BITS Pilani

Module 9 Part 3

Security Technology & Tools

Harvinder S Jabbal
SSZG653 Software Architectures

Contents

- Transport Layer Security (TLS)
- OpenID & OpenAuth
- LDAP
- Identity & Access management
- Firewalls

Introduction

The objective of this session is to provide an introduction to a few important technology topics.

Transport layer security (TLS)

(Older version is SSL)

- Used for secure communication between **client & server** (example between browser and a web site)

- It provides

  - **Privacy:** No intruder can know what communication is going on
  - **Data integrity:** Data being communicated can not be modified by an intruder. If he does, it can be detected

TLS: How does it work?

Client & server do the following:

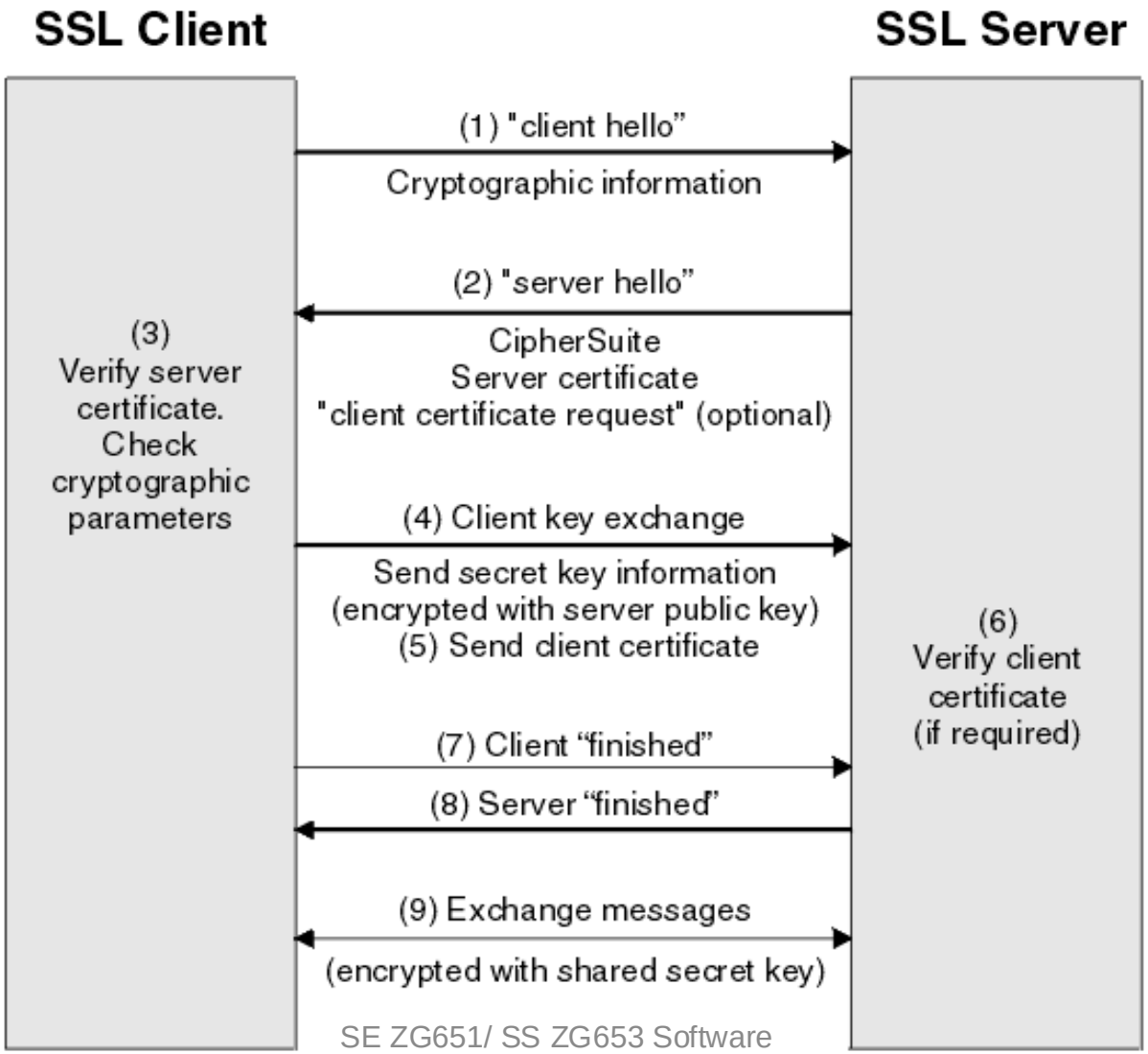
- Agree on the version of the TLS protocol to use.
- Select cryptographic algorithms to use
- Authenticate each other by validating digital certificates.
- Generate a shared secret key, for the symmetric encryption of messages (This is faster than asymmetric encryption)

Source: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm

Encryption algorithms used

- Key Exchange Algorithms (RSA, DH, ECDH, DHE, ECDHE, PSK)
- Authentication/Digital Signature Algorithm (RSA, ECDSA, DSA)
- Bulk Encryption Algorithms (AES, CHACHA20, Camellia, ARIA)
- Message Authentication Code Algorithms (SHA-256, POLY1305)

TLS / SSL steps

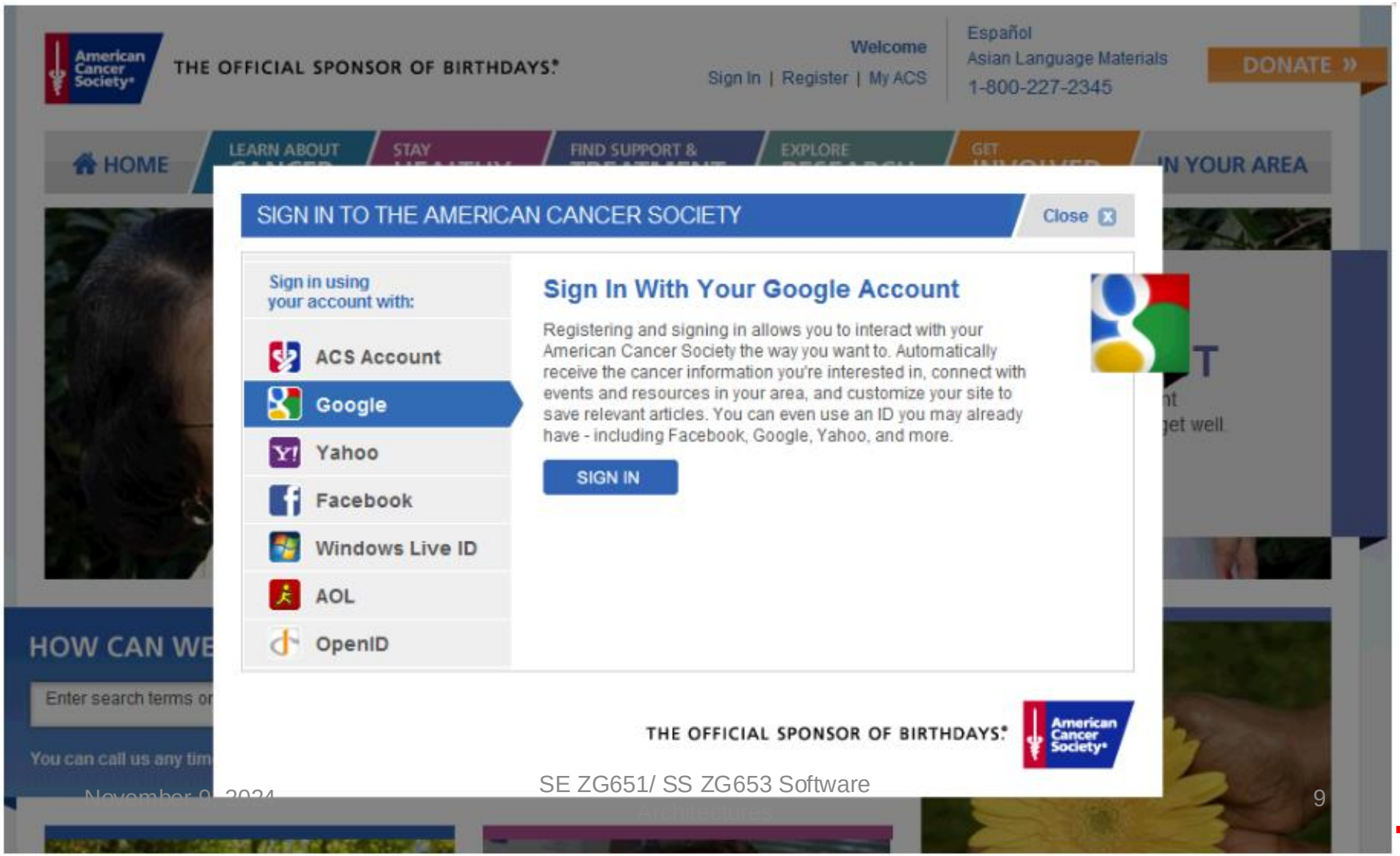


Source: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm

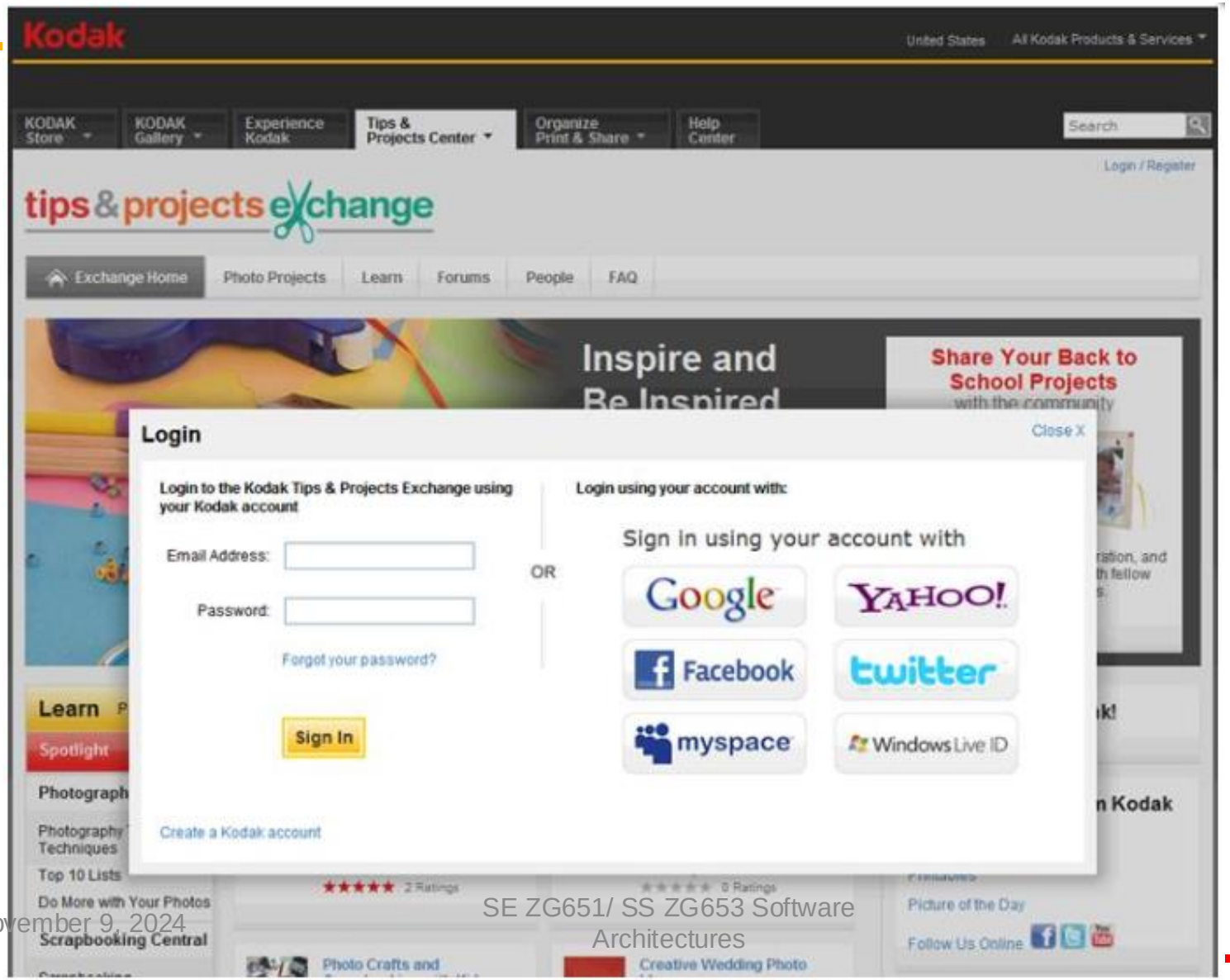
OpenID

- We use several websites.
- One issue we face is, remembering user ids & passwords of several websites
- With OpenID technology, we can use a single account, such as Facebook, Google or Yahoo, to sign-in to thousands of websites

Sample login page: American Cancer Society



Sample login page: Kodak Tips and project Exchange



OpenID: How does it work?

(One typical approach)

- The website redirects the user to an OpenId provider such as Facebook or Google
- The OpenID provider authenticates the user
- The user is redirected back to the website along with the end-user's credentials (such as user id, but not the password)

Reference: https://en.wikipedia.org/wiki/OpenID

OAuth

OpenID is to authenticate users.

OAuth authorizes a client to access your data stored in another website such as Yahoo (data such as your profile, contacts in Yahoo)

Reference: https://tools.ietf.org/html/draft-ietf-oauth-use-cases-01#section-2.1

OAuth: Use cases

Use case 1:

- An application can *use OAuth* to obtain permission from users to store files in their Google Drives.

Use case 2

- A photo printing application (www.printphotos.example.com) can access your photographs stored on a server www.storephotos.example.com and then print them

Reference: https://tools.ietf.org/html/draft-ietf-oauth-use-cases-01#section-2.1

OAuth: How does it work?

- You try to log onto a website and it offers opportunities to log on using Google, Yahoo, etc. Let us say you choose Google.
- You are redirected to Google
- Google authenticates you, and returns a token to the website.
- The token enables the website to login to Google as you, and access resources such as your contacts.

https://www.csoonline.com/article/3216404/what-is-oauth-how-the-open-authorization-framework-works.html

LDAP: Lightweight Directory Access Protocol

Scenario suitable for LDAP

- Imagine you have a website that has a million registered users with thousands of page requests per second.
- By using LDAP, you can easily offload the user validation and gain significant performance improvement.
- Good use cases for LDAP:
  - You need to locate ONE piece of data many times and you want it fast
  - You don’t update, add, or delete the data very often
  - The size of each data entry is small

https://stackoverflow.com/questions/239385/what-is-ldap-used-for

LDAP

- LDAP is an Internet protocol to talk to a Directory service such as Active Directory of Microsoft
- Directory services store information in a tree structure
- LDAP is used in many open source solutions such as Docker, Kubernetes, Jenkins, etc.

Identity & Access management

- Identity and access management (IAM), is a framework for ensuring that **people in an enterprise have the appropriate access** to technology resources.

- IAM solutions are typically used in large organizations to ensure regulatory compliance.

- **Features of IAM**
  - Authentication of a user
  - Authorization to use applications
  - Definition of Roles. A User belonging to a group is authorized to perform certain operations defined for the role. Operations such as create sales order, approve credit card request, etc.
  - Delegation of permission to another user
  - Interchange identify information with trusted entities using OpenID, etc.

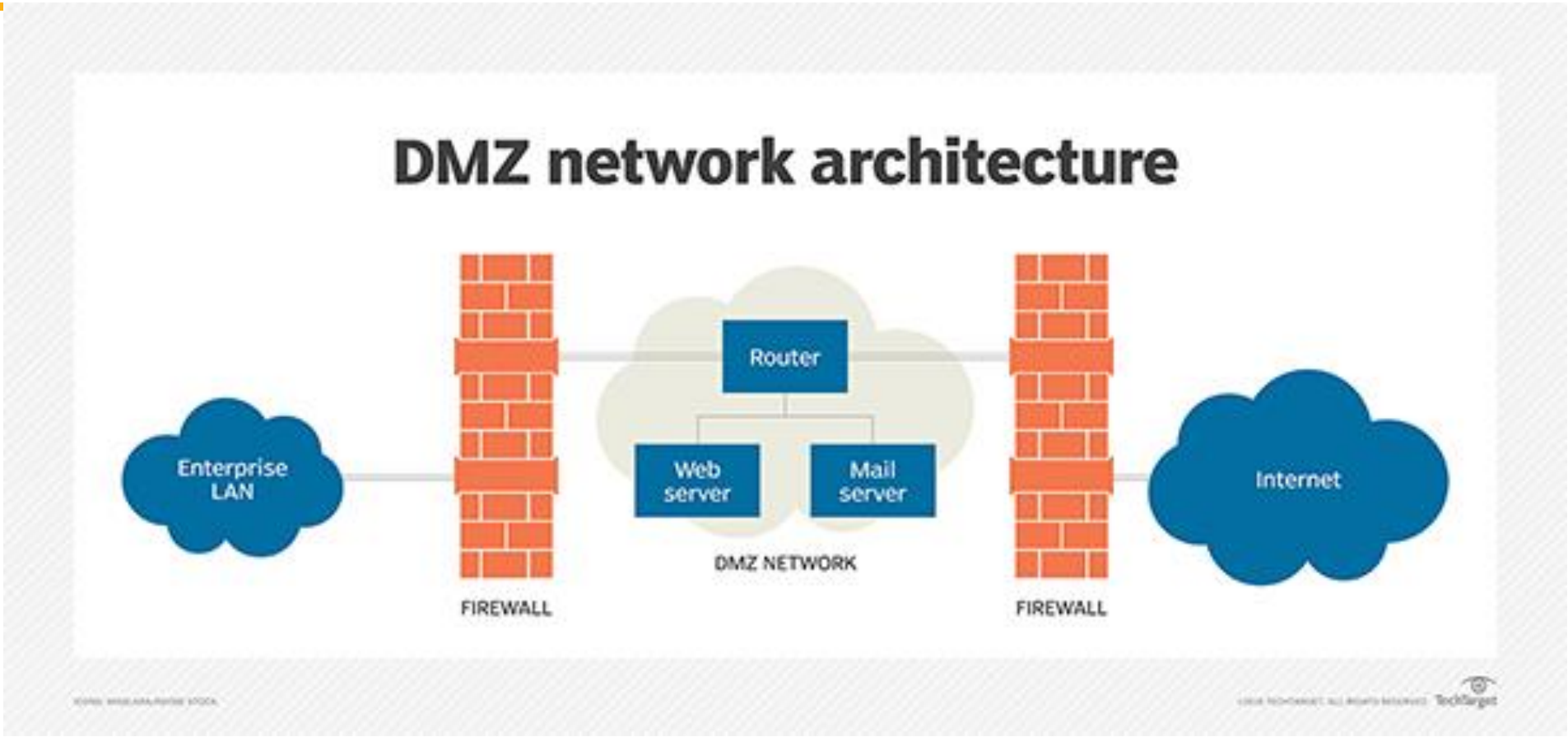
Leading Identity & Access management products

- Azure Active Directory
- IBM Security Identity and Access Assurance
- Oracle Identity Cloud Service
- Okta

Firewall

- A firewall is a network security device that **monitors incoming and outgoing network traffic** and decides whether to **allow or block** specific traffic based on a defined set of **security rules.**

De-Militarized Zones (DMZ)



DMZ acts a buffer between Internet and organization network

https://searchsecurity.techtarget.com/definition/DMZ

How DMZs work?

- DMZs are intended to function as a sort of **buffer zone between the public internet and the organizational network.**

- If a better-prepared threat actor is able to get through the first firewall, they must then gain unauthorized access to those services before they can do any damage

Some Firewall features

- Intrusion detection: Identify & block security threats such as malware, spyware, etc.
- Grant access to users based on business need
- Fingerprint applications and track their usage: # users, bandwidth usage
- Allocate bandwidth to applications (ex. Allocate more BW to SalesForce.com and less to YouTube)

https://www.cio.com.au/article/365101/top_seven_firewall_capabilities_effective_application_control/

https://www.fortinet.com/products/next-generation-firewall.html#services

https://www.securedgenetworks.com/blog/11-Features-to-Look-for-in-Your-Next-Generation-Firewall

Firewall techniques

Techniques used:

1. Packet filtering: Looks at IP address and Port # and drops packets coming from or destined to certain IP addresses

2. Circuit level gateways: Detect conversations by looking at end-point pairs

3. Application layer filtering: Detects applications trying to use disallowed protocols or ports

4. Hide addresses and perform network address translation.
   - Hacker can not know the IP address of the server that receives the message. Even if it knows, the firewall will block it.

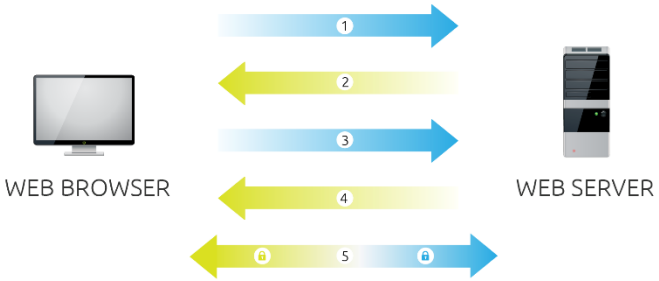
Business Process Management

Business Process Management Tools: **Business Process Management** (**BPM**) **tools** are used for automating, measuring and optimizing business processes.

BPM tools use workflow and collaboration to provide meaningful metrics to business leaders

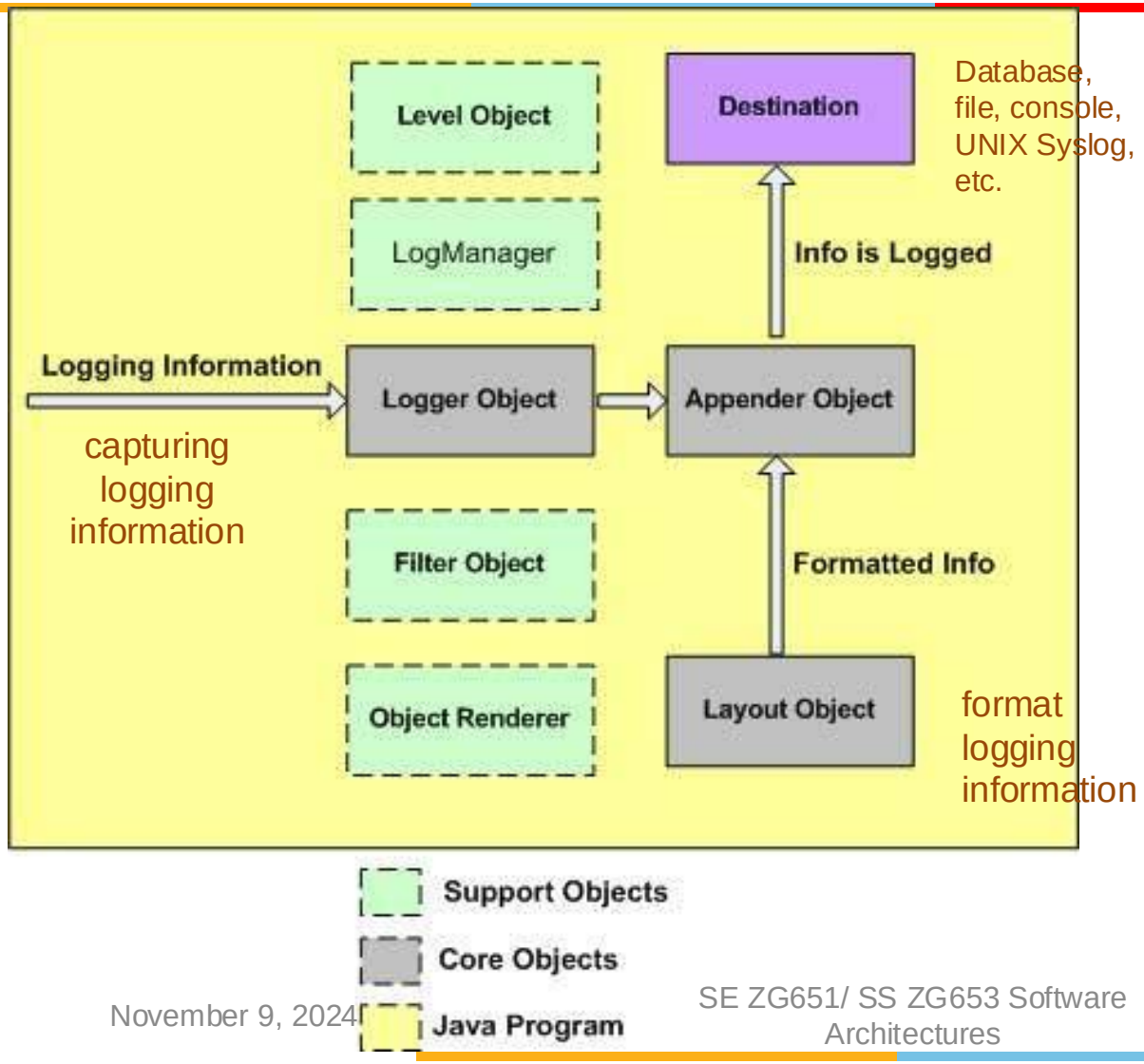
Example: Appian, Zoho

SSL



1. Browser connects to a web server (website) secured with SSL (https). Browser requests that the server identify itself.
2. Server sends a copy of its SSL Certificate, including the server's public key.
3. Browser checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.
4. Server decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.
5. Server and Browser now encrypt all transmitted data with the session key.

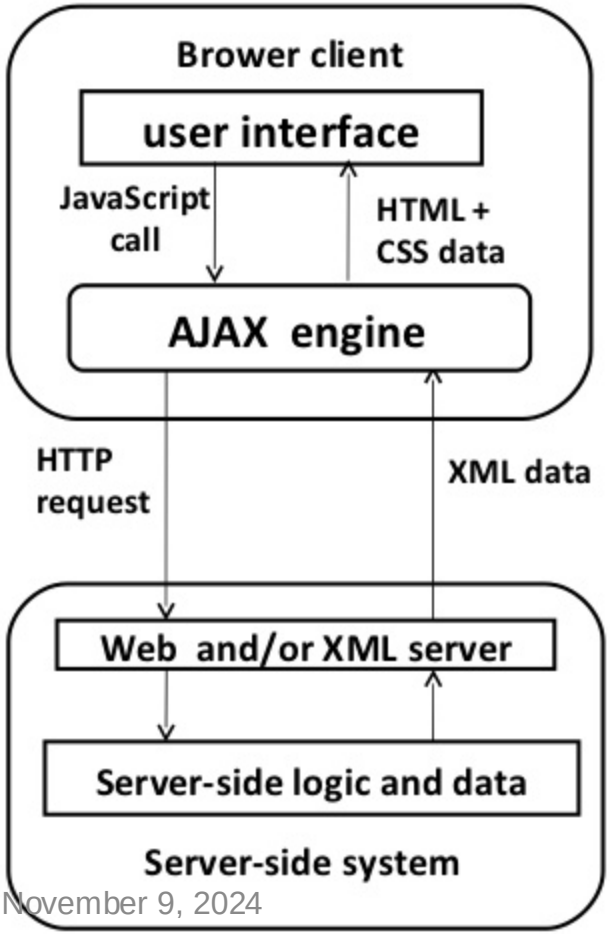
Logging: Apache Log4j



- Logging is an important component of the software development.
- A well-written logging code offers quick debugging, easy maintenance, and structured storage of an application's runtime information.
- Logging does have its drawbacks also. It can slow down an application.

Asynchronous operation

AJAX Architecture



AJAX stands for **A**synchronous **Ja**vaScript and **X**ML.

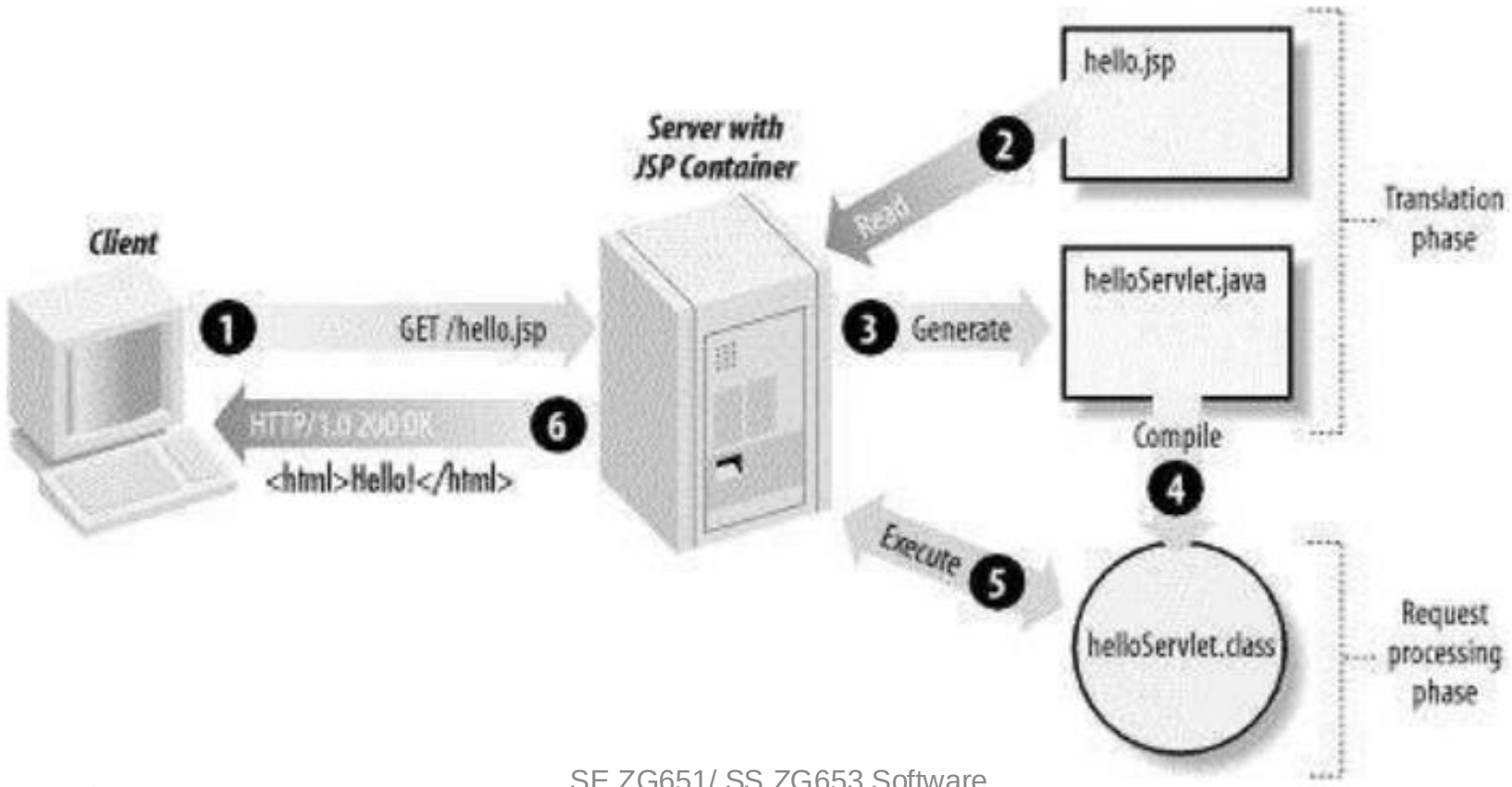
AJAX is a new technique for creating better, faster, and more interactive web applications with the help of XML, HTML, CSS, and Java Script.

Some famous web applications that use AJAX:

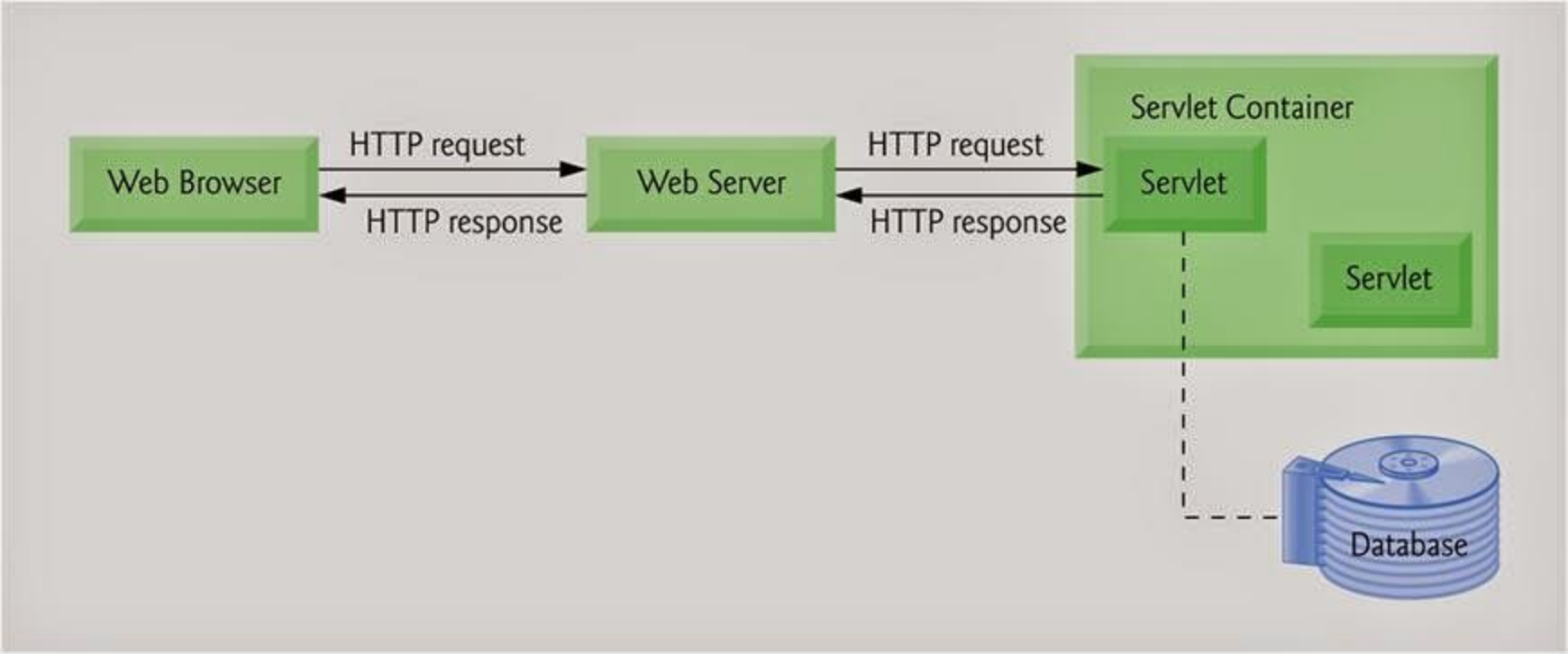
Google Maps (Drag entire map)
Google Suggest (Google suggests as you type)

Simple Web application architecture

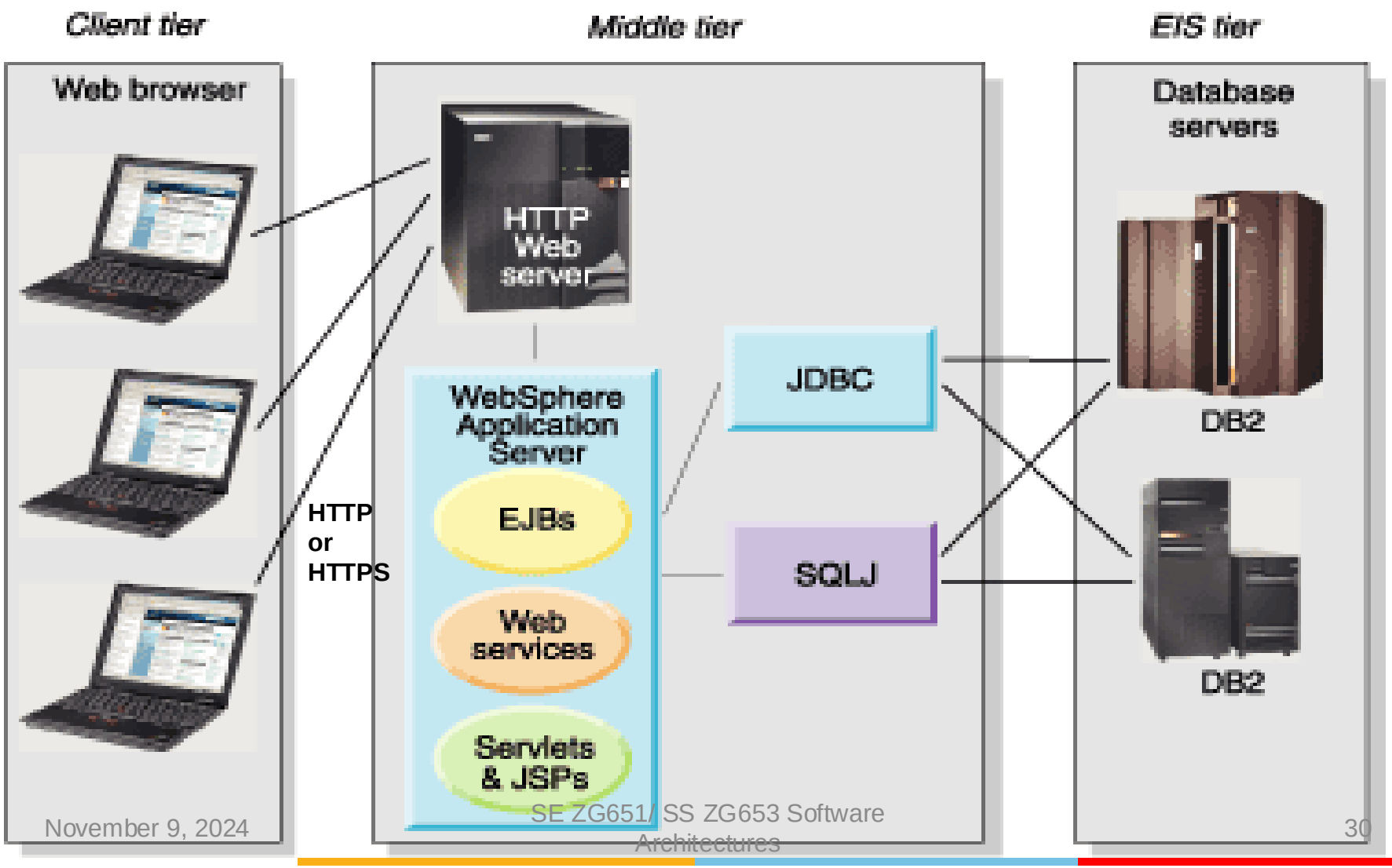
Dynamic web pages – using JSP and Servlet



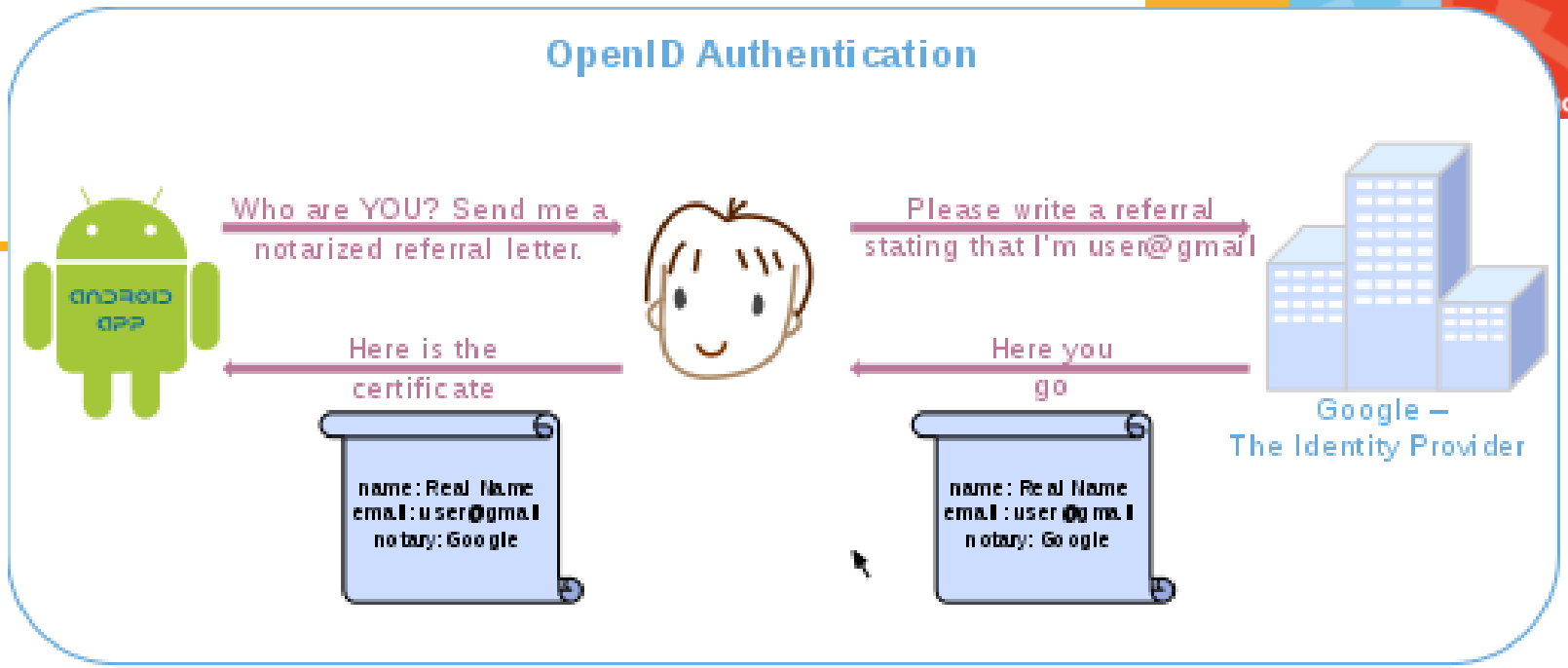
Dynamic web pages



Web application architecture



Source: Wikipedia



vs.