MODULE 5

IMPLEMENTING ACCESS CONTROL, AUTHENTICATION, AND ACCOUNT MANAGEMENT

FEU ALABANG FEU DILIMAN FEU TECH

Technology Driven by Innovation

ACCESS CONTROL AND AUTHENTICATION SERVICES

SUBTOPIC 1

OBJECTIVES

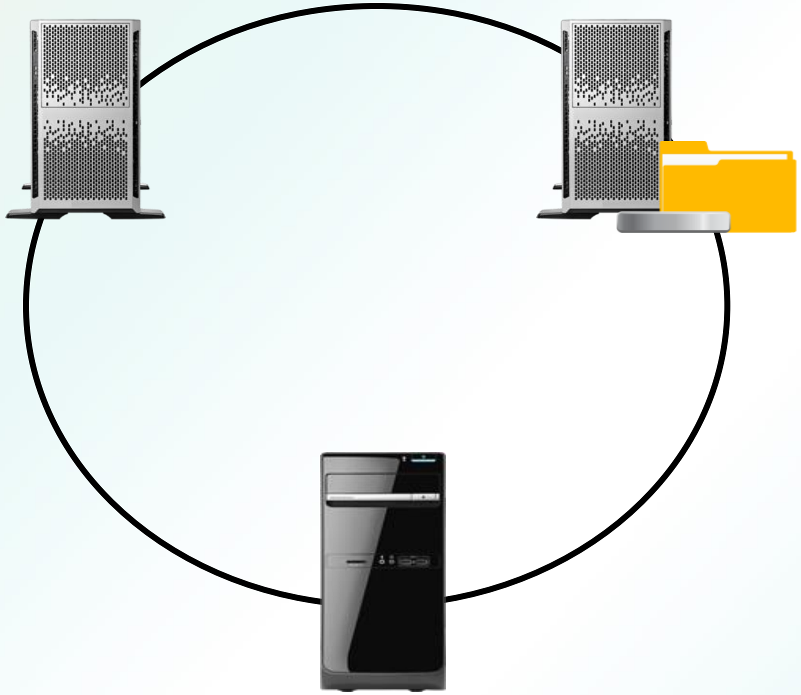
Upon completion of this module, the student would be able to:

- Define the Access Control and its goals;
- Demonstrate the concepts of Directory Services;
- Enumerate the types of securing remote access

ACCESS CONTROL

Access control is a way of limiting access to a system or to physical or virtual resources.

Directory Services



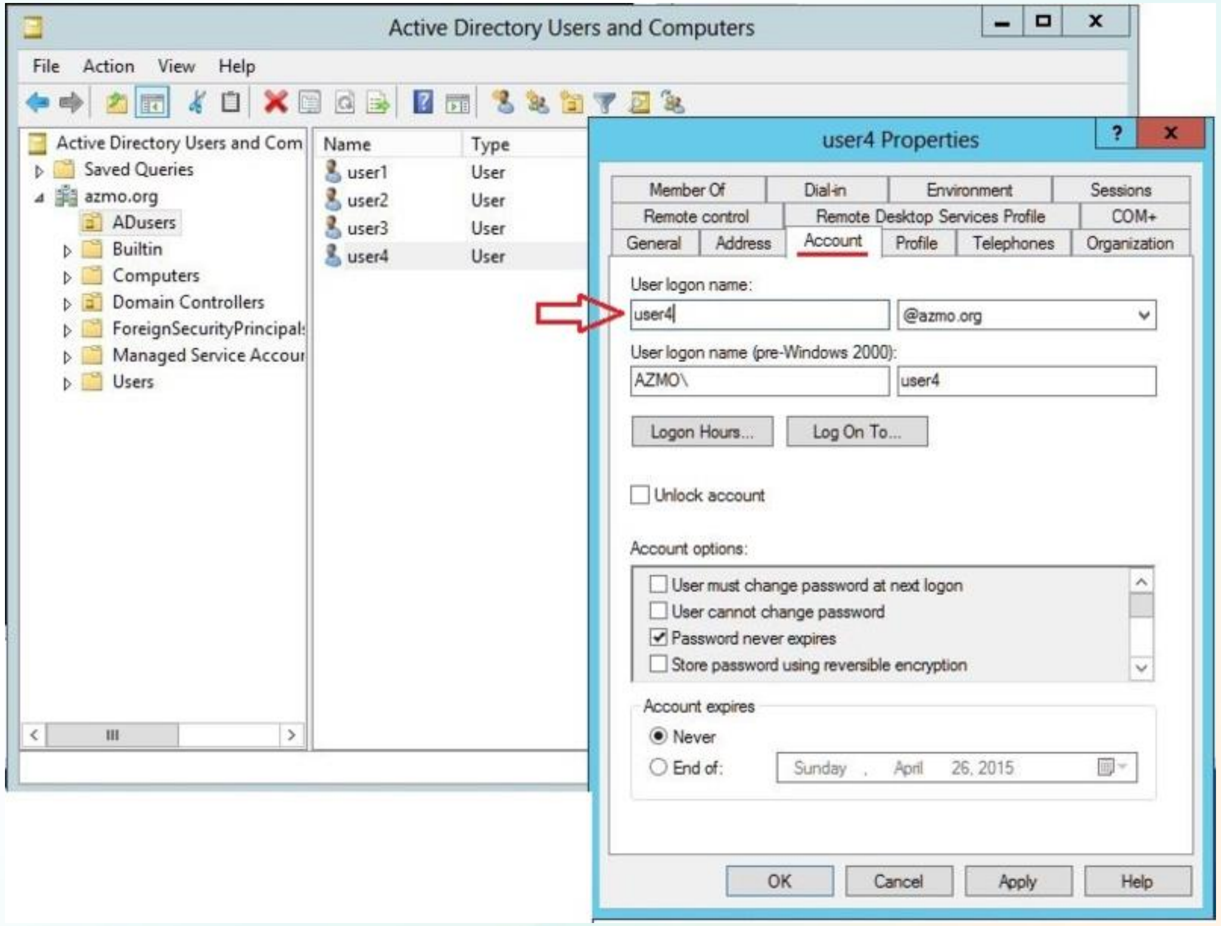
Authentication

Centralized Administration

A **directory service** stores, organizes, and provides access to information in a directory.

Active Directory

Active Directory is a directory services implementation that provides all sorts of functionality like authentication, group and user management, policy administration and more.



Name	Type
user1	User
user2	User
user3	User
user4	User

User logon name:
user4 @azmo.org

User logon name (pre-Windows 2000):
AZMO\ user4

□ Unlock account

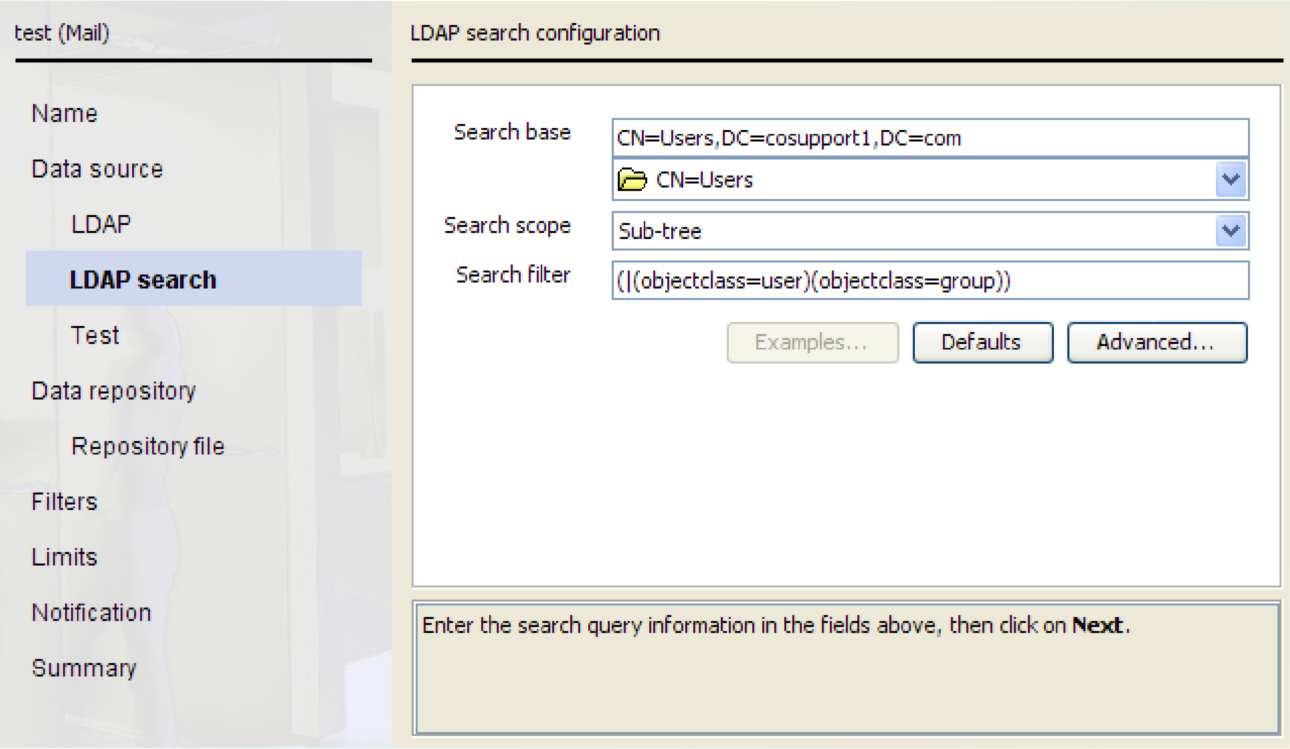
Account options:

□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires
● Never
○ End of: Sunday , April 26, 2015

LDAP

LDAP (Lightweight Directory Access Protocol) is an open and cross platform protocol used for directory services authentication.



Search base: CN=Users,DC=cosupport1,DC=com

CN=Users

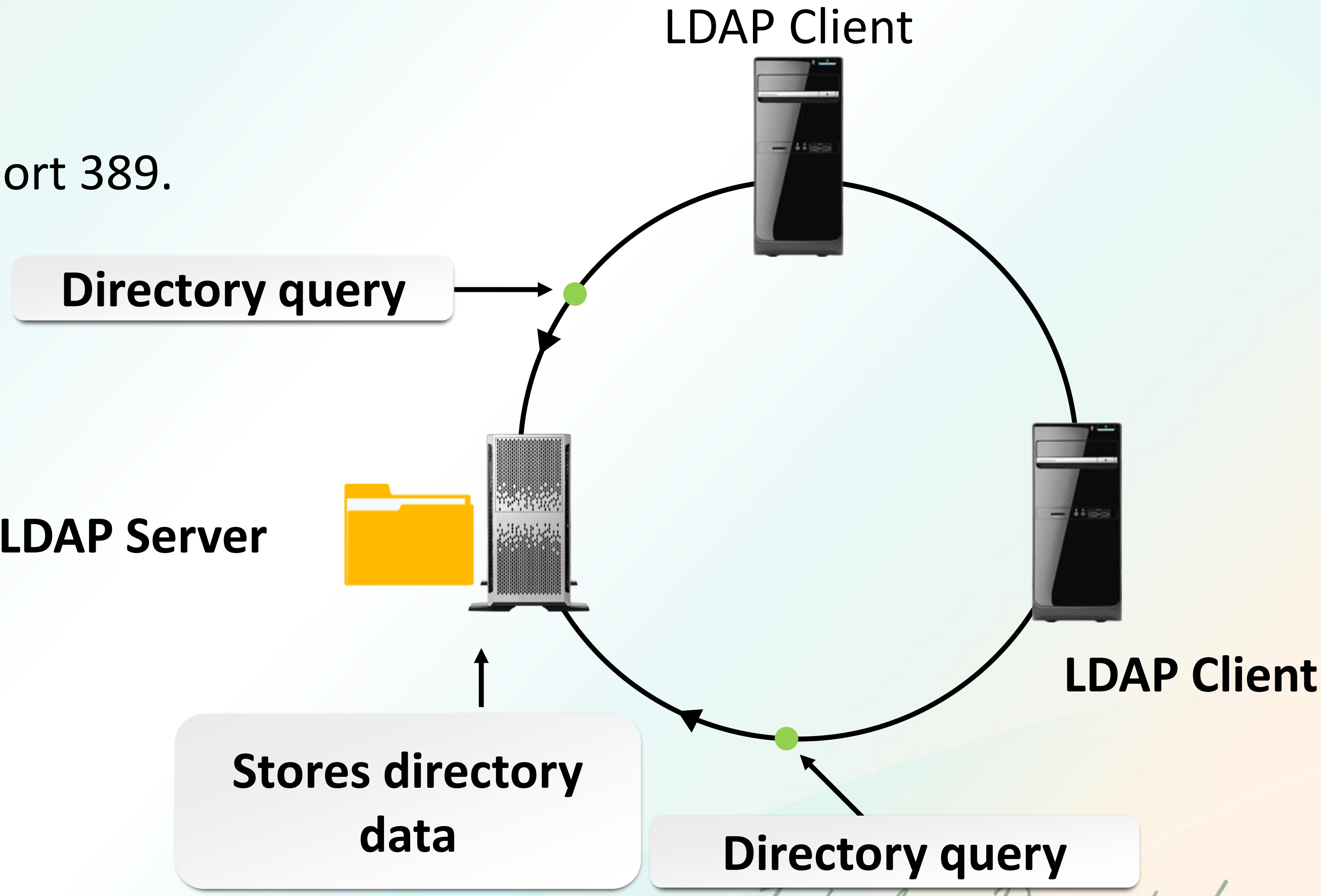
Search scope: Sub-tree

Search filter: (|(objectclass=user)(objectclass=group))

Enter the search query information in the fields above, then click on **Next**.

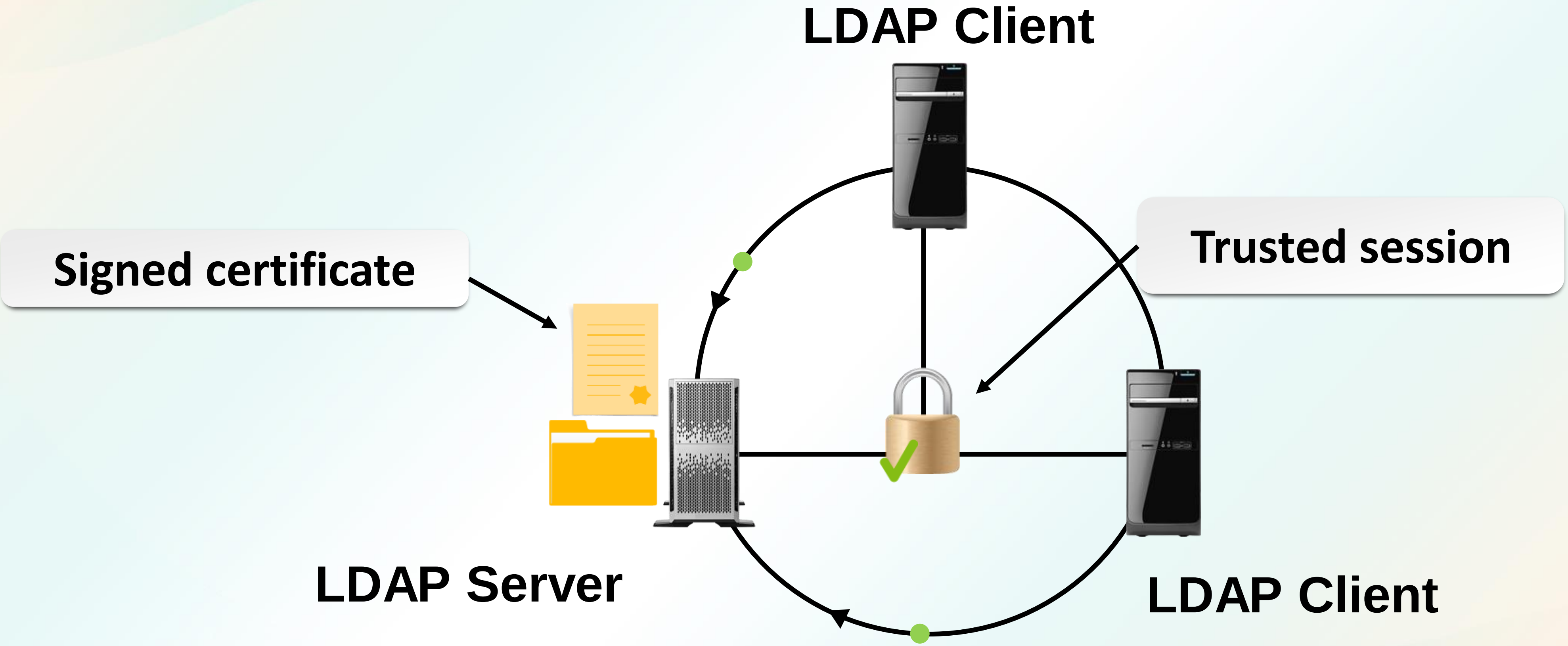
LDAP

LDAP makes use of port 389.



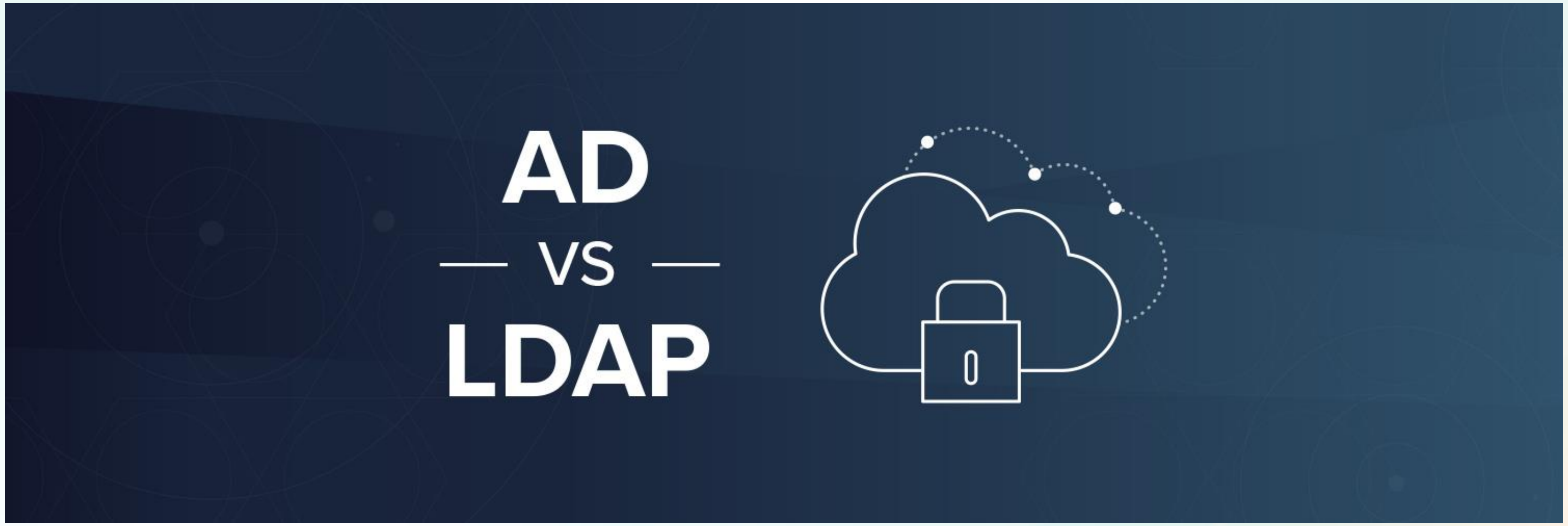
LDAP

Port 636 is used for secure LDAP (LDAPS).



LDAP vs. Active Directory

Realistically, there are probably more differences than similarities between the two directory solutions. Microsoft's AD is largely a directory for Windows® users, devices, and applications. AD requires a Microsoft Domain Controller to be present and when it is, users are able to single sign-on to Windows resources that live within the domain structure.

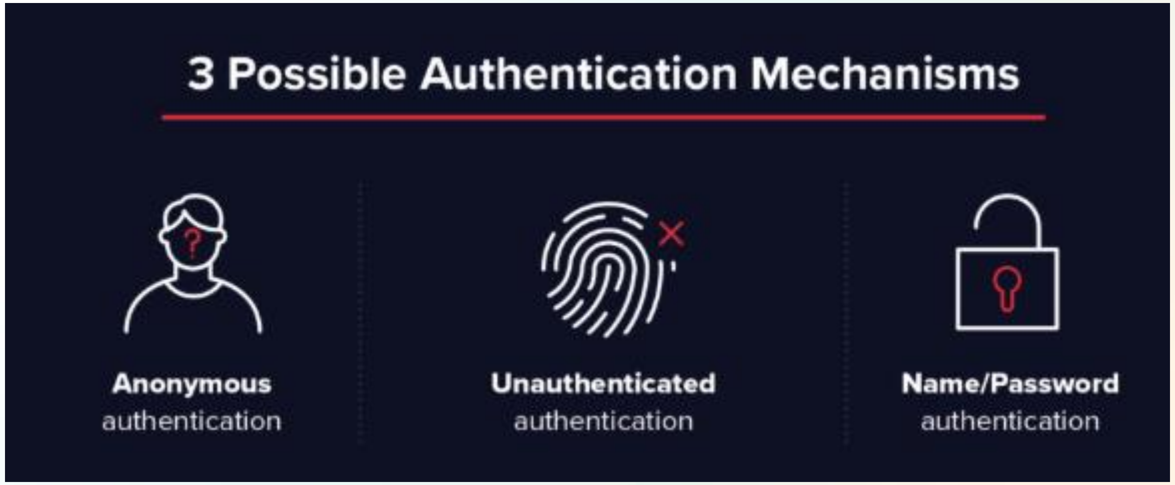


LDAP Authentication

There are two options for LDAP authentication in LDAP v3 – simple and SASL (Simple Authentication and Security Layer).

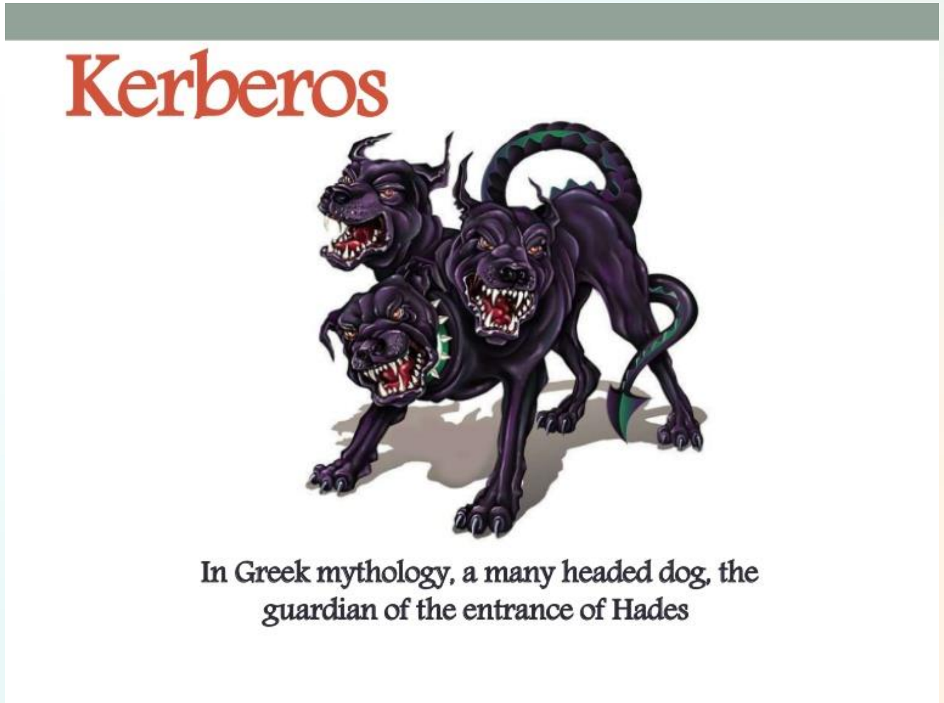
Simple authentication allows for three possible authentication mechanisms:

- ❑ **Anonymous authentication**
- ❑ **Unauthenticated authentication**
- ❑ **Name/Password authentication**


3 Possible Authentication Mechanisms
Anonymous authentication
Unauthenticated authentication
Name/Password authentication

Kerberos

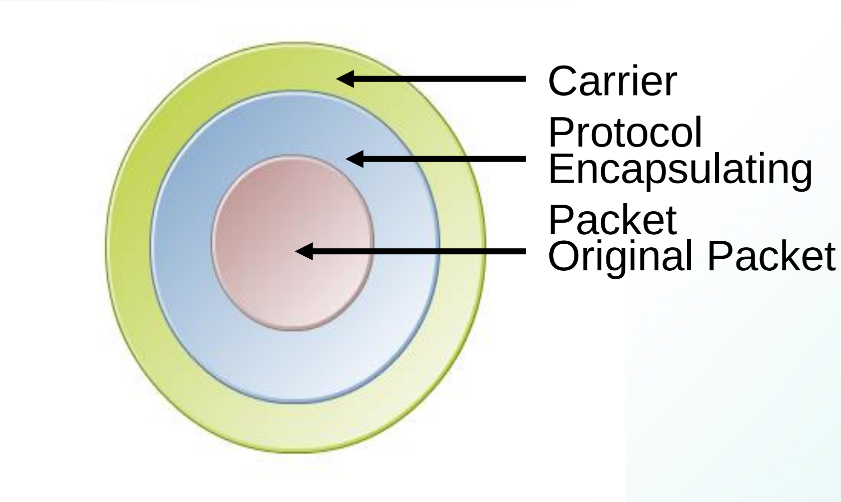
- ❑ Based on a time-sensitive ticket granting system.
- ❑ Developed by MIT to use SSO.
- ❑ Can manage access control to many services using one centralized authentication server.

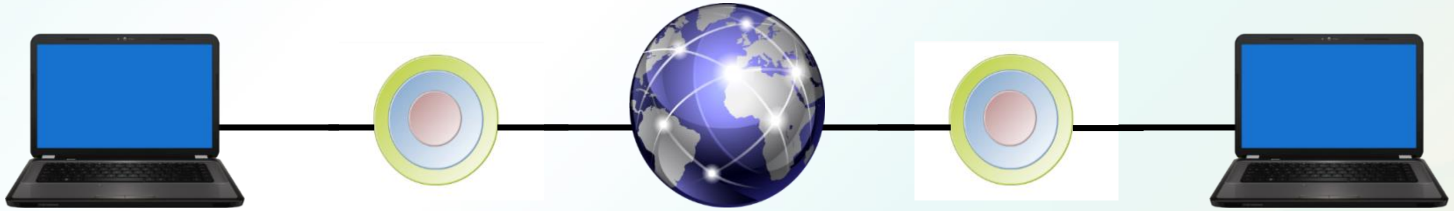


Kerberos

In Greek mythology, a many headed dog, the guardian of the entrance of Hades

Tunneling - A tunneling protocol is a communications protocol that allows for the movement of data from one network to another

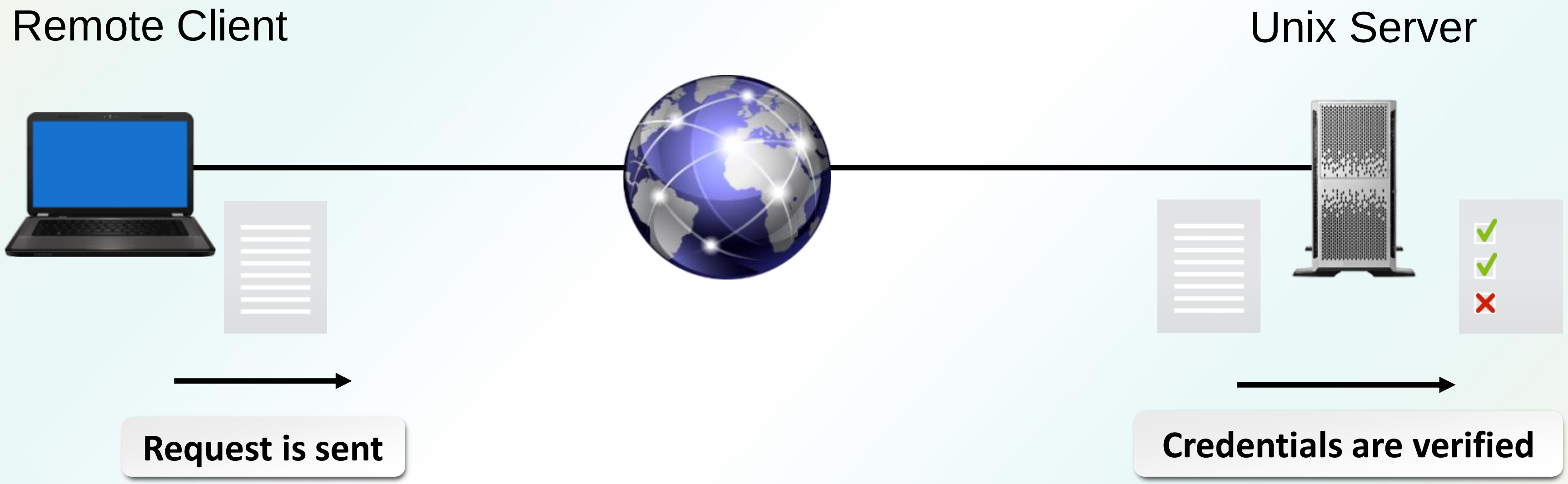




The three types of tunneling protocols used with a VPN server/RAS server running on Windows Server 2008 R2 include:

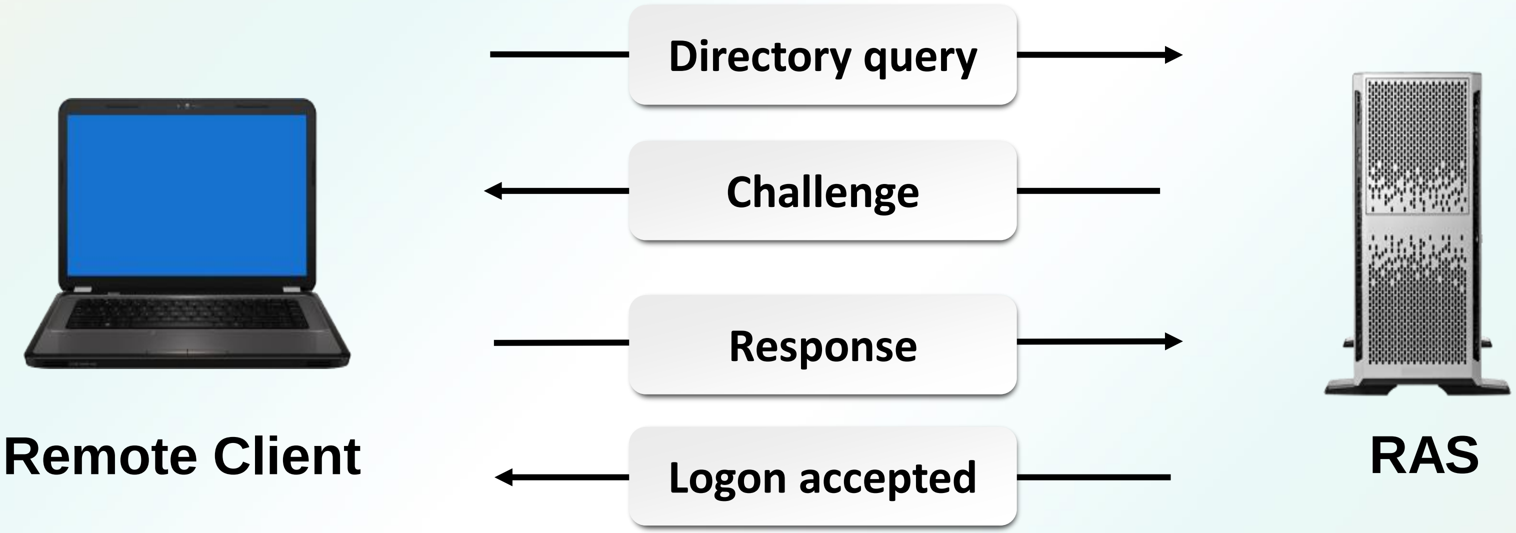
- ❑ **Point-to-Point Tunneling Protocol (PPTP)**
- ❑ **Layer 2 Tunneling Protocol (L2TP)**
- ❑ **Secure Socket Tunneling Protocol (SSTP**

PAP - Password Authentication Protocol



Password Authentication Protocol (PAP): Uses plain text (unencrypted passwords).

CHAP - Challenge-Handshake Authentication Protocol



Directory query

Challenge

Response

Logon accepted

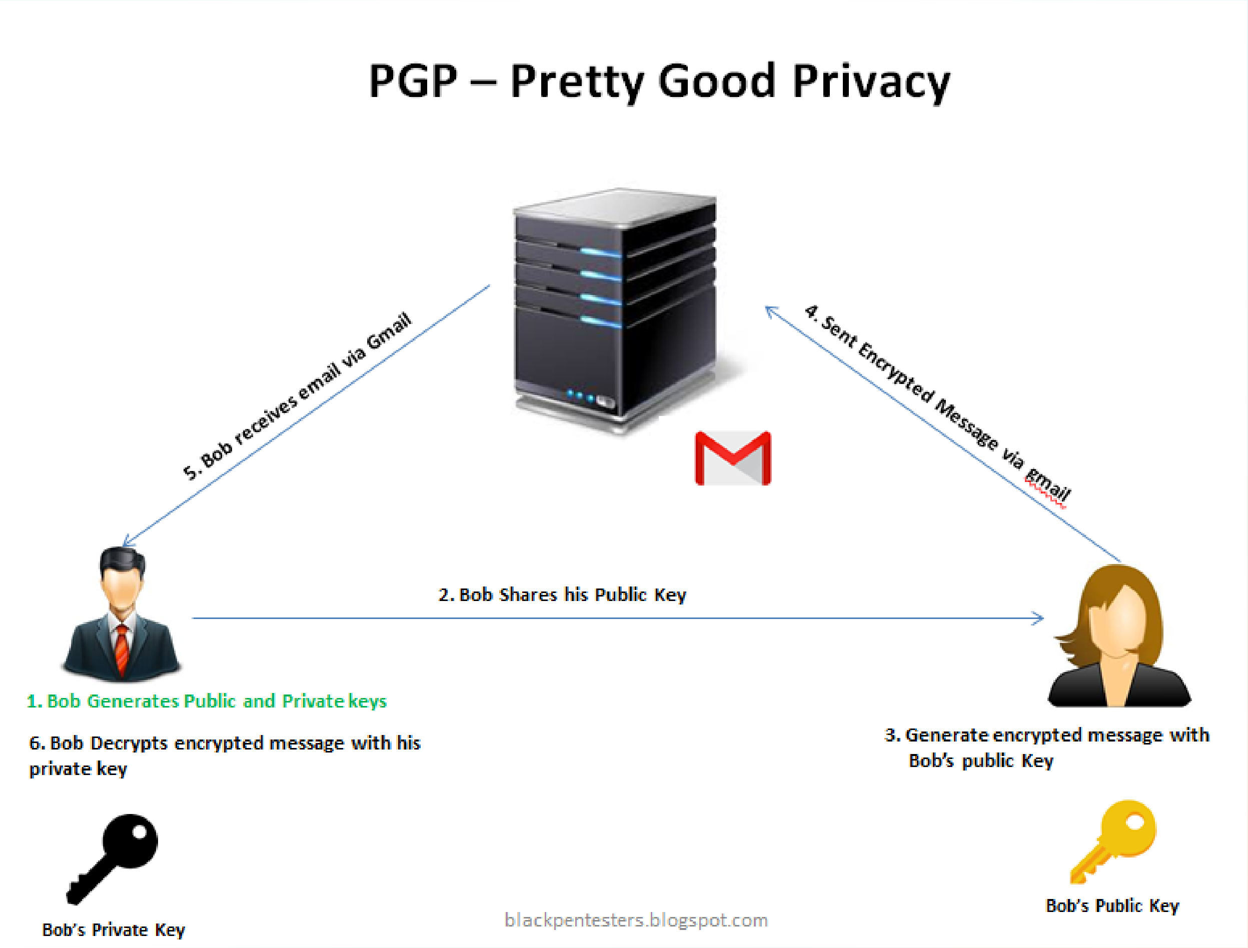
Remote Client

RAS

Challenge Handshake Authentication Protocol (CHAP): A challenge-response authentication that uses the industry standard md5 hashing scheme to encrypt the response.

PGP - Pretty Good Privacy

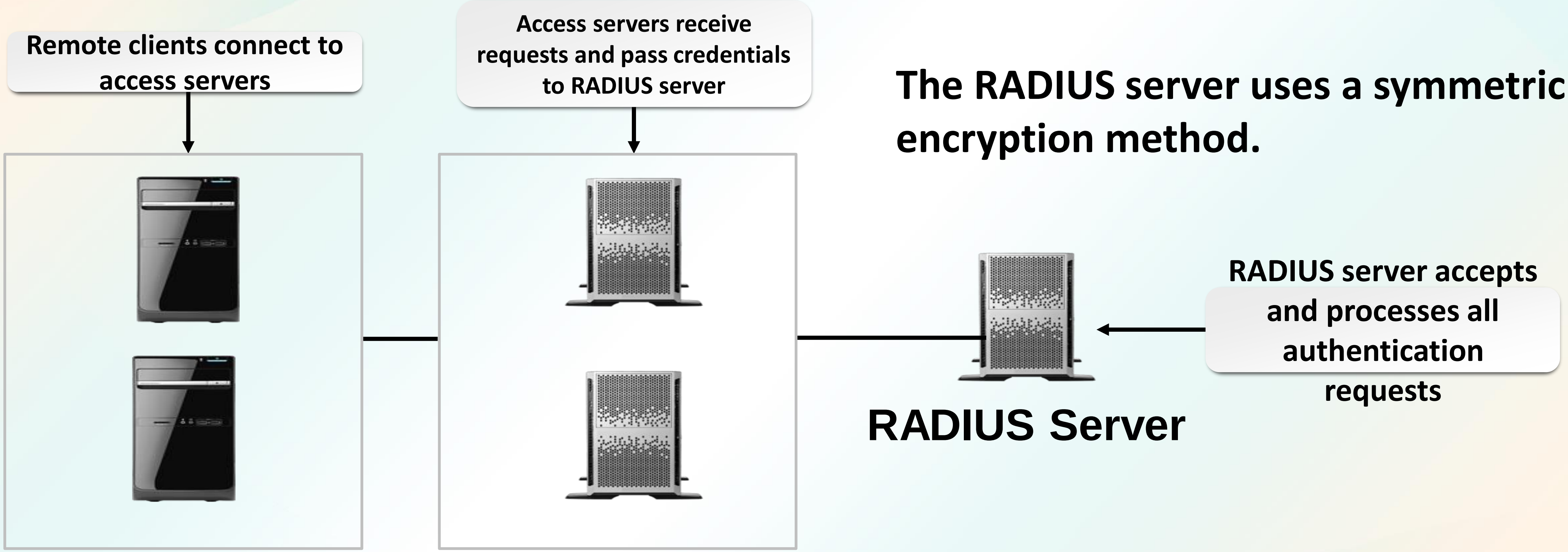
- ❑ **Public email security**
- ❑ **Digital signing**
- ❑ **Encrypt message contents and encrypt key**


PGP – Pretty Good Privacy
5. Bob receives email via Gmail
4. Sent Encrypted Message via gmail
2. Bob Shares his Public Key
1. Bob Generates Public and Private keys
6. Bob Decrypts encrypted message with his private key
3. Generate encrypted message with Bob's public Key
Bob's Private Key
Bob's Public Key
blackpentesters.blogspot.com

Pretty Good Privacy (PGP) is a freeware email encryption system that uses symmetrical and asymmetrical encryption. When an email is sent, the document is encrypted with the public key and a session key.

RADIUS - Remote Authentication Dial-In User Service

The RADIUS server uses a symmetric encryption method.



Remote clients connect to access servers

Access servers receive requests and pass credentials to RADIUS server

RADIUS server accepts and processes all authentication requests

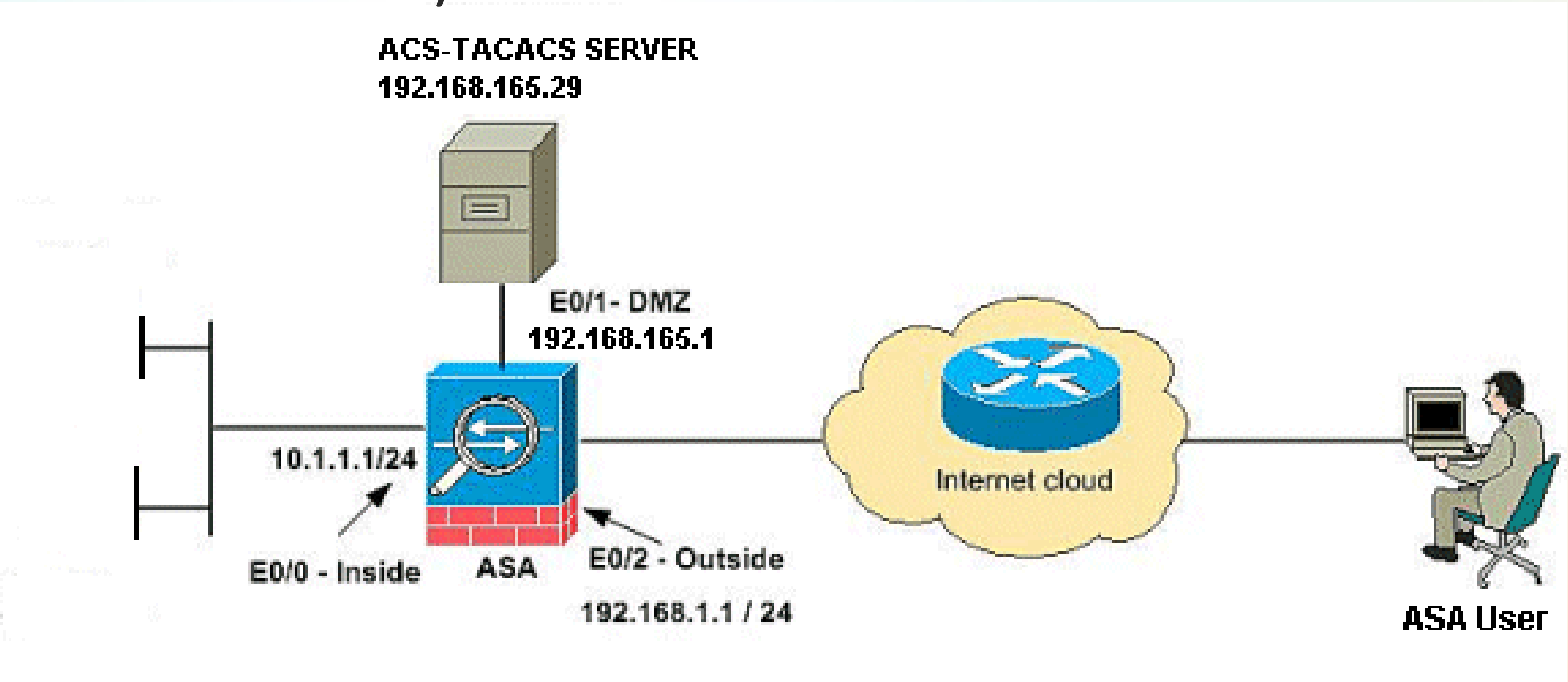
RADIUS Server

Remote Clients

Access Servers Configured as RADIUS Clients

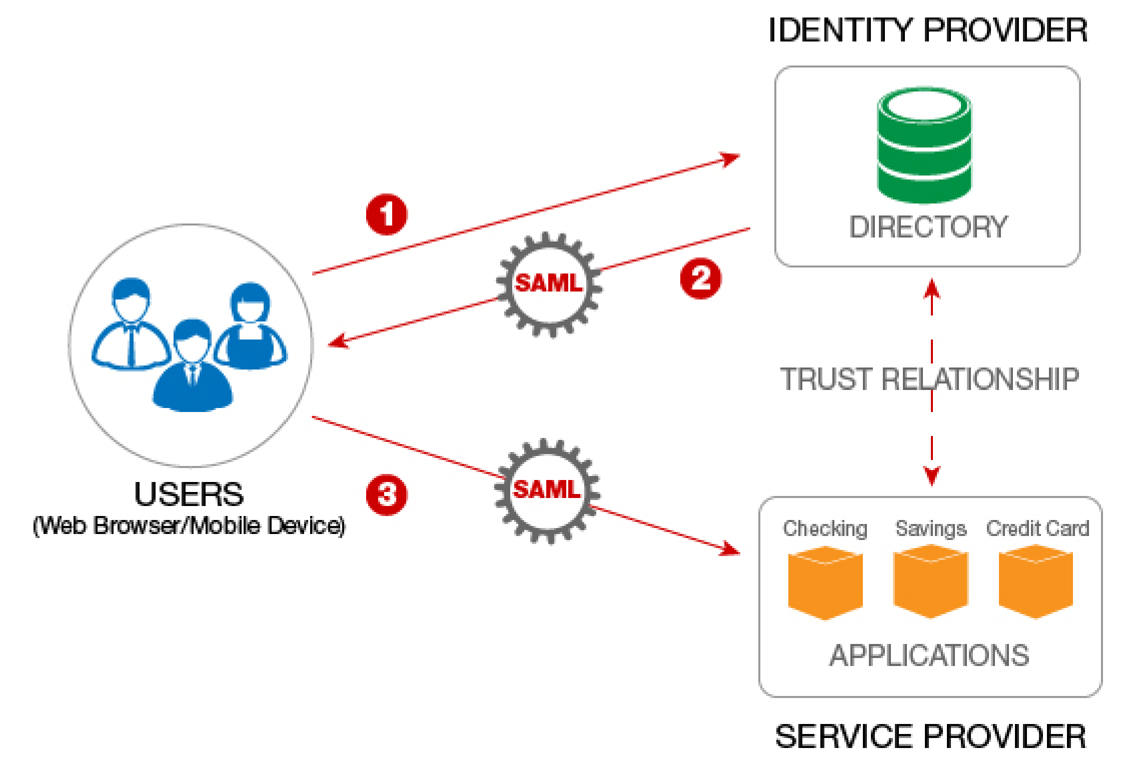
TACACS

- ❑ **TACACS** is known as **Terminal Access Controller Access Control System**, is a remote protocol used to link with a server in networks.
- ❑ It permits a remote access server to connect with an authentication server to determine if the user has access to the system.

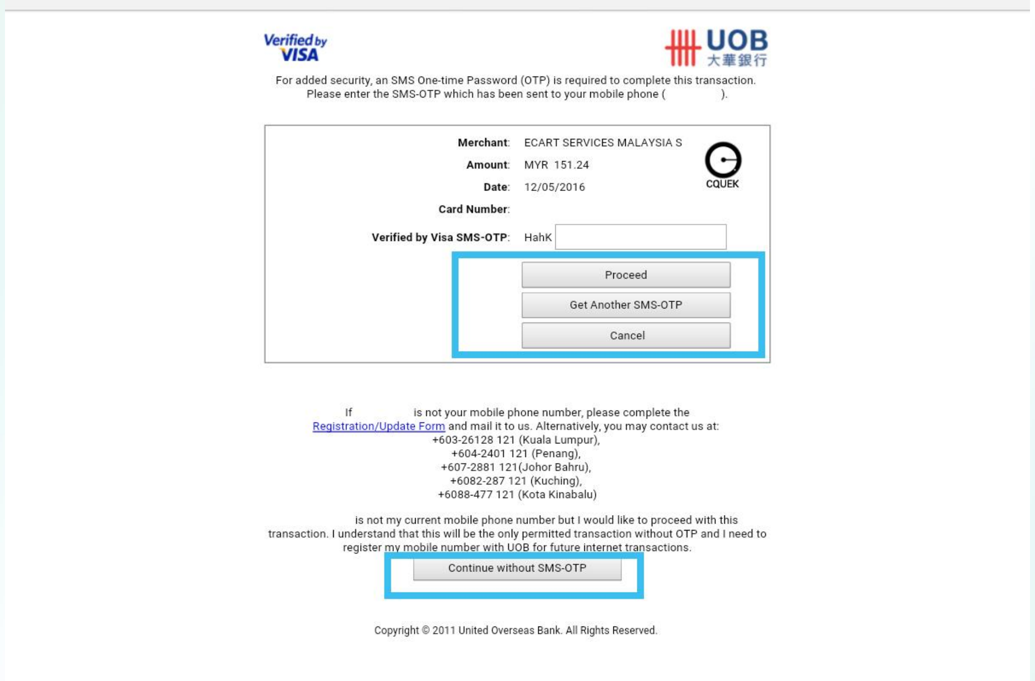


SAML - Security Assertion Markup Language

Security Assertion Markup Language (SAML) is an open standard that allows identity providers (IdP) to pass authorization credentials to service providers (SP).



One-Time Passwords – HOTP and TOTP



For added security, an SMS One-time Password (OTP) is required to complete this transaction.
Please enter the SMS-OTP which has been sent to your mobile phone ( ).

Merchant:	ECART SERVICES MALAYSIA S
Amount:	MYR 151.24
Date:	12/05/2016
Card Number:	
Verified by Visa SMS-OTP:	HahK

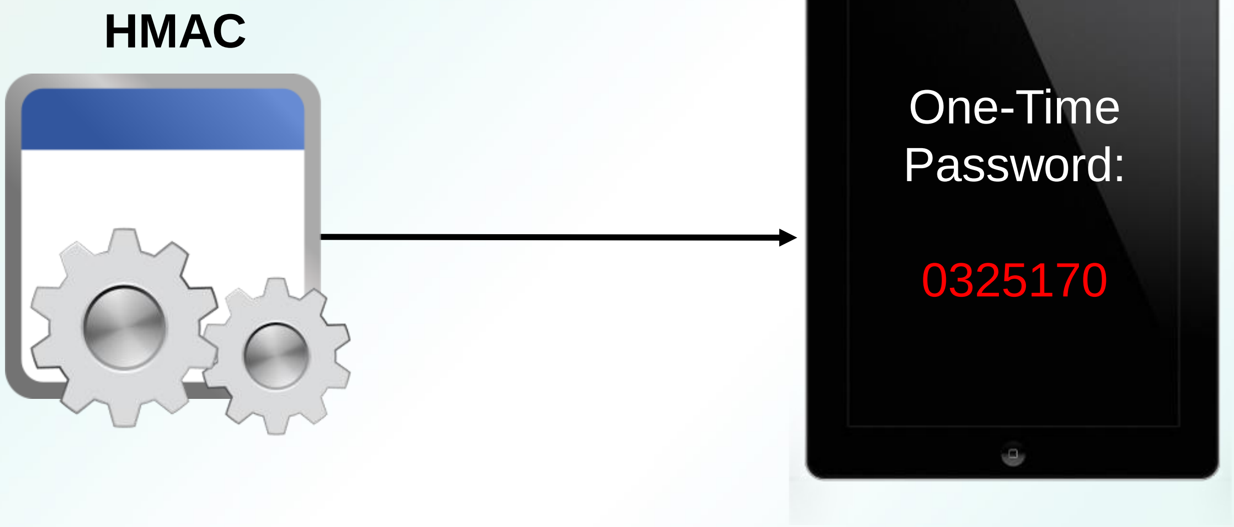
If is not your mobile phone number, please complete the
Registration/Update Form and mail it to us. Alternatively, you may contact us at:
+603-26128 121 (Kuala Lumpur),
+604-2401 121 (Penang),
+607-2881 121(Johor Bahru),
+6082-287 121 (Kuching),
+6088-477 121 (Kota Kinabalu)

is not my current mobile phone number but I would like to proceed with this transaction. I understand that this will be the only permitted transaction without OTP and I need to register my mobile number with UOB for future internet transactions.

Copyright © 2011 United Overseas Bank. All Rights Reserved.

One-Time Passwords (OTP) are pretty much what their name says: a password that can be only used one time.

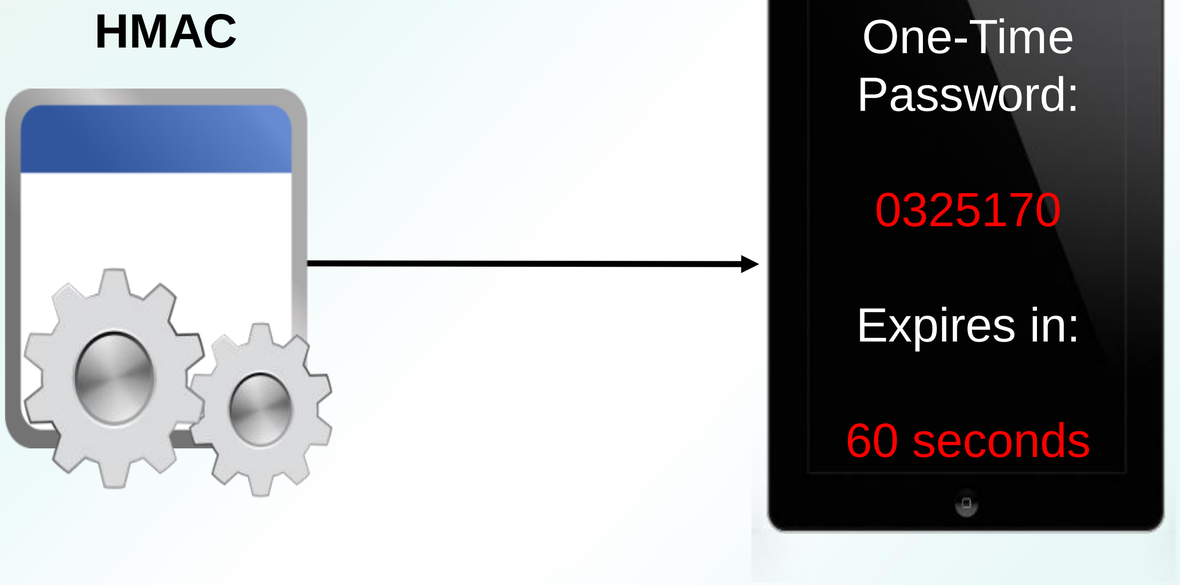
HOTP



HMAC-based one-time password (HOTP) tokens are devices that generate passwords based on a nonrepeating one-way function. It is not restricted to time.

TOTP - Time-based One-Time Password

Tokens are devices or applications that generate passwords at fixed time intervals. Therefore, the password will only be valid for a predefined time interval.



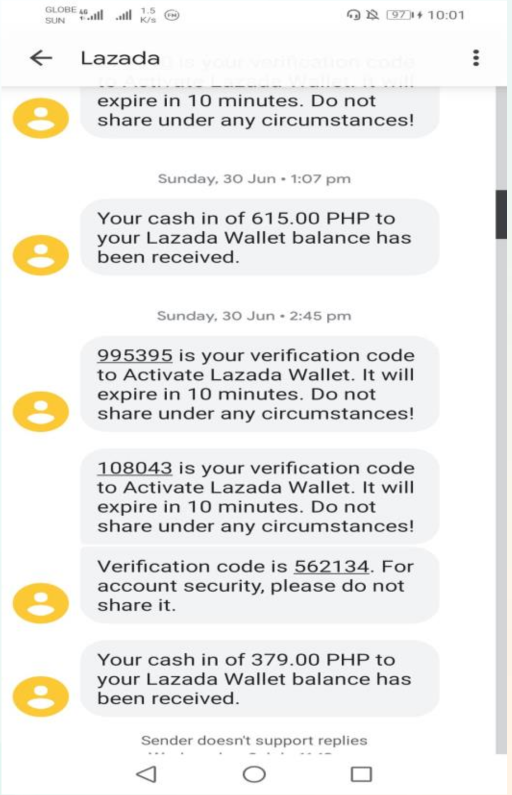
HMAC

One-Time Password:

0325170

Expires in:

60 seconds



10:01

Lazada

expire in 10 minutes. Do not share under any circumstances!

Sunday, 30 Jun • 1:07 pm

Your cash in of 615.00 PHP to your Lazada Wallet balance has been received.

Sunday, 30 Jun • 2:45 pm

995395 is your verification code to Activate Lazada Wallet. It will expire in 10 minutes. Do not share under any circumstances!

108043 is your verification code to Activate Lazada Wallet. It will expire in 10 minutes. Do not share under any circumstances!

Verification code is 562134. For account security, please do not share it.

Your cash in of 379.00 PHP to your Lazada Wallet balance has been received.

Sender doesn't support replies

IMPLEMENT ACCOUNT MANAGEMENT SECURITY CONTROLS

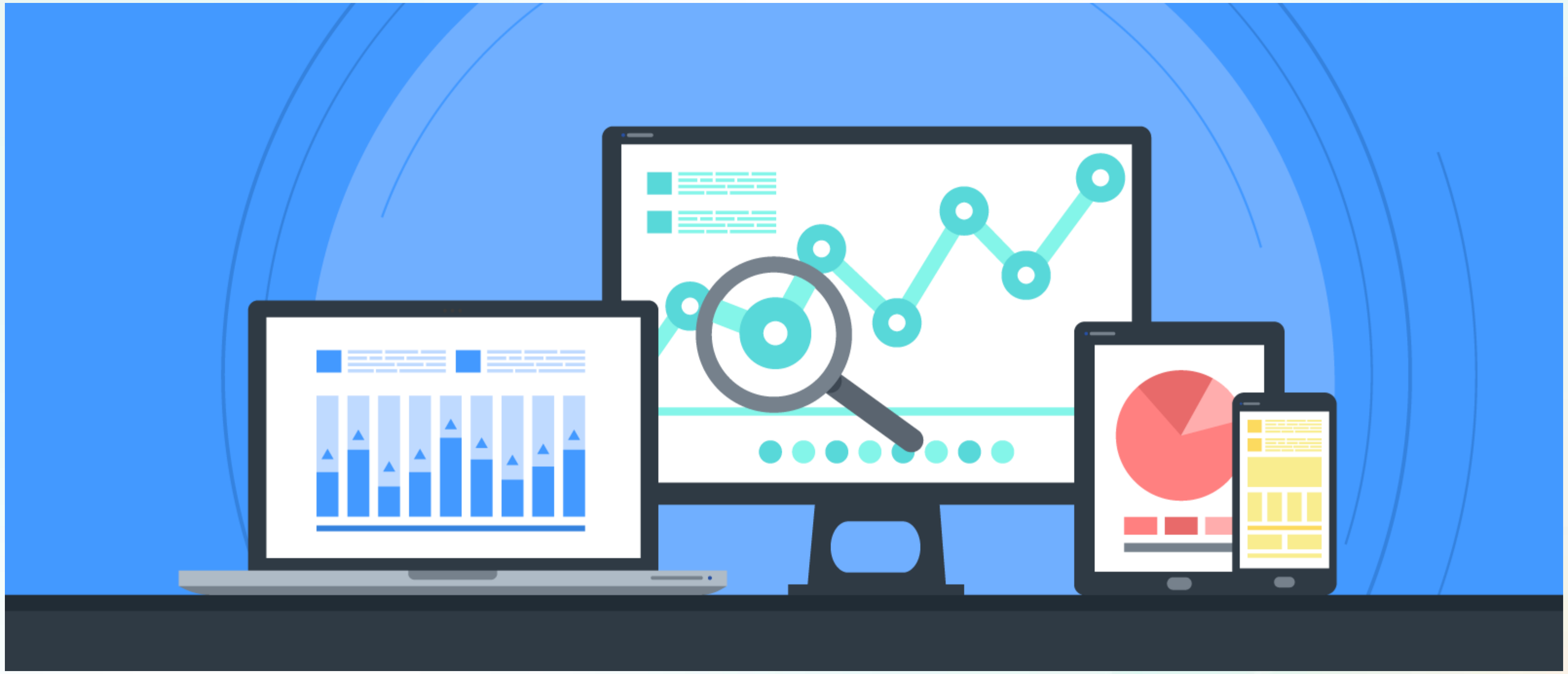
SUBTOPIC 2

OBJECTIVES

Upon completion of this module, the student would be able to:

- Explain the concepts of account management security controls;
- Discuss Account Management Security Controls concepts;
- Give different Account Policy concepts;

ACCOUNT MANAGEMENT is one of the most important aspects of an organization’s security posture.



ACCOUNT TYPES

USER ACCOUNT holds the most limited amount of access to a system, but it is also the level that the vast majority of users have.

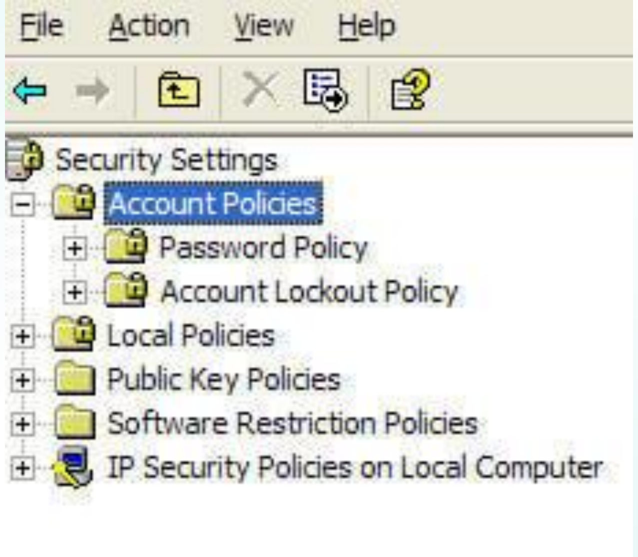
A **SHARED ACCOUNT**, sometimes known as a generic account, is one that can be utilized by more than one assigned user.

SERVICE ACCOUNTS control the privileges and functions of an application.

PRIVILEGED ACCOUNTS should be defined for each administrative role and system within an organization, allowing for separation of duties and preventing too much power being placed in too few accounts.

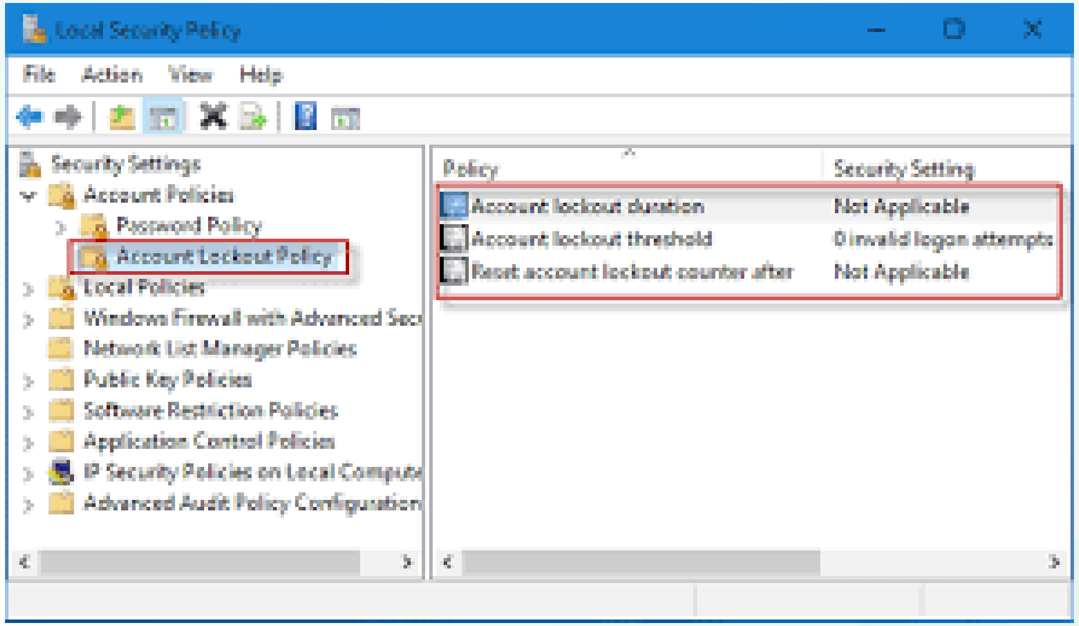
Account Policy Enforcement

Account Policy enforcement comes into play because all users have the right level of access and account type to meet their business function does not mean an organization is as secure as it could be.



CREDENTIAL MANAGEMENT is an overall service that stores, manages, and often audits logins of user credentials in a central location, offered to both individuals and enterprise networks.

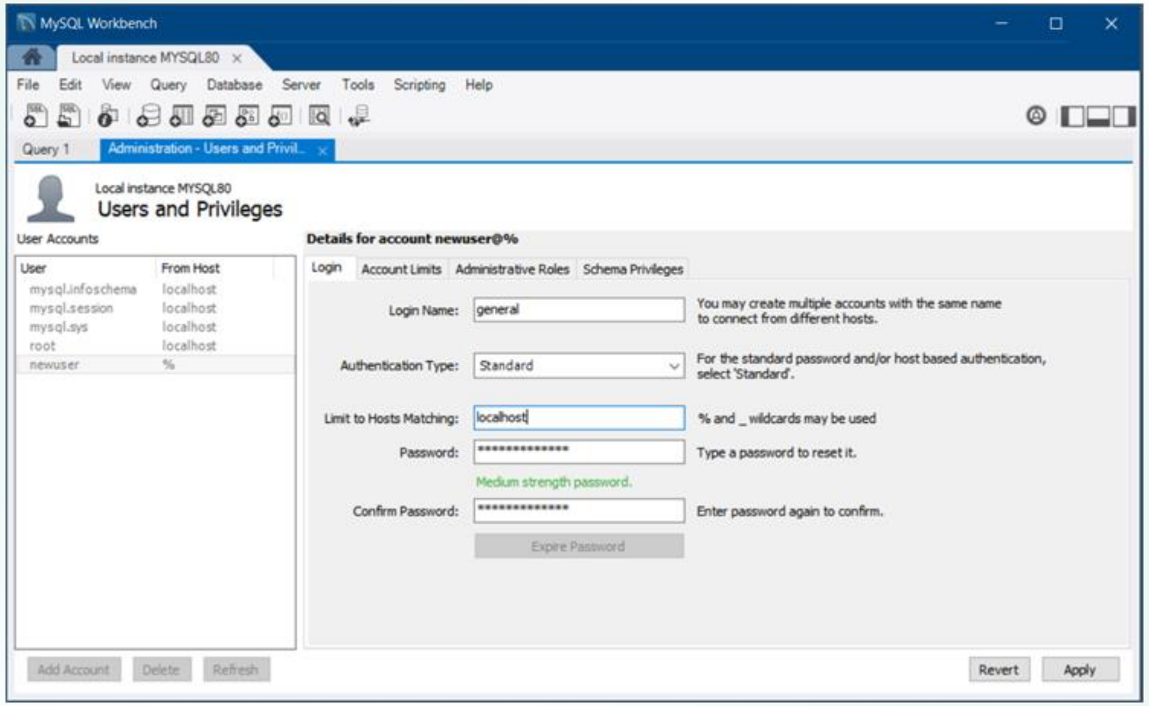
ACCOUNT LOCKOUT is another policy that automatically disables an account when a certain threshold of incorrect passwords are used to log in, requiring a user to recover access to their account with a new password or by satisfying other requirements, such as security questions.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Sec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

Account Privileges

A **PRIVILEGED ACCOUNT** is a user account that has more privileges than ordinary users.



Local instance MYSQL80

Users and Privileges

User Accounts

User	From Host
mysql.infoschema	localhost
mysql.session	localhost
mysql.sys	localhost
root	localhost
newuser	%

Details for account newuser@%

Login Name: general — You may create multiple accounts with the same name to connect from different hosts.

Authentication Type: Standard — For the standard password and/or host based authentication, select 'Standard'.

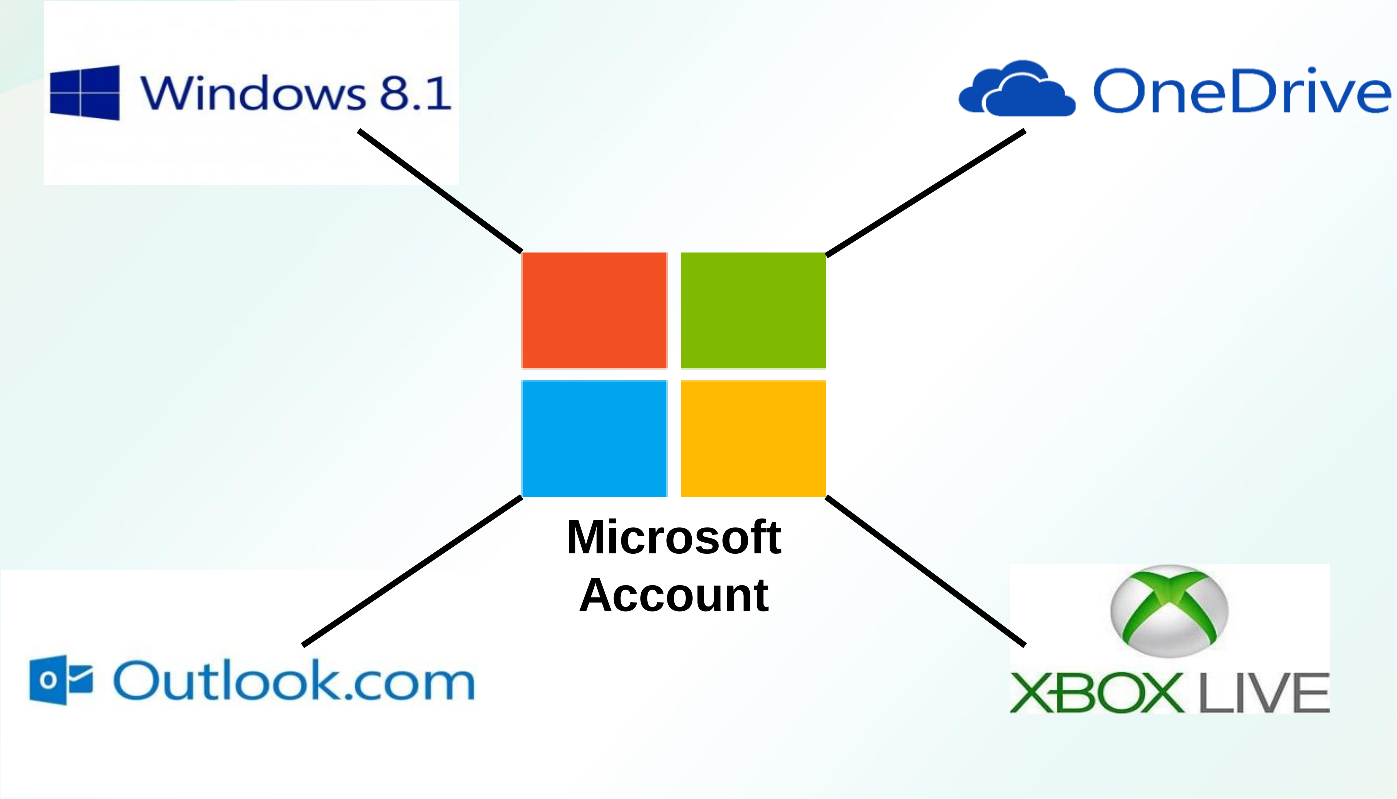
Limit to Hosts Matching: localhost — % and _ wildcards may be used

Password: ************** — Type a password to reset it.

Medium strength password.

Confirm Password: ************** — Enter password again to confirm.

Account Federation

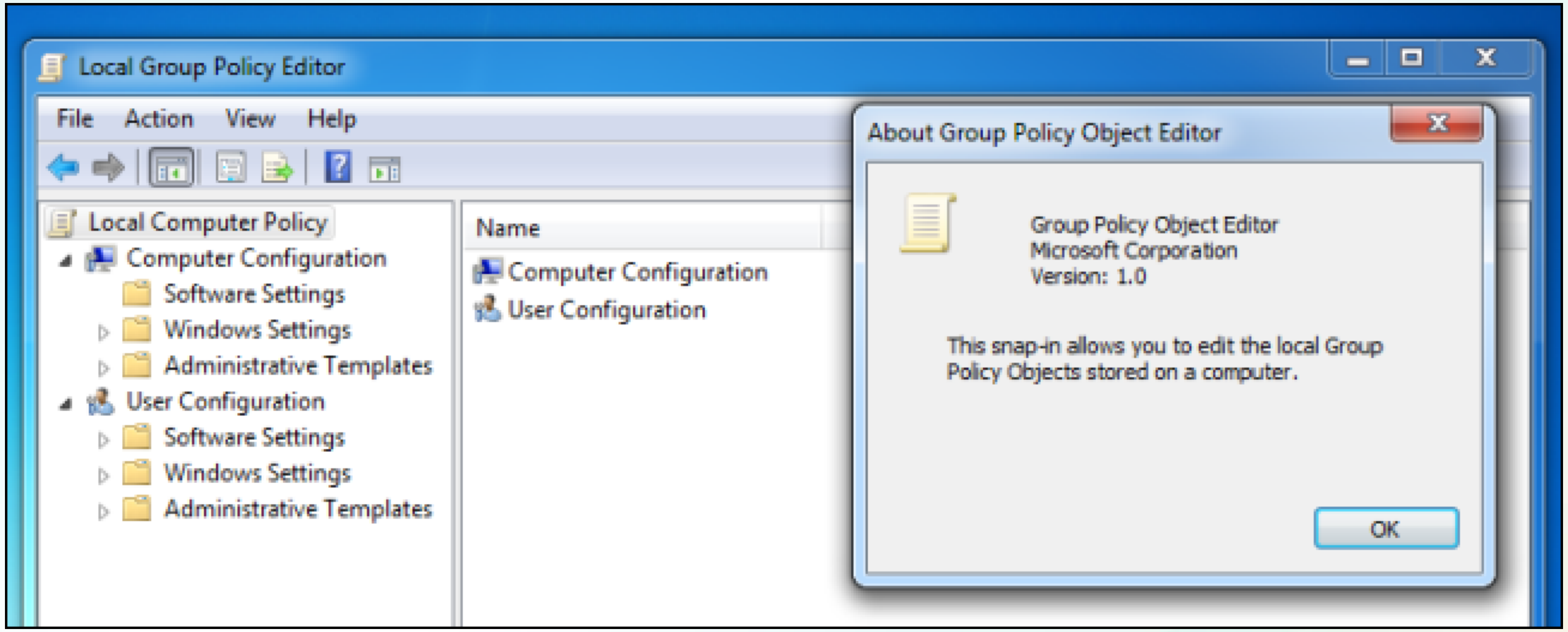


Microsoft
Account

A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.

Group Policy

Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.



Group Policy Object Editor
Microsoft Corporation
Version: 1.0

This snap-in allows you to edit the local Group Policy Objects stored on a computer.

ACCOUNT LOCKOUT

Account lockout keeps the account secure by preventing anyone or anything from guessing the username and password. When your account is locked, you must wait the set amount of time before being able to log into your account again.

PASSWORDS

A password is a string of characters used for authenticating a user on a computer system.

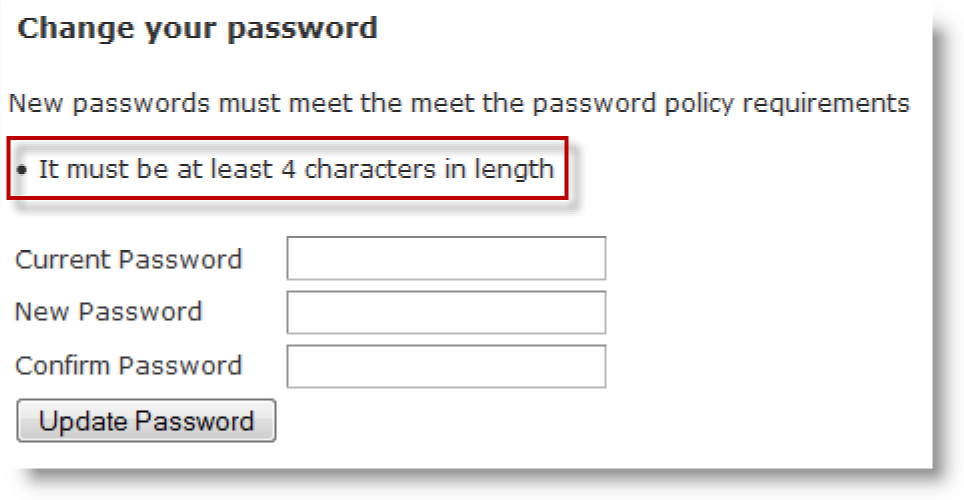
PASSWORD COMPLEXITY

A complex password uses different types of characters in unique ways to increase security. Passwords must meet or exceed these criteria:

- Changed at least every 180 days.
- Between 8 and 128 characters long.
- Use at least 3 of the following types of characters:
  - ✓ uppercase letters,
  - ✓ lowercase letters,
  - ✓ numbers, and/or
  - ✓ special characters
  - ✓ Password must be unique and cannot be re-used.

Password Length

The length of a password is a key component of ensuring the strength of a password. Password length is the number of characters used in a password. A password with 2 characters is considered very insecure, because there is a very limited set of unique passwords that can be made using 2 characters. A 2-character password is considered trivial to guess.



Change your password

New passwords must meet the meet the password policy requirements

- It must be at least 4 characters in length

Current Password

New Password

Confirm Password

Password complexity deals with the characters used to make up the password. A complex password will use characters from at least three of the following categories:

- ✓English uppercase characters (A through Z)
- ✓English lowercase characters (a through z)
- ✓Numeric characters (0 through 9)
- ✓Non-alphanumeric characters (such as !, @, #, $, %, ^, &)

Microsoft provides several controls that can be used to ensure the security associated with passwords is maintained. These include:

Password complexity

Account lockout

Password history

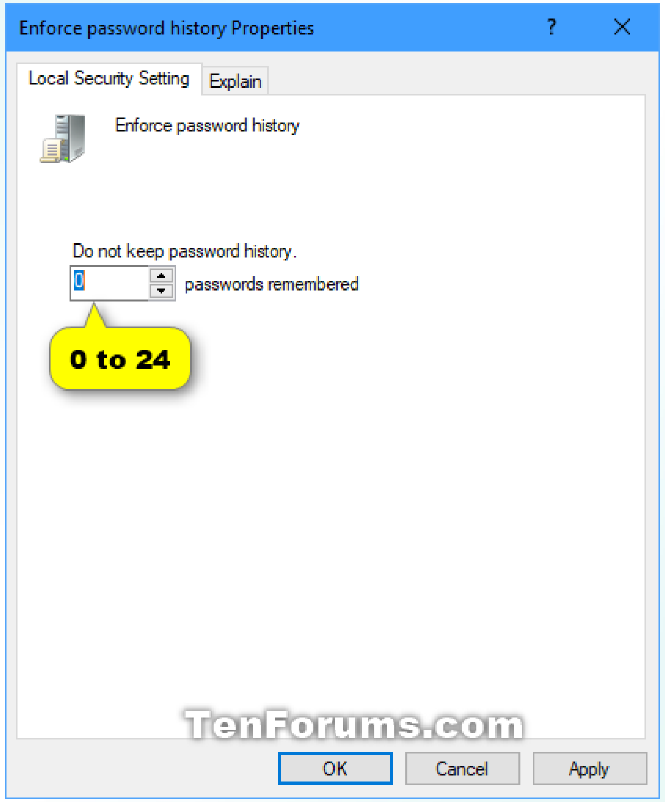
Time between password changes

Group Policies that enforce password security

Education on common attack methods

PASSWORD HISTORY

Password history policy setting determines the number of unique new passwords that must be associated with a user account before an old password can be reused.



Enforce password history Properties

Local Security Setting | Explain

Enforce password history

Do not keep password history.

0 passwords remembered

0 to 24

Account lockout refers to the number of incorrect logon attempts permitted before the system will lock the account.

❑ **Account lockout duration**: This setting determines the length of time a lockout will remain in place before another logon attempt can be made

❑ **Account lockout threshold**: This setting determines the number of failed logons permitted before the account lockout occurs.

❑ **Reset account lockout counter after**: This setting determines the period of time, in minutes, that must elapse before the account lockout counter is reset to 0 bad logon attempts.

Setting Time Between Password Changes

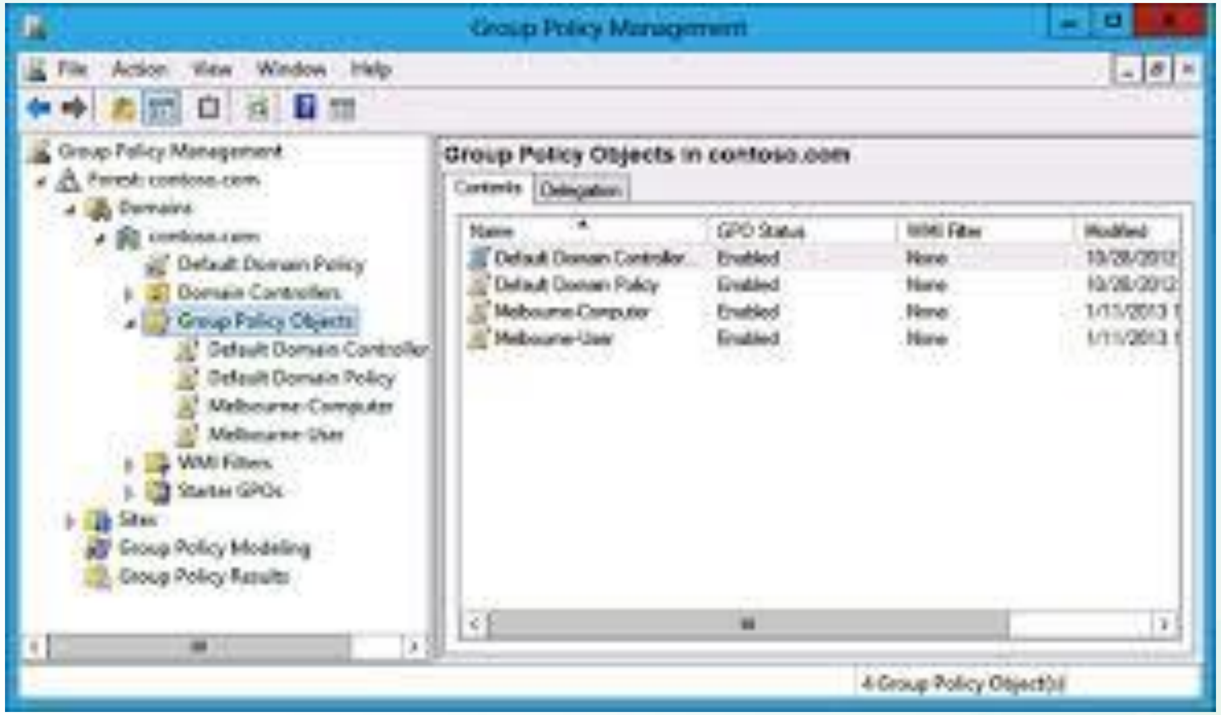
Minimum Password Age: The minimum password age setting controls how many days a user must wait before they can reset their password. This can be set to a value from 1 to 998 days.

Maximum Password Age: The maximum password age setting controls the maximum period of time permitted before a user is forced to reset their password.

Passwords should always expire, unless under unique circumstances, such as service accounts for running applications.

Group Policies to Enforce Password Security

A ***Group Policy Object (GPO)*** is a set of rules which allow an administrator granular control over the configuration of objects in Active Directory (AD), including user accounts, operating systems, applications, and other AD objects.



Group Policy Objects in contoso.com

Name	GPO Status	WMI Filter	Modified
Default Domain Controller...	Enabled	None	10/28/2012
Default Domain Policy	Enabled	None	10/28/2012
Melbourne-Computer	Enabled	None	1/11/2013
Melbourne-User	Enabled	None	1/11/2013

4 Group Policy Object(s)

INSTALL (CA) / ENROLL CERTIFICATES

SUBTOPIC 3

OBJECTIVES

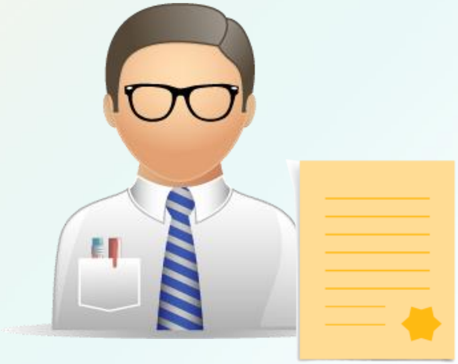
Upon completion of this module, the student would be able to:

- Define the Certificate Authority (CA) and its goals;
- Explain the concepts of certificates;
- Demonstrate the operation of Certificate Authentication;
- Enumerate the types of CA and services provided

Certificate Authority

Certificate Authority (CA) (or Certification Authority) is an entity that issues digital certificates.

Digital Certificates

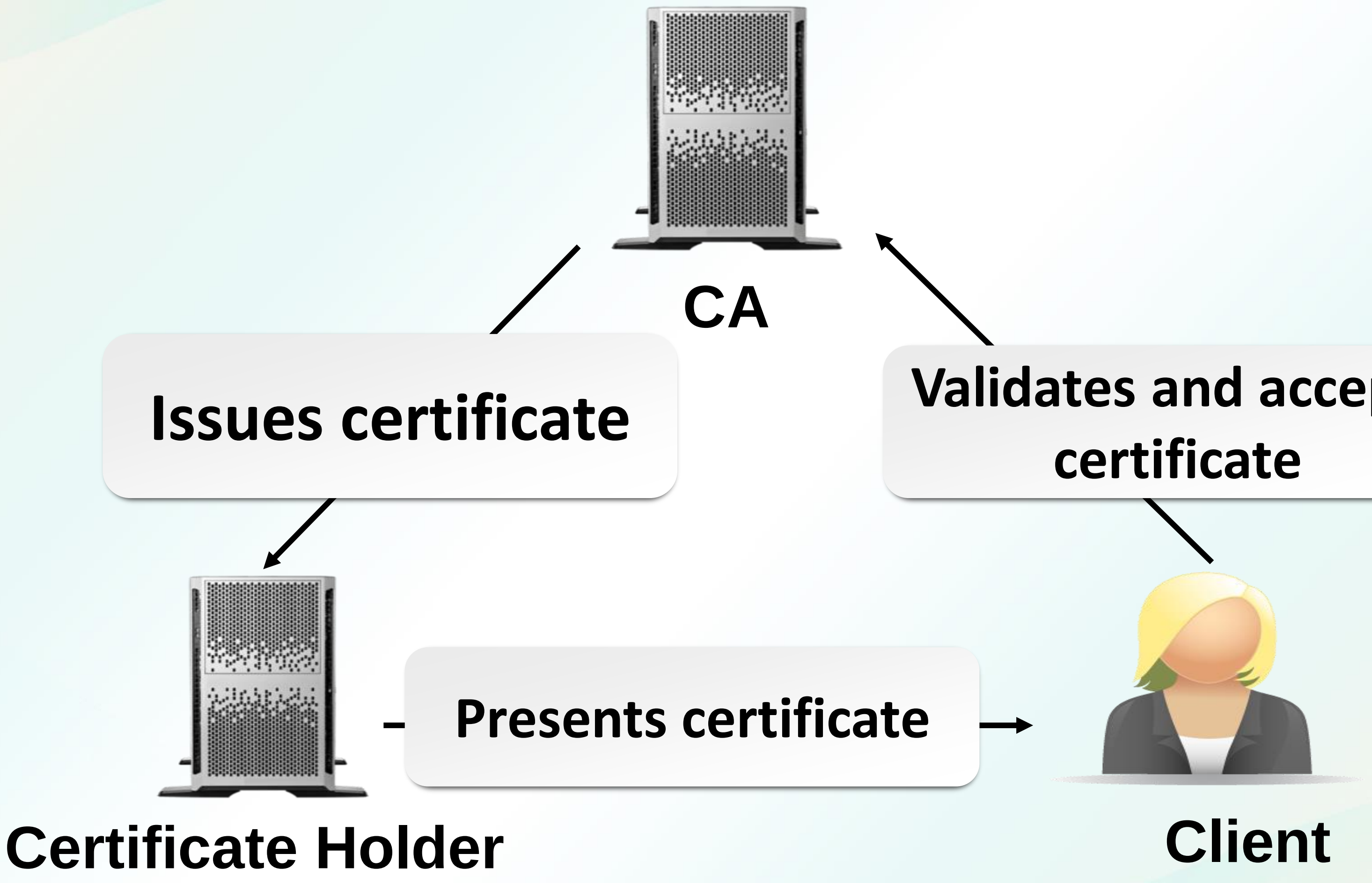


User with Certificate

Device with Certificate

The ***digital certificate*** is an electronic document that contains an identity such as a user or organization and a corresponding public key.

Certificate Authentication



CA

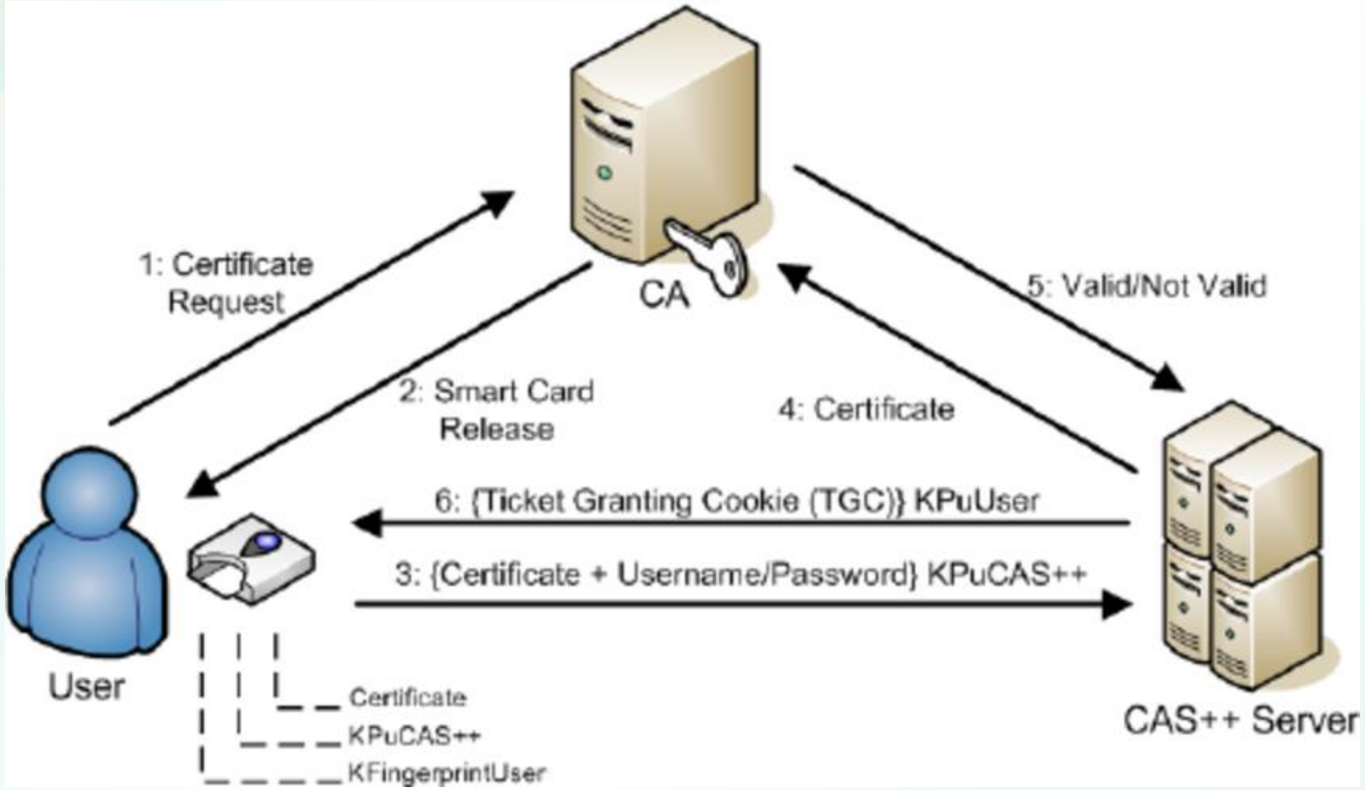
Issues certificate

Validates and accepts certificate

Presents certificate

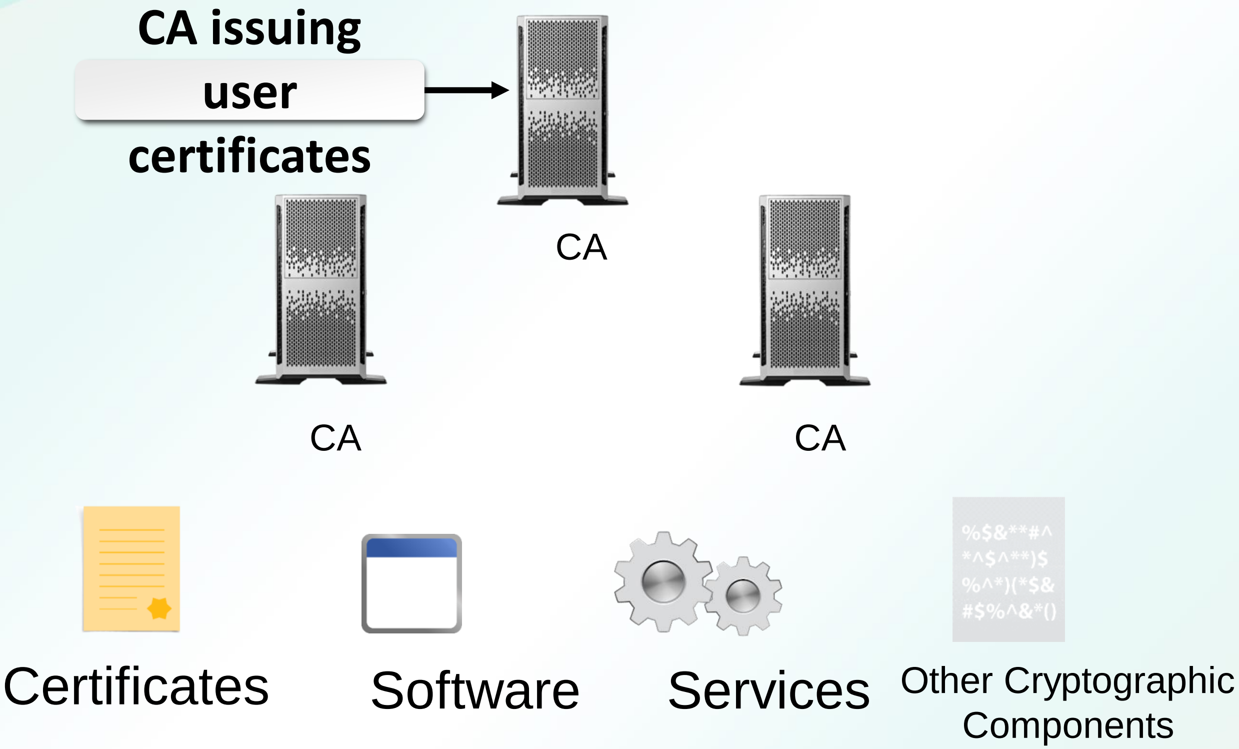
Certificate Holder

Client



Certificate authentication is the use of a Digital Certificate to identify a user, machine, or device before granting access to a resource, network, application, etc.

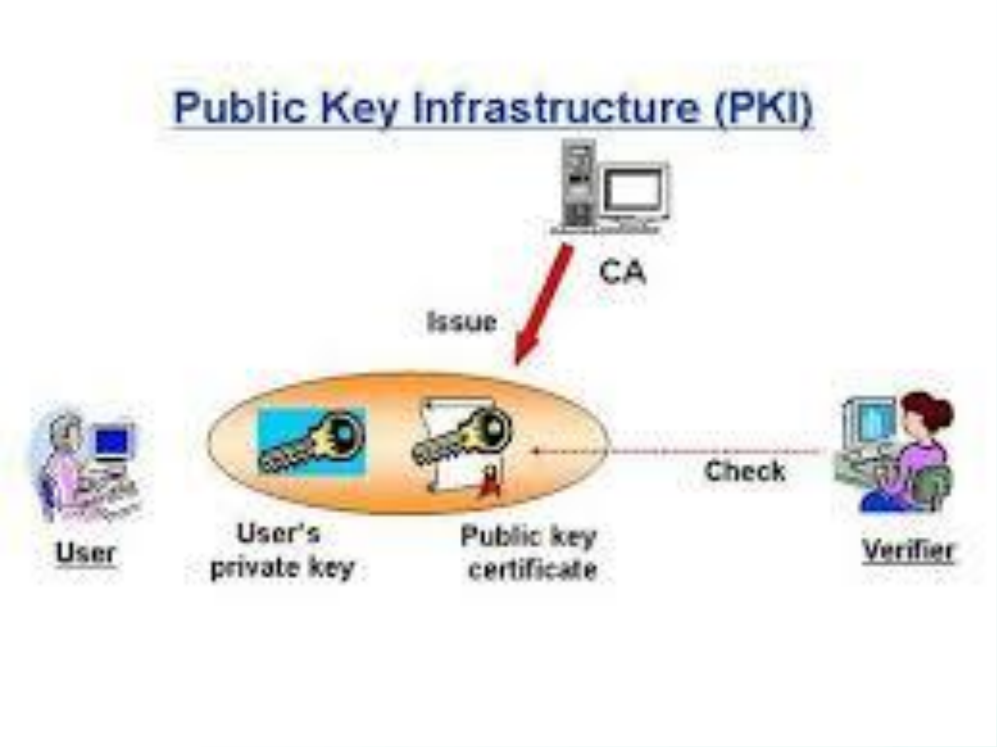
PKI - Public Key Infrastructure



A ***public key infrastructure (PKI)*** is a system consisting of hardware, software, policies, and procedures that create, manage, distribute, use, store, and revoke digital certificates.

Public Key Infrastructure

Public Key Infrastructure (PKI) is that it uses a pair of keys to achieve the underlying security service. The key pair comprises of private key and public key.



Key Management

Key management refers to management of cryptographic keys in a cryptosystem

PKI Components

✓ Public key

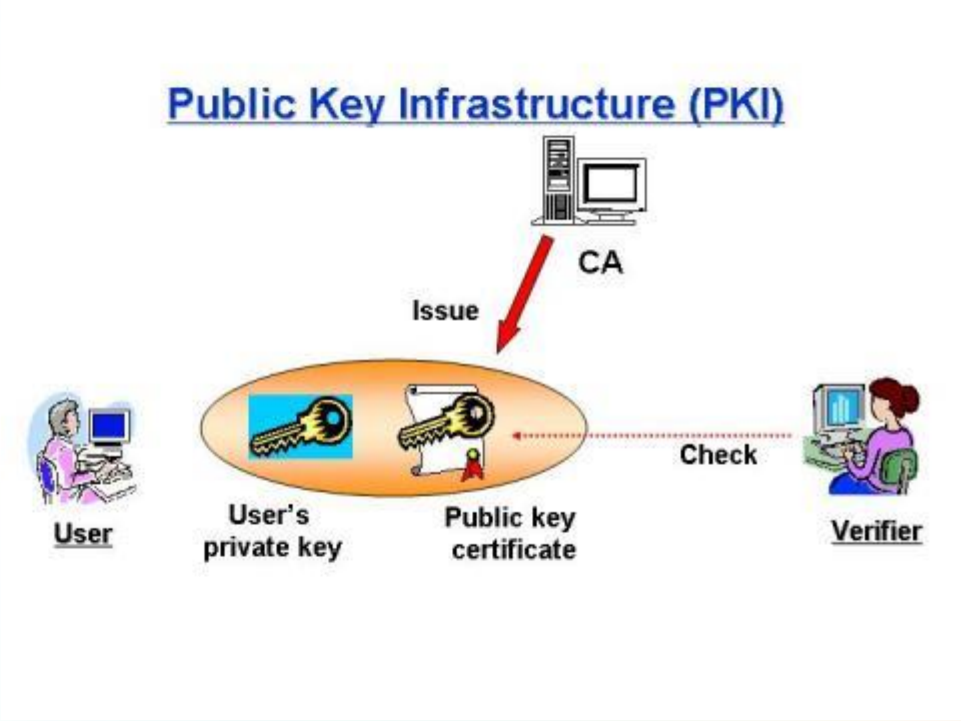
✓ Private key

✓ Certificate Authority

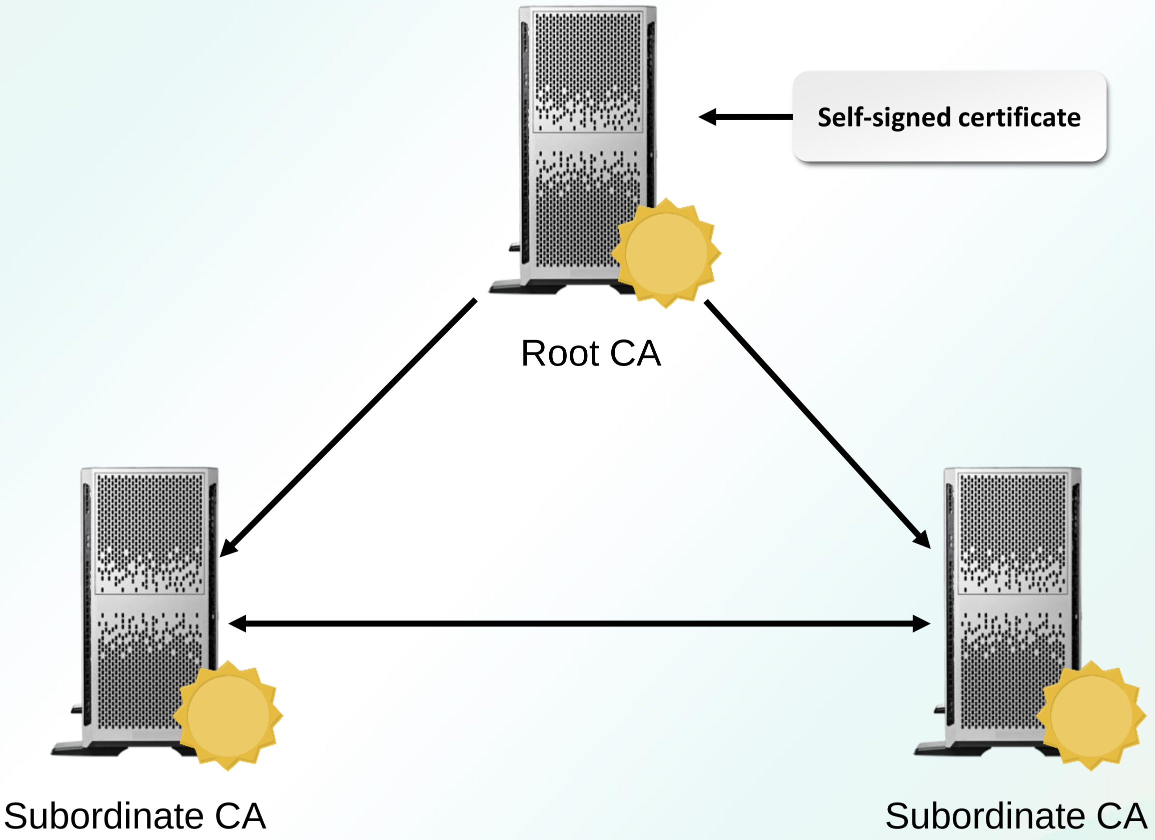
✓ Certificate Store

✓ Certificate Revocation List

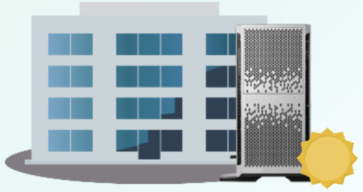
✓ Hardware Security Module



Root CA


Self-signed certificate
Root CA
Subordinate CA
Subordinate CA

Public and Private Roots



Private Root CA

Public Root CA

When to use Public CAs?
When we provide services for the general public, we use certificates signed by a “trusted” third-party.

When to use a Private CAs?
The situation changes completely when private services are provided, which are not for the general public.

Offline Root CAs

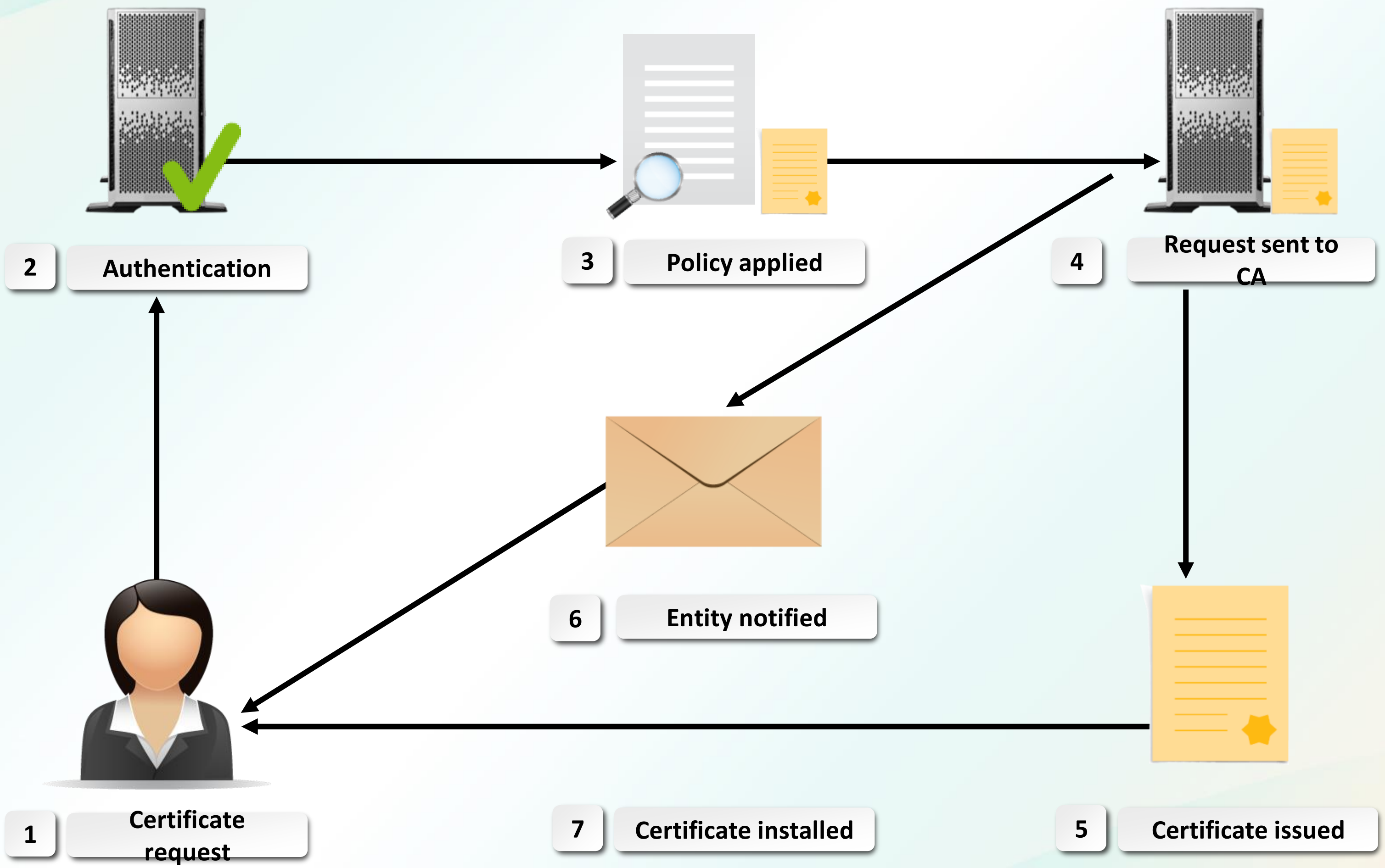
❑The root CA remains offline.

❑Subordinate CAs will issue certificates.

❑All updates are made only to subordinate CAs.

Offline root CAs can issue certificates to removable media devices (USB drive, CD/DVD) and then physically transported to the subordinate CAs that need the certificate in order to perform their tasks.

Certificate Enrollment Process



1 Certificate request

2 Authentication

3 Policy applied

4 Request sent to CA

5 Certificate issued

6 Entity notified

7 Certificate installed

REFERENCES

- CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide Paperback – October 12, 2017 by Darril Gibson

- CompTIA Security+ SY0-501 Cert Guide (4th Edition) (Certification Guide), David L. Prowse (2018)

- CompTIA Security+ Study Guide: Exam SY0-501 7th Edition by Emmett Dulaney (Author), Chuck Easttom (Author)