

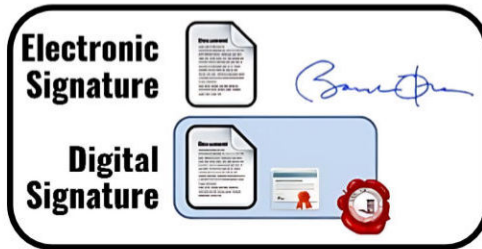
Name: _____ Student No.: _____ Date: ____/____/____

Digital Signatures

DIGITAL SIGNATURES

A **digital signature** on an electronic document or other object is **created by using a form of cryptography** and is **equivalent to a personal signature on a written document**.

It provides **proof of the object's origin** and a means by which to **verify the object's integrity**.



In this worksheet, you will understand how digital signatures ensure that the information **originated from the signer** and was **not altered** when signing a PDF file.

How to Digitally Sign a PDF File?

You can digitally sign a PDF using **Adobe Acrobat Sign**, which supports digital signatures.



According to Adobe, unlike a handwritten signature, digital signatures can be **easily verified** and **informs recipients whether the document was modified** after the signer initially signed it.

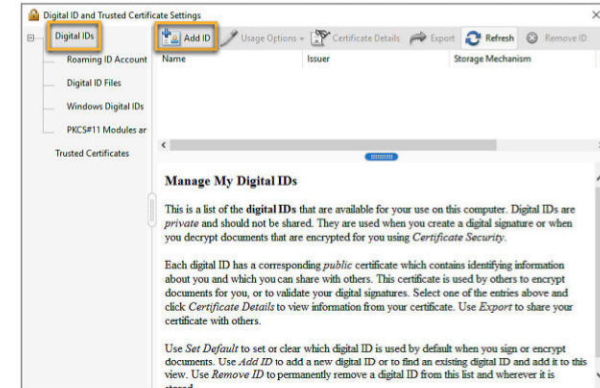
When you digitally sign a document, you also share a **certificate** and a **public key**, which confirm your identity. These certificates can be obtained from a **cloud-based trust service provider** or the **signer's local system**.

In the Philippines, the **Department of Information and Communications Technology (DICT)** provides **free digital certificates**, valid for up to two years. You can learn more and apply by scanning this **QR code**.

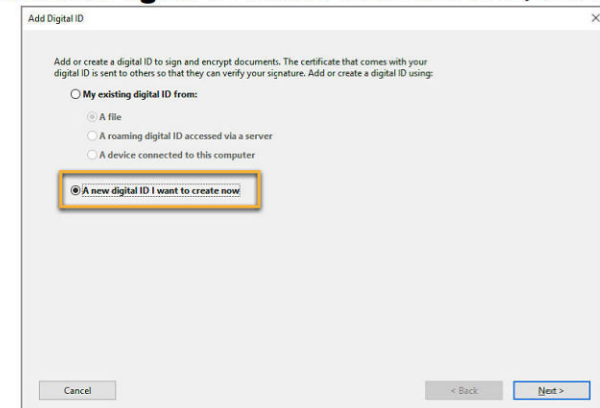


Let us create a digital certificate on your local system to sign your Certificate of Registration for this semester.

1. **Check if Adobe Acrobat is installed.**
 - a. If it is not installed, scan the QR code to download it.
 - b. On the download page, **uncheck the "Install McAfee Security Scan Plus" option** under More add-ons to avoid installing extra software.
 - c. Follow the on-screen instructions to complete the installation.
2. In Acrobat, select the hamburger menu  and then choose **Preferences**.
3. In the Categories list on the left, select **Signatures**. On the right, select **More** for **Identities & Trusted Certificates**.
4. Select **Digital IDs** on the left, and then click the **Add ID** button .

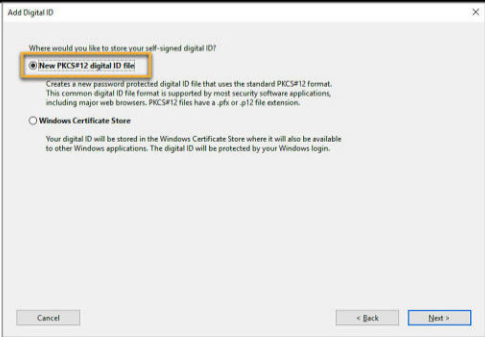


5. Select the option **A New Digital ID I Want To Create Now**, and click **Next**.



6. Select the option **New PKCS#12 Digital ID File**, and click **Next**.

PKCS#12 is a binary format for storing a **certificate chain** and **private key** in a single, encryptable file.

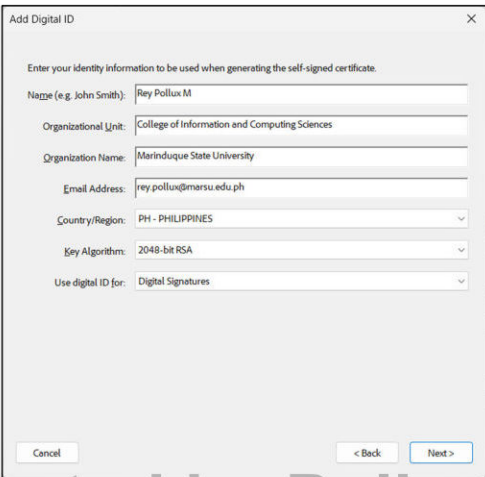


7. Enter your personal information for the certificate:

Name: Your name in this format: Last Name First Name Middle Initial
Organizational Unit: College of Information and Computing Sciences
Organization Name: Marinduque State University
Email Address: Your institutional email address
Country: PH - PHILIPPINES

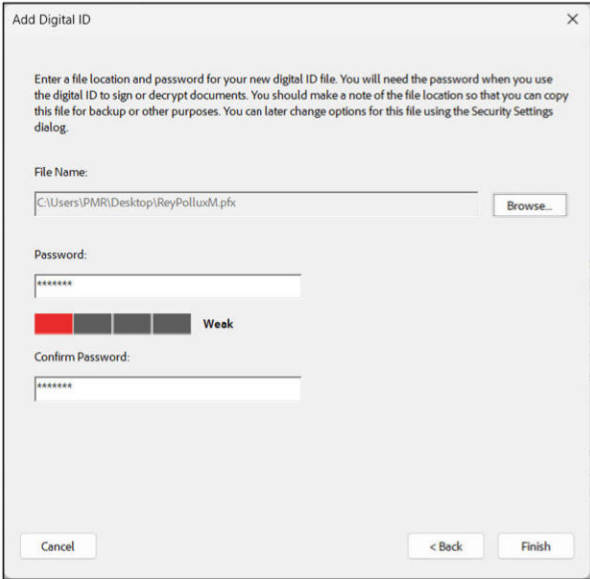
8. Choose the **2048-bit RSA** option from the **Key Algorithm** menu.

9. From the **Use Digital ID For** menu, select the option to use your digital ID for **signatures only**.

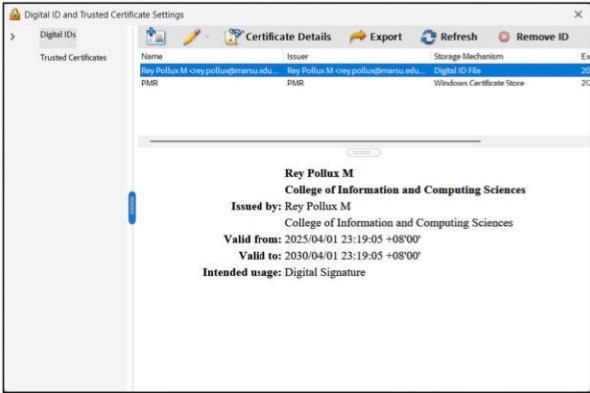


10. Save the digital certificate on your Desktop by clicking **Browse** and selecting the **Desktop** folder.

11. Enter your **student number** (e.g., 25B1234) as the **password** for the digital ID file and click **Finish**.




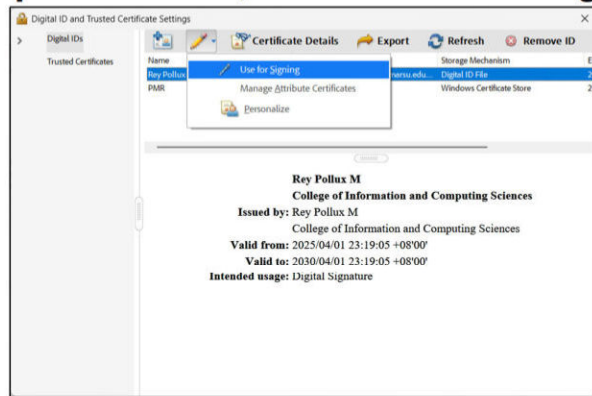
12. You should now see your digital certificate has been created.



To avoid being prompted to select a digital ID each time you sign a PDF, you can select a default digital ID.

1. In Acrobat, select the hamburger menu  and then choose **Preferences > Signatures**. In **Identities & Trusted Certificates**, select **More**.

2. Select **Digital IDs** on the left, then select the digital ID you want to use as the default.
3. Click the **Usage Options** button , and choose the **Use for Signing** option.



Now that you have a digital certificate, you can use it to sign your Certificate of Registration (COR).

1. In PRIISMS, download your COR for the current semester.
2. Open your COR in Adobe Acrobat.
3. Choose **All Tools > View more > Use a certificate** in the global bar.
4. Select **Digitally Sign** to apply a visible digital signature.
5. Using your mouse, click and drag to draw the area where you would like the signature to appear.
6. In the **Sign with a Digital ID** dialog box, choose the Digital ID you want to use for signing the document and select **Continue**.
7. A preview of your digital signature will be displayed.
8. Enter the password for your digital certificate and select **Sign**.
9. Save the signed COR to your Desktop, adding “_Signed” to the file name (e.g., `cor-mscGp41YENgZ8_Signed.pdf`).
10. Look for the blue ribbon that says “**Signed and all signatures are valid**” to confirm the document hasn’t been modified.
11. View your certificate and public key:
 - a. Click on your digital signature in the document.

- b. In the **Signature Validation Status**, click **Signature Properties > Show Signer’s Certificate**.
- c. In the **Certificate Viewer**, click **Details** to see your certificate (X.509 data) and public key.
- d. As mentioned earlier, when you digitally sign a document, you also share a certificate and a public key.

12. Take screenshots of your certificate and public key:

- a. Click the **public key**, take a screenshot of your entire screen, and save it as: `LastName_FirstName_PublicKey.jpg`.
- b. Click the **X.509 data**, take a screenshot of your entire screen, and save it as `LastName_FirstName_Certificate.jpg`.

What happens when you edit a digitally signed document?

When you make any changes-even something as minor as **highlighting text**-in a digitally signed document, Acrobat will prompt you to **validate the digital signatures**.

This validation process checks if any changes have been made to the document.

If changes are detected, the **original digital signature becomes invalid** unless the modifications are **re-signed by the person who made them**.

Let us see how this works by making some changes to the document.

1. Highlight your name in the COR.
2. The blue ribbon will say “At least one signature requires validating” this could mean that the document may have been modified the time after it was digital signed.
3. To validate this signature, choose **All Tools > View more > Use a certificate** in the global bar.
4. Click **Validate All Signatures**.
5. The blue ribbon will now update to say, “**Signed and all signatures are valid, but with unsigned changes after the last signature**”.

6. To see these changes, open the **Signature Panel** in the blue ribbon. A sidebar will appear showing **Annotations Created**, where you can review the modifications.
7. Take a screenshot of your entire screen and save it as:
LastName_FirstName_Modifications.jpg
8. To finalize the modifications, you need to digitally sign the document again.
9. In **Use a Certificate**, select **Digitally Sign**.
10. Place your digital signature below the **Data Privacy Consent** section for consistency.
11. Follow the previous instructions for signing.
12. Save the signed COR to your desktop, adding “_2” to the filename (e.g., cor-mscGp41YENgZ8_Signed_2.pdf).
13. You have now validated the changes. You can open the **Signature Panel** to review the document’s change history.

Submission Instructions (Google Classroom)

Submit the following files in Google Classroom:

1. **PKCS#12 Digital ID File** - Your digital ID file (e.g., ReyPolluxM.pfx).
2. **Initially Signed PDF** - The first version of your signed PDF (e.g., cor-mscGp41YENgZ8_Signed.pdf).
3. **Public Key Screenshot** - A screenshot showing your public key (e.g., Rey_Pollux_PublicKey.jpg).
4. **Certificate Screenshot** - A screenshot of your certificate (e.g., Rey_Pollux_Certificate.jpg).
5. **PDF Modification Screenshot** - A screenshot of the modifications shown in the Signature Panel (e.g., Rey_Pollux_Modification.jpg).
6. **Final Signed PDF with Modifications** - The updated PDF, signed again after modifications (e.g., cor-mscGp41YENgZ8_Signed_2.pdf).

Resources:

https://helpx.adobe.com/ph_en/acrobat/using/digital-ids.html

<https://helpx.adobe.com/sign/config/digital-signatures/overview.html>

<https://www.ibm.com/docs/en/i/7.5?topic=concepts-digital-signatures>

<https://www.ibm.com/docs/en/b2badv-communication/1.0.0?topic=overview-digital-signature>

<https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96>