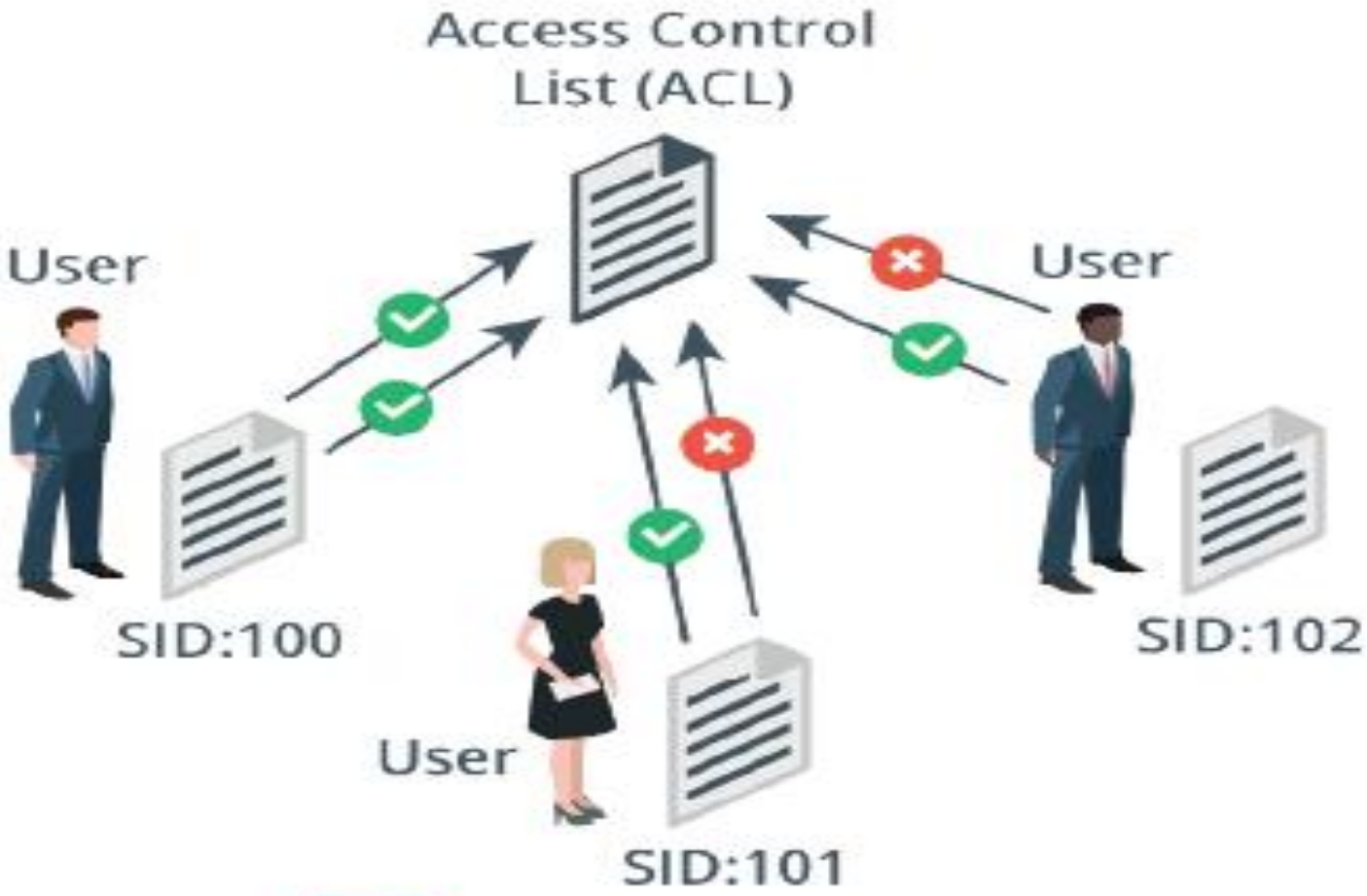
- a **credential management policy** should instruct users on how to keep their authentication method secure, whether this be a password, smart card, or biometric ID.
- The credential management policy also needs to alert users to diverse types of social engineering attacks.

- **Guest Accounts:** A guest account is a special type of shared account with **no password**.
- It allows anonymous and unauthenticated access to a resource.

Security Group-Based Privileges

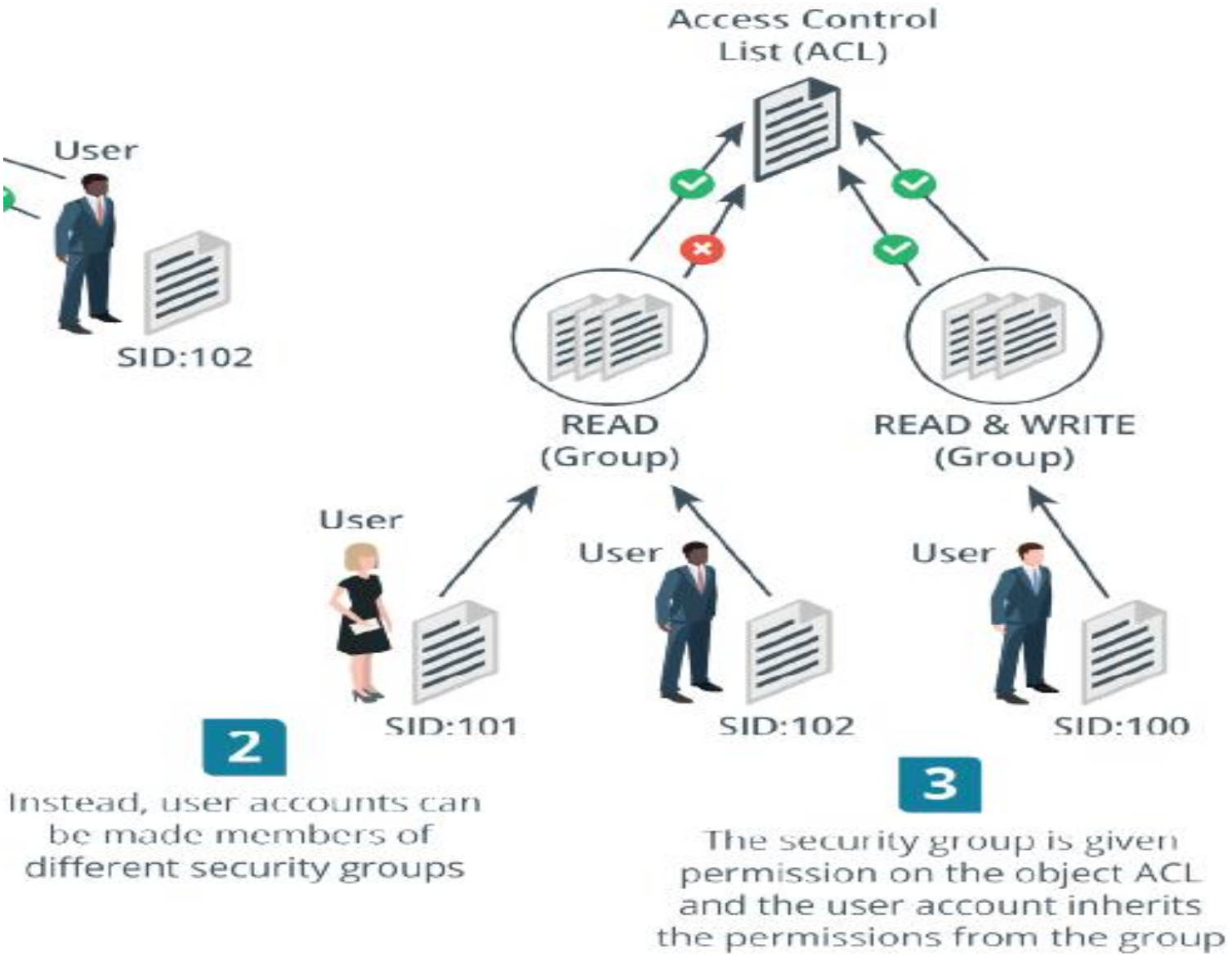
- The concept of a **security group account** simplifies and centralizes the administrative process of assigning rights.
- Rather than assigning rights directly, the system owner assigns them to security group accounts.

- User accounts gain rights by being made a member of a security group.
- A user can be a member of **multiple groups** and can therefore receive rights and permissions from several sources.



1

Assigning permissions directly to user accounts does not scale well


Access Control List (ACL)
User
SID:102
READ (Group)
READ & WRITE (Group)
User
SID:101
User
SID:102
User
SID:100
2
Instead, user accounts can be made members of different security groups
3
The security group is given permission on the object ACL and the user account inherits the permissions from the group

Administrator/Root Accounts

- Administrative or privileged accounts are **able** to install and remove apps and device drivers, change system-level settings, and access any object in the file system.

- A **default account** is one that is created by the operating system or application when it is installed.
- The default account has **every permission** available.
- In Windows, this account is called **Administrator**; in Linux, it is called **root**.
- This type of account is also referred to as a **superuser**.

- **Service accounts** are used by scheduled processes and application server software, such as databases.
- Windows has several default service account types.
- These do not accept user interactive logons but can be used to run processes and background services:

Shared/Generic/Device Accounts and Credentials

- A **shared account** is one where passwords (or other authentication credentials) are known to more than one person.

- Typically, simple **SOHO** networking devices do not allow for the creation of multiple accounts and a single "Admin" account is used to manage the device.
- These accounts might be configured with a default password.

Secure Shell Keys and Third-Party Credentials

- Secure Shell (SSH) is a widely used remote access protocol.
- It is very likely to be used to manage devices and services.
- SSH uses two types of key pairs:
  - A host key pair identifies an SSH server.
  - A user key pair is a means for a client to login to an SSH server.

- A **third-party credential** is one used by your company to manage a vendor service or cloud app.

Implement Account Policies

- Account policies enforce the privilege management policy by setting what users can and cannot do. This helps you to enforce strong credential policies and to detect and manage risks from compromised accounts. Auditing and permission reviews can reveal suspicious behavior and attempts to break through security.

Account Attributes and Access Policies

- **Account Attributes**
  - A user account is defined by a unique **security identifier (SID)**, a name, and a credential. Each account is associated with a profile. The profile can be defined with custom identity attributes describing the user, such as a full name, email address, contact number, department, and so on. The profile may support media, such as an account picture.

- **Access Policies**
  - Each account can be assigned permissions over files and other network resources and access policies or privileges over the use and configuration of network hosts. These permissions might be assigned directly to the account or inherited through membership of a security group or role.

Account Password Policy Settings

- System-enforced **account policies** can help to enforce credential management principles by stipulating requirements for user-selected passwords:
  - Password length
  - Password complexity
  - Password aging
  - Password reuse and history

Account Restrictions

- To make the task of compromising the user security system harder, account restrictions can be used.
- **Location-Based Policies**
  - A user or device can have a logical network location, identified by an IP address, subnet, virtual LAN (VLAN), or organizational unit (OU). This can be used as an account restriction mechanism.

- **Geofencing** refers to accepting or rejecting access requests based on location. Geofencing can also be used for push notification to send alerts or advice to a device when a user enters a specific area.

- Geotagging refers to the addition of location metadata to files or devices. This is often used for asset management to ensure devices are kept with the proper location.

- **Time-Based Restrictions:**
- There are three main types of time-based policies:
  - A **time of day policy** establishes authorized logon hours for an account.
  - A time-based login policy establishes the maximum amount of time an account may be logged in for.

- An impossible travel time/risky login policy tracks the location of login events over time. If these do not meet a threshold, the account will be disabled. For example, a user logs in to an account from a device in New York. A couple of hours later, a login attempt is made from LA, but this is refused and an alert raised because it is not feasible for the user to be in both locations.

Account Audits

- Accounting and auditing processes are used to detect whether an account has been compromised or is being misused.



Account Permissions

- Where many users, groups, roles, and resources are involved, managing account permissions is complex and time-consuming. Improperly configured accounts can have two different types of impact. On the one hand, setting privileges that are too restrictive creates a large volume of support calls and reduces productivity. On the other hand, granting too many privileges to users weakens the security of the system and increases the risk of things like malware infection and data breach.

Usage Audits

- Usage auditing means configuring the security log to record key indicators and then reviewing the logs for suspicious activity.

Account Lockout and Disablement

- If account misuse is detected or suspected, the account can be manually disabled by setting an account property. This prevents the account from being used for login.

Implement Authorization Solutions

- **Discretionary and Role-Based Access Control:** An important consideration in designing a security system is to determine how users receive rights or **permissions**.

- **Discretionary access control (DAC)** is based on the primacy of the resource owner. The owner is granted full control over the resource, meaning that he or she can modify its access control list (ACL) to grant rights to others.

- **Role-based access control (RBAC)** adds an extra degree of centralized control to the DAC model. Under this system, the right to modify roles is reserved to a system owner.

- **File System Permissions**



Mandatory and Attribute-Based Access Control

- **Mandatory access control (MAC)** is based on the idea of security clearance levels.

- **Attribute-based access control (ABAC)** is the most fine-grained type of access control model.

- **Rule-based access control** is a term that can refer to any sort of access control model where access control policies are determined by system-enforced rules rather than system users.

- **Directory services** are the principal means of providing privilege management and authorization on an enterprise network, storing information about users, computers, security groups/roles, and services.

Federation and Attestation

- **Federation** is the notion that a network needs to be accessible to more than just a well-defined group of employees. In business, a company might need to make parts of its network open to partners, suppliers, and customers.

- ***ADDITIONAL READING IS STRONGLY RECOMMENDED***

References

- https://www.lbmc.com/blog/three-tenets-of-information-security/
- https://www.tcdi.com/information-security-compliance-which-regulations/
- https://www.edureka.co/blog/what-is-cryptography/
- https://www.thesslstore.com/blog/what-is-pki-a-crash-course-on-public-key-infrastructure-pki/
- http://www.netcontractor.pl/blog/?p=221
- https://aboutssl.org/root-certificates-vs-intermediate-certificates/
- https://aboutssl.org/about-ssl/
- https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption
- https://opensource.com/resources/what-open-source
- https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html