Digital Signatures -Evaluation Rubric

lucasqhliu@gmail.com Switch account

Not shared

Saving…

* Indicates required question

Please specify your group: e.g. BBY-1 or DTC-1 *

BBY25

Which Group's work did you review? *

BBy32

*

Based on the following, how do you evaluate the other group's answer to the first question?

1. Purpose of Requesting E-Signatures in Adobe Acrobat Pro: The primary purpose of requesting e-signatures in Adobe Acrobat Pro is to streamline and digitize the document signing process. E-signatures, or electronic signatures, offer a secure and legally recognized method for individuals and businesses to sign documents electronically, eliminating the need for physical signatures on paper. This feature facilitates a more efficient and convenient way to sign, send, and receive documents, reducing the time and resources required for traditional paper-based signatures.

	No Evident Effort (0/4)	Way Below Expectations (1/4)	Needs Improvement (3/4)	Meets Expectations (4/4)
Purpose of requesting e-signatures	○	○	○	◉

Please read the following section carefully and evaluate the other group's work: Have they adequately mentioned/explained each specific part of an e-signature system? *

2. How E-Signatures Work: E-signatures use cryptographic methods to ensure the authenticity and integrity of a signed document. Here's a simplified overview of how e-signatures work:
Authentication: The sender initiates the signing process, often through a platform like Adobe Acrobat Pro. The recipient is notified and accesses the document through a secure link.

Document Hashing: The document is hashed, creating a unique identifier for that specific document. This hash is a digital fingerprint that represents the content of the document.

Digital Signature: The sender's digital signature, generated using their private key, is applied to the document. The digital signature includes information about the signer and the document, providing a way to verify the sender's identity.

Public Key Infrastructure (PKI): E-signature systems often use PKI, where the sender has a private key to sign the document, and the recipient can use the sender's public key to verify the signature.

Secure Transmission: The signed document, along with the digital signature, is securely transmitted to the recipient. The recipient can verify the signature using the sender's public key.

Legal Validity: E-signatures are legally recognized in many jurisdictions, providing a valid and secure alternative to traditional signatures.

	No Evident Effort (0/4)	Way Below Expectations (1/4)	Needs Improvement (3/4)	Meets Expectations (4/4)
Authentication	○	○	○	◉
Document Hashing	○	○	◉	○
Digital Signature	○	○	○	◉
Public Key Infrastructure	○	○	○	◉

(PKI)

Secure Trasmission	○	○	◉	○
Legal Validity	○	○	○	◉

Quality of Communication: *

- The document is readable and well organized.
- you can easily follow and understand the document.

- ○ No Evident Effort (0/4)
- ○ Way Below Expectations (1/4)
- ○ Needs Improvement (3/4)
- ◉ Meets Expectations (4/4)

Please sum up all the grades and record the final grade you have given this group (total is 32): *

30

IMPORTANT: before submitting this form, PRINT it as a PDF file and provide an electronic copy to the other team. *

- ◉ Yes, we provided a PDF copy to the other team.

Submit Clear form

Never submit passwords through Google Forms.