**NAME**

**COLLEGE NUMBER**

**Instructions:**

Based on the security objectives in the following table, design an enterprise encryption strategy—a public key infrastructure (PKI) that supports internal employees, external business partners, and clients. Include the design and reasoning for using the selected encryption strategy.

**Introduction**

In growing and mid-level to international curate companies, there is need to safeguard company information, this has a lot do with data. Data being the heart of the organisation needs to be safeguarded at all costs. In order to achieve this, there is need to identify key information sources, the resources associated with source touch points and then observing the whole infrastructure. During such an activity, one thing that should be keenly observed are data leaks. Data leaks are the points at which a company is likely to lose vital information either internally, extremely or externally. Designing an effective public key infrastructure is one way to absolving this. The below following ways can be implemented at different levels in the company:

**Privacy and confidentiality**

Privacy is concerned with protecting information from unauthorised persons. One way to achieving this is by storing confidential information in a secure server where anyone who wants access to this information will have to download a onetime few second’s expiry remote desktop protocol with a signature specifically assigned to the user id, this way, only authorized persons and access these information. Also, the server can record every user activity within the remote server, for audit purposes, this is very key.

**Integrity**

Cryptography and encryption algorithms can be applied on the resources that users would like to access, e.g., by having one time passwords that last only a few minutes to be used by authenticate user to access a resource.

**Message authentication**

Firewalls and proxies should be implemented on the network to ensure that the income information is only from an allowed client and if not, client should be flagged and blocked. Also, all URL requests coming both at intranet and extranet level should be encrypted with secure shell encryption to avoid man in the middle attacks.

**Signature**

A Unix or Linux sever or a dedicated VPS is recommended for storing sensitive information, in such a manner, one would have to obtain a private key without the system and use it to log in to the server in order to access a resource. Example here is an RSA.pub for remote connection.

**Authorisation**

Can be achieved by having intranets and extranets that are only accessible by an IP address that is mapped to a given a user ID table. If that ID is not found on the IP table then the authorisation is denied. Also, complex passwords can be system generated and sent to users by mail, if the password expires automatically and user has not requested, then they won’t log in to the resource application.

**Validation**

Remote desktop protocols are significant in accessing file servers and should only be available for a small period of time after which they expire.

**Access control**

Role based access can be implemented in accessing certain sensitive information of users and URLs. For instance, top level managers could have access to a more sensitive info than their juniors.

**Certification**

Development and installation of certain antivirus applications can be used to flag unauthorised or suspicious email attachments, links and demounts circulating the network.

**Time stamping**

One way of achieving this is by configuring business applications to store audit trails and user activity of the various activities that a logged in user can perform. A specific key generate by the sever identifying the logged in use can be used to establish and terminate connections of users.

**Witnessing**

Document approval and request processing is one way of uploading a document and signing it digitally for the next senior level to also sign and approve, this ensures that the document is fully witnessed by all needed by the end of the day, a private key assigned to the document can be used on the public key of all users responsible in viewing the document.

**Receipt**

Can be achieved by allowing a user to download a pdf copy of the activity or job that they just completed and then sending it via email to the same user.

**Confirmation**

Whenever a user would like to complete a given request or process, a page could exist where users have to digitally sign in with their passwords before the completion status is guaranteed.

**Ownership**

By using role based access, users within a given level of governance can access a given business application, be able to modify and send resources to others for actions.

**Anonymity**

In certain cases like job interviews and tender hiring, identity of users can be masked by encrypting their IDs to avoid conflict of interest.

**Non-repudiation**

Users sending information to each other over an encrypted network, can have digital signatures applied to those information sets and by use of both the private and public key be able to interpret and open these information. In such a case, a user will not deny as to have viewed or manipulated the resource.

**Revocation**

Revocation of a digital certificate could apply if the DS is no longer valid or expired.