CYB 300 5-2 Milestone Three: PKI, FSDP, and CIA Worksheet

Andree Salvo
Southern New Hampshire University
CYB 300-14668
Instructor: Jason Keltner

I. Security Analysis Table

Security Analysis Table		
Fundamental Security Design Principles	Describe how the FSDPs relate to PKI (2–3 sentences)	Describe how the FSDPs relate to the CIA triad (2–3 sentences)
Isolation	A Public Key Infrastructure (PKI) ensures that systems are separated by granting access to certificates only to authorized users and devices. Meaning that if something gets compromised,	Isolation relates to confidentiality and availability. It helps ensure that only the right people can access the data, and nothing is shared until they're verified. Furthermore, once someone has cleared the data, it remains available and ready for them, which keeps things accessible when needed.
Modularity	Modularity is evident in PKI by breaking down tasks into smaller sections, such as creating keys, verifying a person's identity, and then using those keys to grant access or transfer data. Each piece has its role, and they all work together without relying too heavily on one another.	As for modularity, it relates to availability because everything runs on sections, meaning that the system won't be overwhelmed by users when they need to access all at once. This ensures that things run smoothly and that only authorized individuals can access them when available.
Minimzation of Implementation	PKI ties into minimization by keeping things simple and specific, such as each user receiving their unique certificate from the certificate authority, so there's no guessing who's who. It's a clean way to confirm someone's identity without adding extra steps or complexity to it.	This relates to **integrity** because each certificate is unique to one specific user, so you know exactly who's making changes. This keeps things tight and traceable, ensuring that only authorized personnel can access that data.

Layering	As for layering, you can issue, check, or revoke certificates whenever needed. In other words, if someone attempts to access something, the individual's certificate is checked, which adds an extra layer of defense to the system.	This supports **integrity** because it gives you the ability to double-check every request with an authentication certificate. If something seems a bit off, the certificate can be revoked immediately, which helps prevent data from being tampered with.
Least Privilege	With PKI, you can give people access only to the exact things they need through certificates. This helps keep things tight and secure, reducing risks.	This supports **confidentiality** by locking people out of stuff they don't need and helps **integrity** by limiting who can change things and preventing any data being tampered with.
Fail-Safe Defaults/Fail Secure	If something's wrong, such as a bad or expired certificate, the system should immediately block access until it's fixed till further notice.	This supports **availability** and **integrity** by preventing systems from running with incorrect settings. It's better to deny access than risk damage.
Trust Relations	PKI relies on trust—much like trusting the root CA and every step down from it. If you trust the source, you can trust the key or certificate that's being handed out.	This supports confidentiality and integrity, as only trusted sources can send or receive secure information. If the trust chain is broken, everything falls apart.

II. Scenario-Based Short Response Questions

A. **Temporary Contractor**: The use of CAs as part of PKI provides a mechanism for key management and secure communications. If you were asked to provide access to information systems to a temporary contractor, what areas of a PKI and CIA triad would you be concerned with? Which of the FSDPs most applies here?

If I needed to grant access to a temporary contractor, my primary concerns would be with the duration of validity of their certificate, the types of systems they can access, and the management and revocation of their key. With respect to the CIA triad, I would be most concerned about confidentiality, ensuring that the contractor sees only what they are supposed to see, and integrity, ensuring that they do not alter sensitive but otherwise visible data while performing their functions.

The most relevant Federal Standard for Data Protection (FSDP) is the principle of least privilege. This principle is commonly known, which dictates that users of a system should be granted access only to the information and resources necessary for their specific job role, enabling them to perform their tasks effectively.

B. **Cryptography**: As part of PKI, a cryptographic system is established. Explain how cryptography is used and what forms of implementation can be accomplished.

PKI uses cryptography to perform the essential tasks of encrypting data, creating digital signatures, and authenticating users or devices. Its implementations include asymmetric encryption (using public/private key pairs), digital certificates issued by CAs, and secure hashing algorithms. This helps verify identity, secure communications, and maintain data integrity across networks.