Protocols d'Internet

Preguntes Topic 2

Pregunta 1. Explica los conceptos de servicio, arquitectura orientada a objetos y sistema distribuido.

Servei: Un mecanisme que permet l'accés a una o més capacitats, en els quals es presta l'accés mitjançant una interfície prescrita i es manifesta l'exercici consistent amb les restriccions i polítiques com s'especifica en la descripció del servei.

Arquitectura Orientada a Objectes: Un paradigma per organitzar i utilitzar capacitats distribuïdes que poden estar sota el control de diferents dominis de propietat. Proporciona una manera unificada d'oferir, descobrir, interactuar amb capacitats d'ús per produir els efectes desitjats en consonància amb les condicions prèvies i expectatives mesurables.

Sistema Distribuit: Consta de diversos agents de programari que han de treballar junts per realitzar algunes tasques. Els agents en un sistema distribuït no operen en el mateix entorn de processament, per la qual cosa han de comunicar per piles de protocols (maquinari o programari) en una xarxa. SOA és un tipus de sistema distribuït.

Pregunta 2. Explica brevemente el rol del protocolo WSDL (Web Services Description Language) en un servicio Web y como se estructura un servicio web con WSDL.

Llenguatge basat en XML que proporciona un model per a la descripció dels serveis que ofereix un web i la seva localització i els paràmetres i mètodes que suporta. Un programa client que es connecta a un servei web pot llegir el fitxer WSDL per determinar quines operacions estan disponibles en el servidor. El client pot utilitzar SOAP per cridar una de les operacions enumerades en l'arxiu WSDL utilitzant XML o HTTP.

Un servei web amb WSDL s'estructura amb un document WSDL per a cada servei. S'utilitza, com s'ha dit, XML i en ell es defineixen els elements: portType, message, types, binding, port i service.

Pregunta 3. Explica el rol de SOAP (Simple Object Access Protocol) en un servicio Web y describe el tipo de encapsulamiento que usa. ¿Qué diferencias hay entre un Web Service basado en JSON y XML?

SOAP és un protocol per a l'intercanvi d'informació estructurada entre el client i els servidor Web Services. El missatge és escrit en llenguatge XML i utilitza protocols d'aplicació com HTTP, SMTP o XML-RPC.

Les diferències entre un Web Service basat en JSON i XML és que el primer permet rebre notificacions (informació enviades al servidor que no requereixen una resposta) i fer múltiples crides al servidor que pot respondre fora d'ordre. A més, JASON no és tan complexe com XML (sobretot si no es necessiten *namespaces*). JSON, a diferència també de XML no és extensible, ja que no és un llenguatge de marcat de documents, pel que no és necessari definir noves etiquetes o atributs per a representar dades en elles.

Amb tot, JSON i XML tenien proposits diferents. XML és una manera d'estructurar dades mentre que JSON és una manera d'intercanviar dades a través d'un llenguatge que hauria de ser senzill (per exemple Javascript). En general, de fet, la majoria del que JSON pot fer XML també.

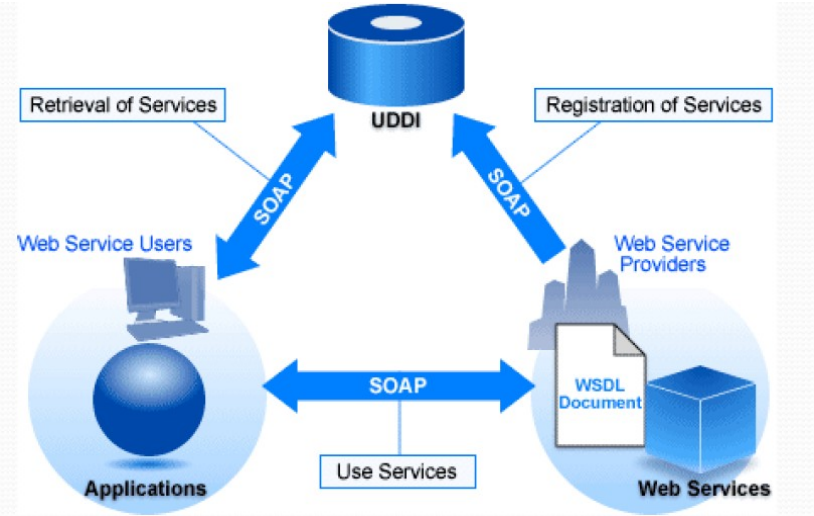
Pregunta 4. Explica qué diferencias hay en usar RPC, RPC-XML y SOAP.

RPC (Remote Call Procedure): Permet la invocació d'una funció a través d'una xarxa. Una RPC és iniciada pel client, que envia un missatge de sol·licitud a un servidor remot conegut per executar un procediment

especificat amb paràmetres proporcionats. El servidor remot envia una resposta al client, i l'aplicació continua el seu procés.
RPC-XML: Un RPC que utilitza XML per serialitzar els paràmetres. Utilitza HTTP com a protocol de transport. Defineix pocs formats de dades: booleà, enter, doble, cadena, data / hora, base 64 (per dades binàries), estructura i matriu. No utilitza l'esquema XML i per tant no suporta la validació automàtica. No té en compte la denominació i les capacitats de descobriment.

SOAP és un protocol per a l'intercanvi d'informació estructurada entre el client i els servidor Web Services. El missatge és escrit en llenguatge XML i utilitza protocols d'aplicació com HTTP, SMTP o XML-RPC.

Pregunta 5. Dibuja un esquema que defina la arquitectura de referencia de los Web Services y explica su funcionamiento básico.



Service Requester: Sol·licita l'execució d'un servei web.
Service Provider: Processa una sol·licitud de servei web.
Discovery Agency: Agència a través de la qual la descripció del servei web és publicada i es pot trobar (UDDI).

Pregunta 6. Explica que diferencias hay entre usar una arquitectura basada en XML o en JSON.

Les diferències entre un Web Service basat en JSON i XML és que el primer permet rebre notificacions (informació enviades al servidor que no requereixen una resposta) i fer múltiples crides al servidor que pot respondre fora d'ordre. A més, JASON no és tan complexe com XML (sobretot si no es necessiten *namespaces*). JSON, a diferència també de XML no és extensible, ja que no és un llenguatge de marcat de documents, pel que no és necessari definir noves etiquetes o atributs per a representar dades en elles.

Amb tot, JSON i XML tenien proposits diferents. XML és una manera d'estructurar dades mentre que JSON és una manera d'intercanviar dades a través d'un llenguatge que hauria de ser senzill (per exemple Javascript). En general, de fet, la majoria del que JSON pot fer XML també.

Pregunta 7. Explica el funcionamiento básico de la criptografía de llave simétrica y como se asegura el intercambio de la llave.

La criptografia de clau simètrica parteix de la base que emissor i receptor comparteixen una clau privada que és necessària per encriptar i desencriptar missatges. Aquesta clau pot servir per encriptar el missatge a través d'un algorisme com DES o AES.

En aquest sentit, un handicap és compartir la clau a través d'un mitjà segur. Per això sorgeix la figura del KDC (Key Distribution Centre) que assegura a les dues parts la coneixença fiable de la clau.

Pregunta 8. Explica el funcionamiento básico de la criptografía de llave pública. Explica en un ejemplo como podemos firmar un documento y a continuación encriptarlo.

El funcionament de la clau pública o criptografia asimètrica parteix de la base que un emissor d'un missatge té una clau privada amb la qual encripta un missatge, i una clau pública, que pot obtenir qualsevol persona i que servirà per desencriptar un missatge.

Per firmar un document cal fer una combinació de les claus d'emissor i receptor, clau pública i privada. Si Alice envia un missatge a Bob, cal primer que Alice encripti el missatge amb la clau pública de Bob, de manera que només ell el podrà llegir. Si ara el vol signar, cal que aquest missatge sigui encriptat de nou amb la clau privada de Alice. Així Bob, si vol verificar que el missatge és de Alice, el podrà desencriptar amb la seva clau pública i després aplicar-hi la seva pròpia clau privada.

Pregunta 9. Explica cómo se puede firmar digitalmente con criptografía de llave pública.

Per firmar un document cal fer una combinació de les claus d'emissor i receptor, clau pública i privada. Si Alice envia un missatge a Bob, cal primer que Alice encripti el missatge amb la clau pública de Bob, de manera que només ell el podrà llegir. Si ara el vol signar, cal que aquest missatge sigui encriptat de nou amb la clau privada de Alice. Així Bob, si vol verificar que el missatge és de Alice, el podrà desencriptar amb la seva clau pública i després aplicar-hi la seva pròpia clau privada.

Pregunta 10. Explica mediante un ejemplo como funciona un KDC (Key Distribution Center) en la criptografía simétrica.

Alice es comunica amb el KDC amb la clau simètrica que tenen per a tal fi Alice-KDC.
El KDC li retorna un missatge encriptat Alice-KDC. Aquí dins hi ha un altre missatge encriptat amb la clau KDC-Bob i que només Bob podrà obrir on hi conté la clau Alice-Bob.
Alice envia aquest missatge a Bob per a que el desencripti i podrà obtenir la clau Alice-Bob.

Pregunta 11. Explica para qué sirve y cuál es el mecanismo de funcionamiento de una Autoridad de Certificación (CA), indicando si se usa con criptografía de llave simétrica o asimétrica.

Una Autoritat de Certificació serveix per donar validesa de que una clau pública pertany a una entitat en concret i pugui ser utilitzada per la resta amb seguretat. El mecanisme consisteix en què l'entitat demostra la seva identitat a la CA i li facilita la seva clau pública. Quan ha passat la verificació, la CA emet la clau pública de l'entitat, donant-li validesa, i encriptada amb la clau pública de la CA, de manera que així qualsevol altra entitat pot estar segura de l'originalitat i procedència de les claus.

Per tant, és un sistema que utilitza clau asimètrica, ja que es fa amb les claus públiques de cada part.

Pregunta 12. Explica la diferencia de funcionamiento entre un KDC (Key Distribution Center) y una Autoridad de Certificación (CA) y con qué tipo de criptografía se usa cada uno de ellos.

KDC → Clau simètrica.
Alice es comunica amb el KDC amb la clau simètrica que tenen per a tal fi Alice-KDC.
El KDC li retorna un missatge encriptat Alice-KDC. Aquí dins hi ha un altre missatge encriptat amb la clau

KDC-Bob i que només Bob podrà obrir on hi conté la clau Alice-Bob.
Alice envia aquest missatge a Bob per a que el desencripti i podrà obtenir la clau Alice-Bob.

CA → Clau pública. Una Autoritat de Certificació serveix per donar validesa de que una clau pública pertany a una entitat en concret i pugui ser utilitzada per la resta amb seguretat. El mecanisme consisteix en què l'entitat demostra la seva identitat a la CA i li facilita la seva clau pública. Quan ha passat la verificació, la CA emet la clau pública de l'entitat, donant-li validesa, i encriptada amb la clau pública de la CA, de manera que així qualsevol altra entitat pot estar segura de l'originalitat i procedència de les claus. Per tant, és un sistema que utilitza clau asimètrica, ja que es fa amb les claus públiques de cada part.