**SSN COLLEGE OF ENGINEERING**

**Department of Computer Science and Engineering**

**B.E. Computer Science Semester: 7**

**CS6703 - GRID AND CLOUD COMPUTING**

**Answer Key**

**04 SEP 2017, 8 - 9.30 AM Unit Test 3 Max Marks: 50**

**Academic Year: 2017- 2018 Batch : 2014-2018**

**Staff Dr. K Vallidevi / Ms. Y. V. Lokeswari**

**PART A 5X 2 = 10**

**1. List the goals of OGSA architecture (CO3, K2)**

VO Management

Job submission and Management

Data Management

Workflow

Security

Resource Discovery and Monitoring.

**2. What is the difference between Web Service and Grid Service (CO1, K2)**

**Web Service**: These are stateless services and not persistent

**Grid Services:** Web Services are made stateful with the help of interfaces provided by OGSA standard are termed as Grid Services.

**3. What is the purpose of Factory interface in Grid services. (CO3, K2)**

Services implement this interface to create new Grid service instances.

This service is called a factory.

CreateService() operation creates a requested service and returns the GSH and initial GSR.

Again OGSA does not specify how the instance is created.

**4. Define Trust and Reputation (CO4, K2)**

**Trust** is the firm belief in the competence of an entity to behave as expected such that this firm belief is a dynamic value associated with the entity and it is also subject to the entity’s behavior and applies only within a specific context at a given time.

The **Reputation** of an entity is an expectation of its behavior based on its identity and other entities’ observations or information about the entity’s past behavior within a specific context at a given time.

**5. What is the role of a Certification Authority in providing security? (CO4, K2)**

* A X.509 certificate binds a public key to a name
* It includes a name and a public key (among other things) bundled together and signed by a trusted party (Issuer)
* By checking the signature, one can determine that a public key belongs to a given user.
* **A Certificate Authority is an entity that exists only to sign user certificates**
* The CA signs it’s own certificate which is distributed in a trusted manner
* The public key from the CA certificate can then be used to verify other certificates

**PART B 40 Marks**

**6. a. In detail explain the various Trust Models (CO4,K2) (10)**

* PKI Based Trust Model
* Network Topology Based Trust Model
* Basic Behavior Based Trust Model
* Domain Based Trust Model
* Subjective Trust Model
* Dynamic Trust Model

(OR)

**6. b. List and explain the basic services of OGSA (CO1,K2) (10)**

Common Management Model (CMM)

Service domains

Policy

Security

Provisioning and resource management

Accounting/metering

Common distributed logging

Monitoring

Scheduling

Distributed data access and replication

**7. (a) (i) What is Data Grid? Explain about Data Grid Services. (CO3, K2) (10)**

**Ans:** Data Grid address computational and data intensive applications. Combine huge amounts of data and resources which are geographically distributed. Provide very high availability and reliability

**Data Grid Services:**

GDH, GDR, Data Registry

Factories

Registries

Service Lifecycle Management

(OR)

**(ii) Explain about various Grid Data Access Models. (CO3, K2) (5)**

Ans: In general there are four access models for organizing a data grid as listed here

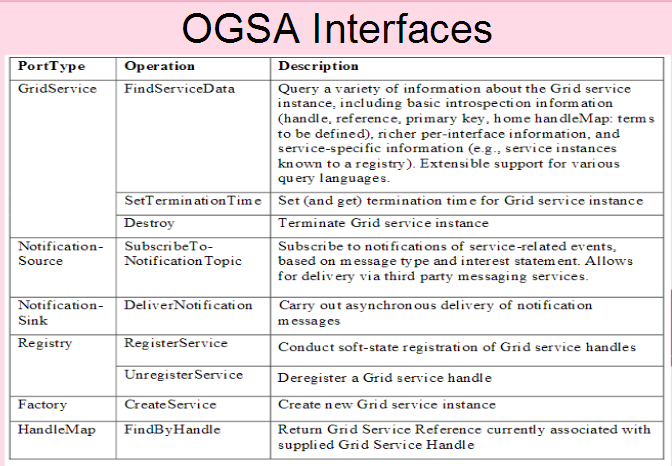
1.Monadic method

2.Hierarchical model

3.Federation model

4.Hybrid model

**7. (b) Explain in detail about OGSA Interfaces and its operations. (CO3, K2) (15)**

****

**8. (a) (i) Discuss about Public Key Infrastructure (PKI) and Grid Security Infrastructure (GSI). (CO4, K2) (10)**

PKI allows you to know that a given public key belongs to a given user

PKI builds off of asymmetric encryption:

Each entity has two keys: public and private

The private key is known only to the entity

The public key is given to the world encapsulated in a X.509 certificate

**Public Key Infrastructure (PKI) Overview**

**X.509 Certificates**

**Certificate Authorities (CAs)**

**Certificate Policies**

**Certificate Policies**

Namespaces

**Requesting a certificate**

Certificate Request

Registration Authority

**Grid Security Infrastructure (GSI)**

The Grid Security Infrastructure (GSI) is a set of tools, libraries and protocols used in Globus to allow users and applications to securely access resources.

GSI is based on a public key infrastructure, with certificate authorities and X509 certificates

Uses SSL for authentication and message protection

Adds features needed for Single-Sign on

Proxy Credentials

Delegation.

GSI is:

X.509 Certificates for authentication

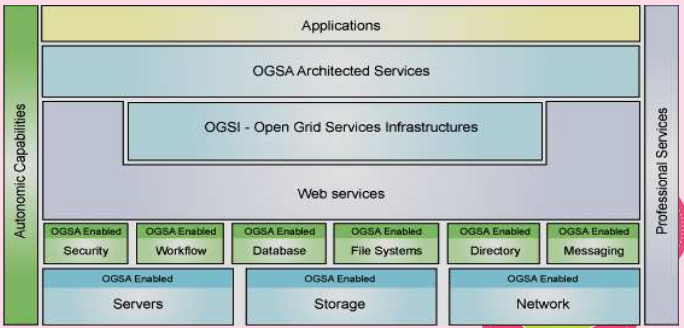
PKI for verifying identities in Certificates

SSL as the protocol for authentication, confidentiality and integrity

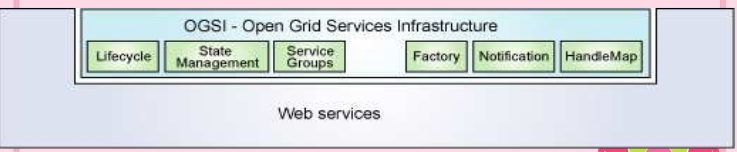
Proxy Credentials and delegation to support single sign-on

**(ii) Sketch and explain the OGSA Architecture. (CO3, K2) (5)**

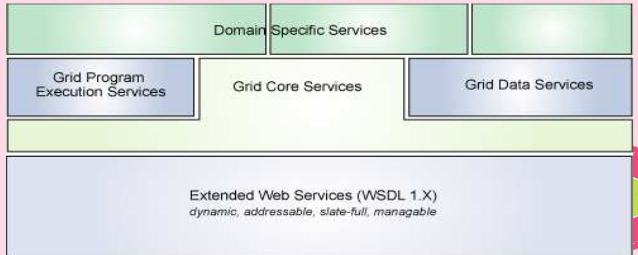
Open Grid Services Architecture (OGSA) is a set of standards that extends Web services and service-oriented architecture to the grid computing environment. OGSA definitions and criteria describe how information is shared and distributed among the components of large, heterogeneous grid systems.

****

**Web Service Layer**

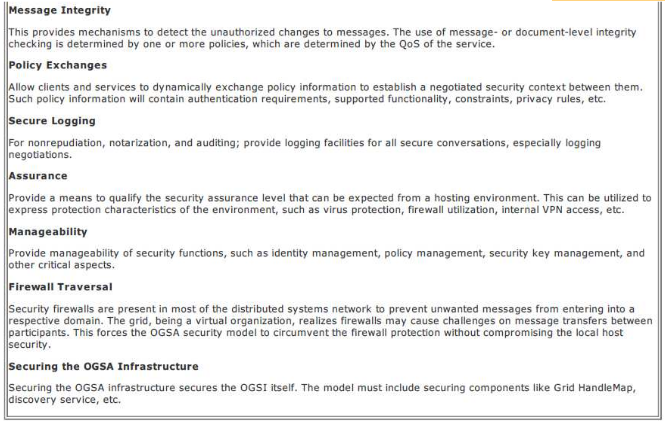
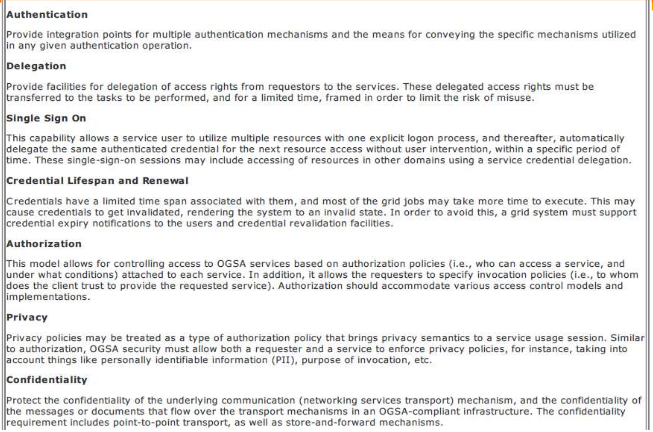
****

**OGSA Architected Service Layer**

****

**8. (b) Explain about the following security parameters. (CO4, K2) (15)**

* **Authentication & Authorization. (2)**
* **Single Sign On. (2)**
* **Delegation & Privacy. (2)**
* **Confidentiality & Message Integrity. (2)**
* **Symmetric Key Cryptography. (2)**
* **Public Key Cryptography. (2)**
* **Digital Signature and Message Digest. (3)**

****