



SIGNATURES PROTOCOL

DURING THE

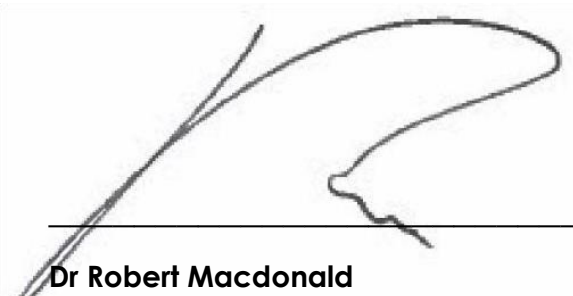
NATIONAL STATE OF DISASTER

DECLARED IN MARCH 2020

Document History

Version	Date	Amended by	Changes
1.0	2 July 2020	M Johnson	Final

Approval



Dr Robert Macdonald
Head of Department: Social Development

2 July 2020

Date

1. Purpose

The purpose of this protocol is to provide guidance on how to deal with the signing of documents during the National State of Disaster. It is based on the Department of the Premier's "Protocol for the use of Electronic Signatures during the National State of Disaster" declared in March 2020 by the President of South Africa that was approved for implementation in the Department of the Premier by the Director General of the Western Cape Government in the Department of the Premier on 22 May 2020. This protocol has been adapted to suit the needs of the Department of Social Development and this policy/protocol thus institutionalizes the use of three methods of approving particular documentation within the Department, one of which is the electronic signature.

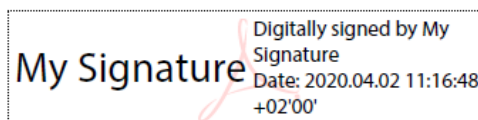
2. Background

- 2.1 During normal business operations, submissions, letters and forms are submitted to the required signatories and are physically signed by them. During the State of Disaster, an e-signature option approved for implementation by the Director General in the Department of the Premier was explored by the Department of Social Development and found to be compatible with its needs and could be added to the signature options currently employed in the Department. This e-signature enables Departmental Officials who are working from home to support, recommend or approve relevant documentation.
- 2.2 MyContent has an e-signature capability, but this has not been fully implemented yet. The Centre for e-Innovation (CeI) is also currently exploring an e-signature capability, but this will still take time to procure and implement.
- 2.3 Two methods are currently available in the Department for the signing of documents during the State of Disaster. These are as follows:
 - 2.3.1 email support, recommendation and approval and;
 - 2.3.2 Scanning of physically signed documents and the emailing of the signed and scanned document to the relevant authority for safeguarding.

- 2.4 A viable third option is the use of e-signatures as outlined in the approved Department of the Premier's Electronic Signatures Protocol. Electronic signatures, being the term used in the Electronic Communications and Transactions Act 25 of 2002¹ (hereinafter referred to as "the ECT Act"), are very useful where a signature on a hard copy document is required but the staff member(s) so required to sign are geographically dispersed and not able to be physically present for said signature(s) and/or do not have access to scanning equipment to provide the required signature to the relevant authority.
- 2.5 Email Support, Recommendation or Approval as well as the scanning and submission of the physically signed document(s) are options that have been successfully used by departmental officials who have had their workstations and printer/scanners located at their homes since the Lockdown. Here of course, physical access to their and user access is controlled by the staff member. No other staff members have access to the workstation at the official's place of residence.

3. Electronic Support, Recommendation and Approval Options

- 3.1. Although the term 'electronic signature' as contemplated by the ECT Act is much wider than the type of electronic signature as described above (i.e. the Adobe Reader's "digital signature"), the under-mentioned electronic signature is one of the three preferred options for the Department of Social Development. Electronic support, recommendation or approval in the Department of Social Development can take the following forms:
- 3.1.1. Electronic Signatures in the form of a "digital signature" as per the Adobe Reader application.



¹ Defined in the Act in section 1 as follows:

“electronic signature” means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature”

3.2. Electronic Signatures

3.2.1. In the context of the Department of Social Development, an electronic signature relates to the official, electronic support, recommendation or approval of any document exported as a pdf document by adding a digitally encrypted electronic signature to the document using Adobe Reader. This type of signature is referred to as a “digital signature” by the Adobe Reader application.

Annexure A provides a guide on how to create and insert this type of electronic signature using Adobe 2020 and **Annexure D**, provides a guide in cases of where Adobe 2018 and older versions are used.

3.3. Email Noting, Supporting, Recommendation and Approval

3.3.1. Signatories to a document can use emails as confirmation when they note, support, recommend or approve a document.

3.3.2. An e-mail by the signatories should be sufficient when noting, supporting, recommending or approving a document as the names of the parties at the foot of their respective emails are intended to serve as signatures and identification of the parties.

3.3.3. E-mails should however be clear and must contain the Noting, Recommendation, Support or Approval of the signatory:

3.3.3.1. A brief description of the document, the version being recommended, supported or approved and the title of the document; and

3.3.3.2. “Noted” or “Recommended” or “Not recommended” or “Supported” or “Not Supported”; or

3.3.3.3. “Approved” or “Not approved”

3.4 Scanning of physically signed documents and emailing to the relevant recipient

3.4.1 Where a document is physically signed and scanned it can be emailed to the necessary recipient for further signatures or finalization.

- 3.4.2 The original signed documents must be made available once the State of Disaster/Lockdown has been lifted and/or the staff member(s) return to office.
- 3.4.3 The scanned signed documents must be attached to the original signed documents and filed accordingly.

4. Electronic Signature Protocol

4.1. Official letters, memos and other documents requiring a single signature

When an official letter, memo or other document requires only one signature, the document must be converted to pdf and digitally signed per paragraph 3.2 above. The initiator must lock the document at the time of applying the electronic signature so that no further changes can be made to the document (see screenshot below).



4.2. Department of Social Development Submissions and other documents requiring more than one signature

4.2.1. Initiator:

After drafting the submission or other document, the initiator must convert/export the document to pdf and append his/her signature to the document as per paragraph 3.2 above prior to sending the document to the official next in line.

4.2.2. All signatories on route (excluding approver):

- 4.2.2.1. All electronic signatures appended to the above documents must be validated by the official receiving an electronically signed document to confirm its authenticity **once off**

(per signature), where-after it will be recognised as a trusted signature. **Annexure B** provides a guide on how to validate electronic signatures.

4.2.2.2. All signatories on route must clearly indicate their recommendation or support on the pdf document by using the comments function in Adobe. Instances where comments must be appended to the document must be handled in the same way. Please note that this must happen **PRIOR** to signing of the document. **Annexure C** provides guidance on indication of agreement and appending of comments on pdf documents.

4.2.2.3. Electronic signatures must be appended by all signatories on route following the same process as per paragraphs 3.2, 4.2.2.1 and 4.2.2.2, where after the document must be sent to the next person on route, copying the initiator of the document.

4.2.2.4. All those required to note the submission must also be included in the route, and their signatures should be appended to the submission as per paragraphs 3.2, 4.2.2.1 and 4.2.2.2.

4.2.3. Approver:

4.2.3.1. The approver must follow the steps indicated in paragraphs 4.2.2.1 and 4.2.2.2, where after his/her signature and indication of approval must be appended as per paragraph 3.2.

4.2.3.2. The approver must lock the document at the time of applying the electronic signature so that no further changes can be made to the document (see screenshot included in paragraph 4.1).

4.2.3.3. The approver must then return the locked and signed pdf document to the initiator, who will be responsible for the further distribution of the signed PDF document to the relevant stakeholders. Where possible, safeguarding of the submission on MyContent is required. Where this is not possible, the pdf documents must be submitted to the DSD registry at either the appropriate regional office and/or head office.

4.3. Department of Social Development Submissions using emails as evidence of signature

- 4.3.1. After drafting a submission, the initiator should email the submission to the next person in the signature list. This includes amongst others agreement, support, recommendation, etc. Each signatory should forward the submission to the next signatory in accordance with the signature list that indicate that he/she agrees with the submission. Normally the final signature relates to the approval of the submission.
- 4.3.2. The approver will be responsible to forward the email to the initiator, who must make sure that all evidence is kept confirming that all signatories agreed to the submission. The initiator must ensure that the document is finally distributed to all relevant stakeholders.
- 4.3.3. In the distribution there must be a clear indication to the person receiving the approved submission that all signatories (inclusive of the approver) duly signed off on the submission via email. The initiator will be responsible for the safeguarding of the approved submission that must be stored on MyContent and/or in the appropriate DSD regional and/or head office registry.

4.4. Documentation where electronic signatures are permitted

- 4.4.1. Submissions including Cabinet submissions;
- 4.4.2. All internal correspondence;
- 4.4.3. All external correspondence; and
- 4.4.4. Any other internal document requiring support, recommendation and/or approval, excluding finance-related documents as contemplated in paragraph 4.5.2.

4.5. Contracts and finance-related documents

- 4.5.1. Electronic signatures are not currently permitted for contracts.
- 4.5.2. The CFO will issue a directive applicable to finance-related documents.

5. Control matters – Security and Encryption

- 5.1. All electronic signatures are self-signed and authenticated and as a result are stored on the local machines where they are created. They are not issued by an independent Certifying or Registration Authority.
- 5.2. Electronic signatures are password protected which presents a medium level of risk to authentication as physical security controls are not within the ambit of the Department in remote working scenarios and Two Factor Authentication is also not available with the Adobe electronic signatures.
- 5.3. Acrobat Reader DC does not allow for the encryption of the document but does offer 2048-bit encryption on the certificate of the electronic signature.
- 5.4. A signature trail is maintained of all signatories to the document and if changes are made, but not specifically on what changes.
- 5.5. Please note that the use of your electronic signature may under no circumstances be delegated. Persons appointed in a delegated position must use their own signatures to sign documents, the same as in physical documentation.

6. Commencement and Duration

- 6.1. The implementation of this protocol is effective for the duration of the National State of Disaster declared in March 2020 irrespective of date of signature thereof.

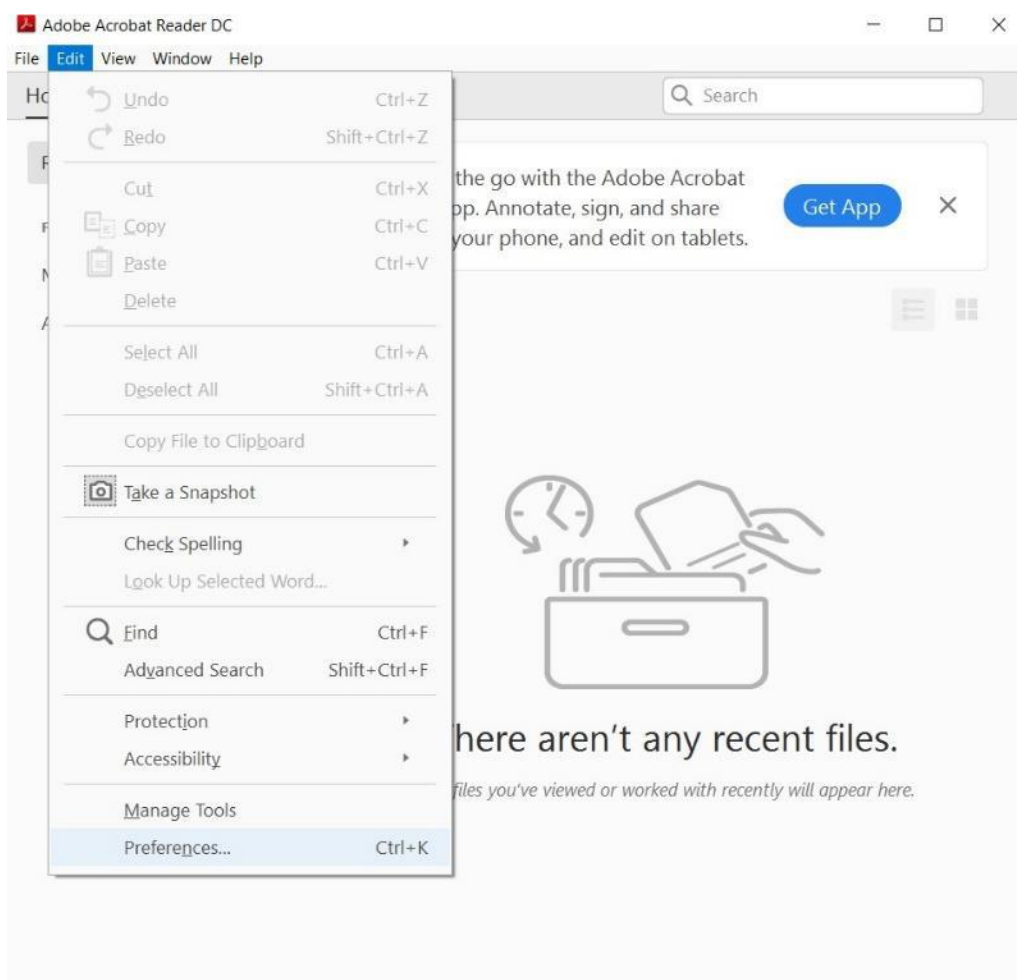
Annexure A – How to create and add an Electronic Signature in a PDF document

1. CREATE A SELF-SIGNED ELECTRONIC ID

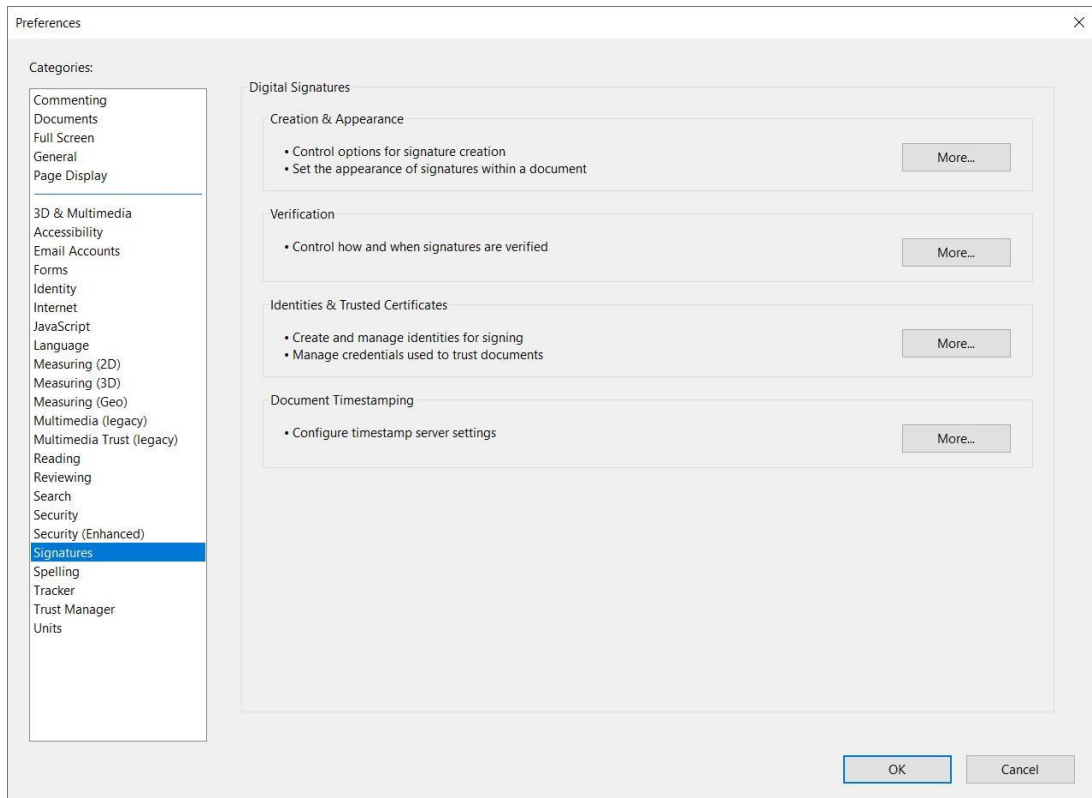
- a. On your Desktop, open Acrobat Reader.



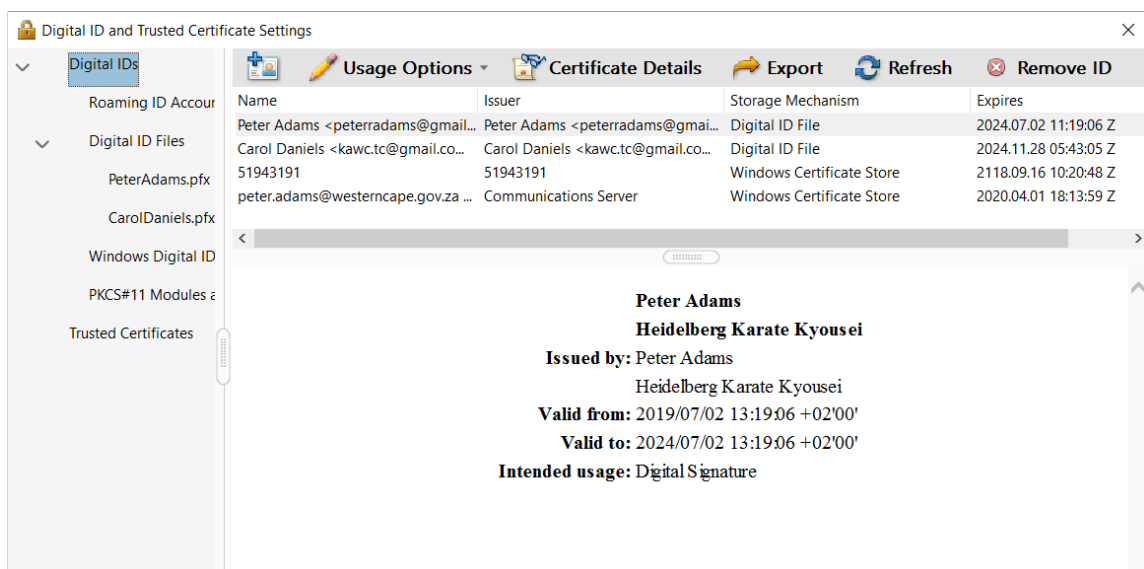
- b. In Acrobat, click the **Edit** menu and choose **Preferences**



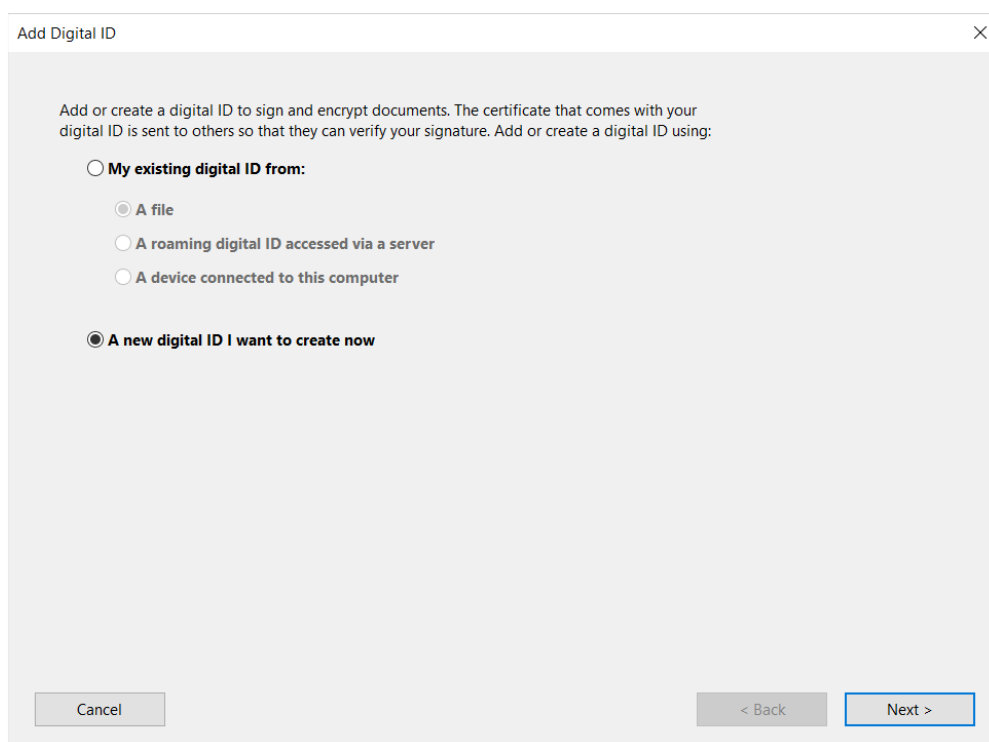
- c. Click on **Signatures**, and then on the **More** button in the **section Identities & Trusted Certificates**.



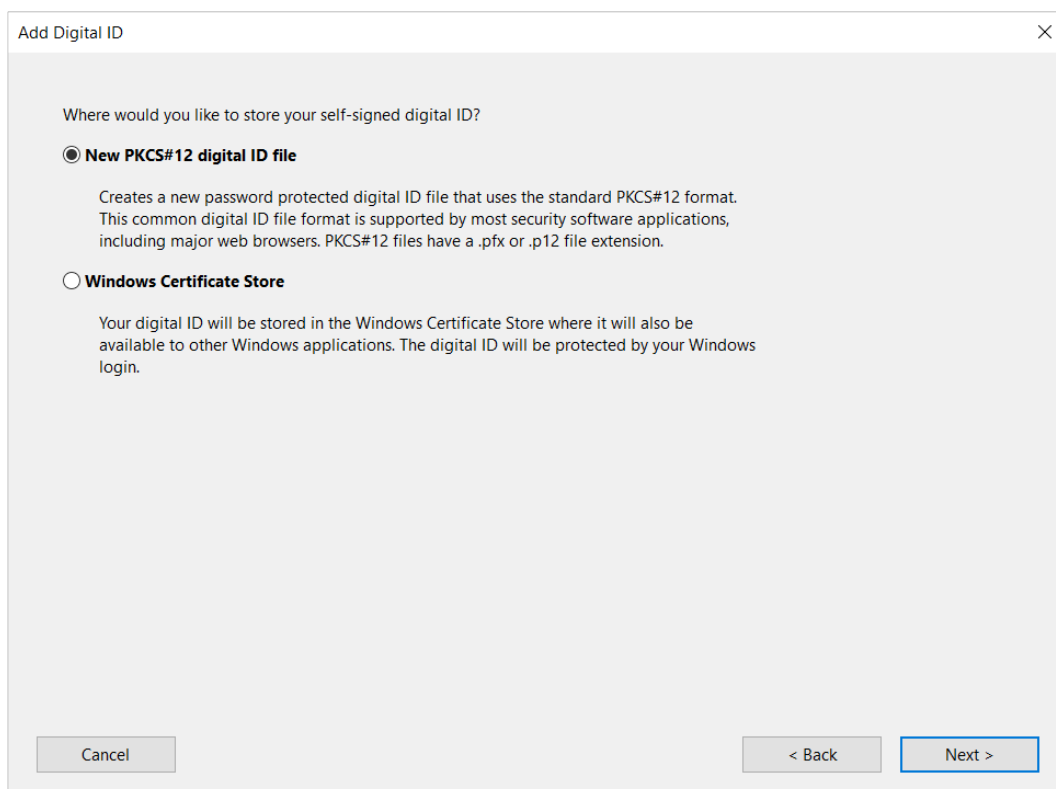
- d. Select **Digital IDs** on the left, and then click the **Add ID** button.



- e. Select the option **A new digital ID I want to create now**. Click on the **Next** button.



- f. Select the **New PKCS#12 digital ID file** option. Click on **Next**.



- g. Add your details and other personal information for your digital ID. When you certify or sign a document, the name appears in the Signatures panel and in the Signature field.

Choose an option from the **Key Algorithm** menu.

From the **Use digital ID for** menu, choose your preferred option. Click **Next**.

Add Digital ID ×

Enter your identity information to be used when generating the self-signed certificate.

Name (e.g. John Smith):

Organizational Unit:

Organization Name:

Email Address:

Country/Region: ▼

Key Algorithm: ▼

Use digital ID for: ▼

- h. Type a **password** for the digital ID.
Browse to save the file in another location. Click **Finish**.

Add Digital ID

Enter a file location and password for your new digital ID file. You will need the password when you use the digital ID to sign or decrypt documents. You should make a note of the file location so that you can copy this file for backup or other purposes. You can later change options for this file using the Security Settings dialog.

File Name:
C:\Users\...AppData\Roaming\Adobe\Acrobat\DC\Security\Johnl

Password:

Best

Confirm Password:

- i. The ID is created.

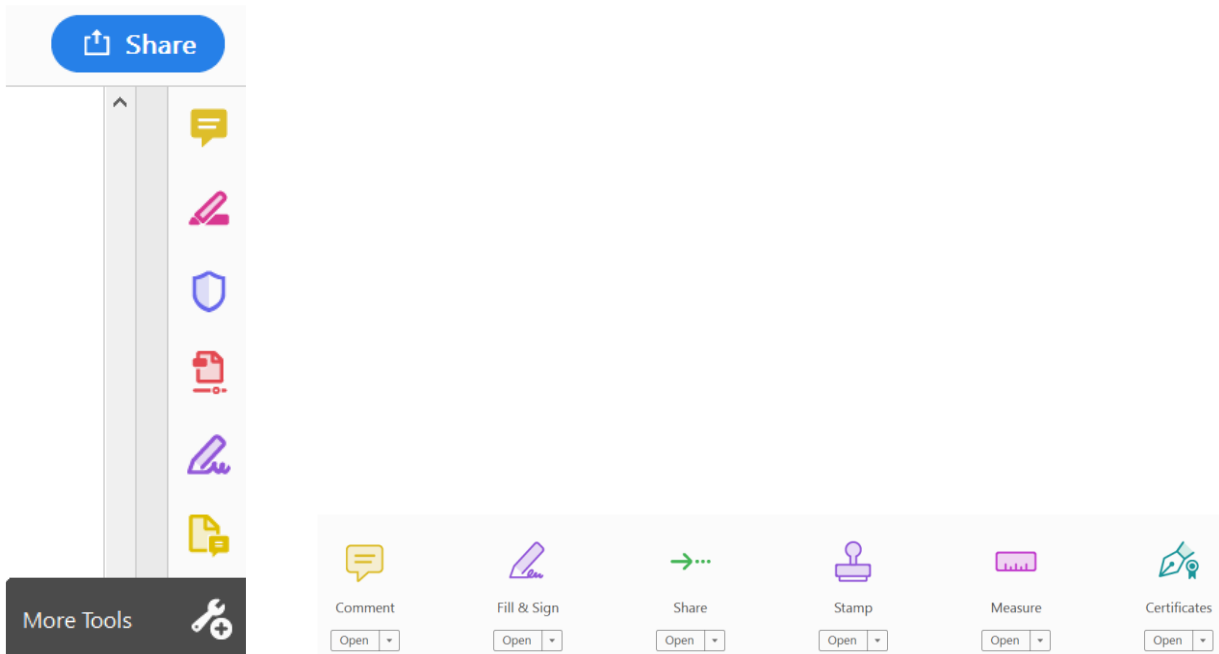
Digital ID and Trusted Certificate Settings

Name	Issuer	Storage Mechanism	Expires
Peter Adams <...@gmail...>	Peter Adams <...@gmail...>	Digital ID File	2024.07.02 11:19:06 Z
Peter Adams <...@gmail.co...>	Peter Adams <...@gmail.co...>	Digital ID File	2024.11.28 05:43:05 Z
Peter Adams <...@gmail.co...>	Peter Adams <...@gmail.co...>	Windows Certificate Store	2118.09.16 10:20:48 Z
...	Communications Server	Windows Certificate Store	2020.04.01 18:13:59 Z

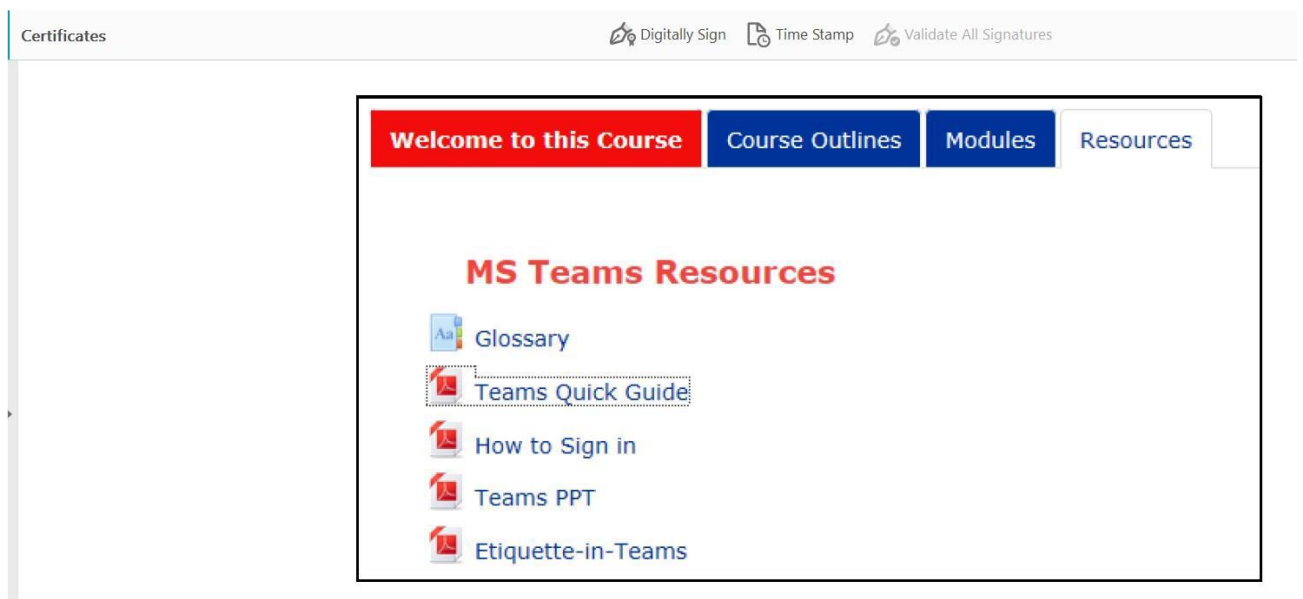
Peter Adams
Western Cape Government
Issued by: Peter Adams
Western Cape Government
Valid from: 2019/07/02 13:19:06 +02'00'
Valid to: 2024/07/02 13:19:06 +02'00'
Intended usage: Digital Signature

2. How to Insert a digital ID into a pdf doc

- a. Open the pdf document to be digitally signed.
- b. Click on the **Certificates** Icon **More Tools** in the lower right-hand corner and choose **Certificates**.



- c. Click on **Digitally Sign**.




- d. Drag your signature box where you want to sign.
Select the signature you want to use for signing and click on **Continue**.

The screenshot shows a dialog box titled "Sign with a Digital ID" with a close button (X) in the top right corner. Below the title bar, there is a prompt: "Choose the Digital ID that you want to use for signing:" followed by a "Refresh" button. There are two digital ID options listed, each with a radio button, a document icon, and a "View Details" link. The first option is "Peter Adams (Digital ID file)" issued by "Peter Adams" and expires on "2024.07.02". The second option is "Carol Daniels (Digital ID file)" issued by "Carol Daniels" and expires on "2024.11.28". At the bottom of the dialog, there is a help icon (question mark), a "Configure New Digital ID" button, a "Cancel" button, and a blue "Continue" button.

- e. Type in your password and click on **Sign**

The screenshot shows a dialog box titled "Sign as 'Peter Adams'" with a close button (X) in the top right corner. Below the title bar, there is an "Appearance" dropdown menu set to "Standard Text" and a "Create" button. The main area of the dialog displays a large signature "Peter Adams" in black, with a red scribble over it. To the right of the signature, the text reads: "Digitally signed by Peter Adams Date: 2020.04.01 15:20:56 +02'00'". Below this, there is a checkbox labeled "Lock document after signing" and a "View Certificate Details" link. At the bottom, there is a password input field with a masked password "*****", a "Back" button, and a blue "Sign" button.

- f. Adobe will require you to save the pdf document before inserting the electronic signature.
- g. Your electronic signature is now inserted in the document.






 Signed and all signatures are valid.

**Peter
Adam
S**

Digitally
signed by
Peter Adams
Date:
2020.04.01
15:25:37
+02'00'

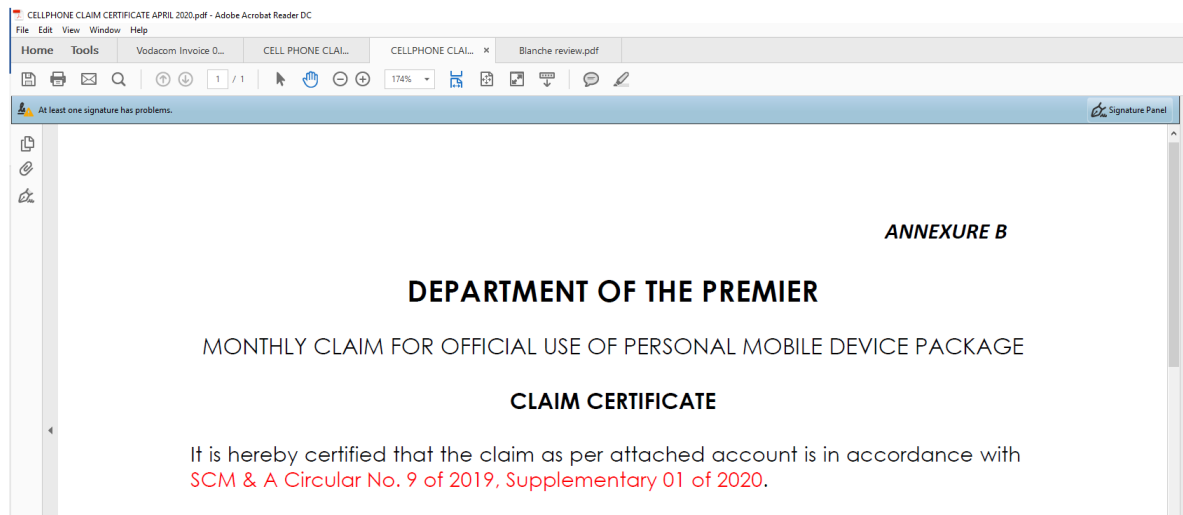
Welcome to this Course | Course Outlines | Modules | Resources

MS Teams Resources

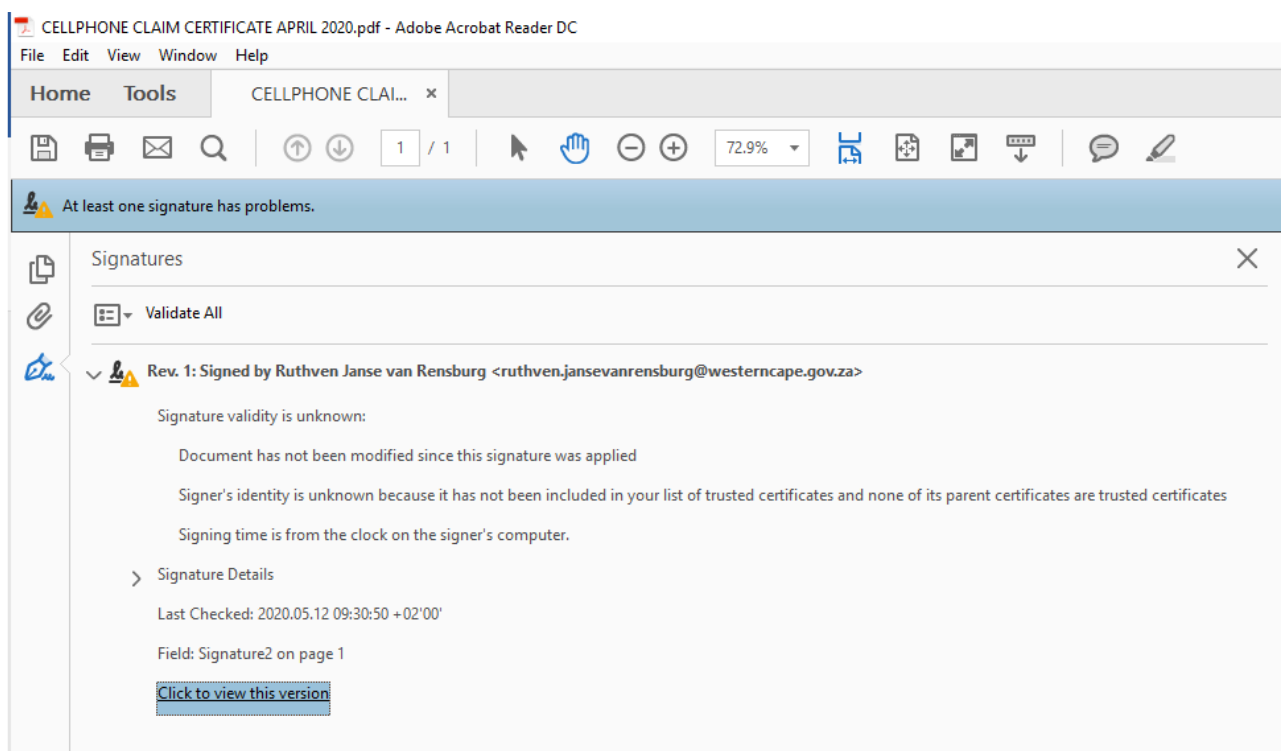
-  Glossary
-  Teams Quick Guide
-  How to Sign in
-  Teams PPT
-  Etiquette-in-Teams

Annexure B – How to validate Electronic Signatures in a PDF document

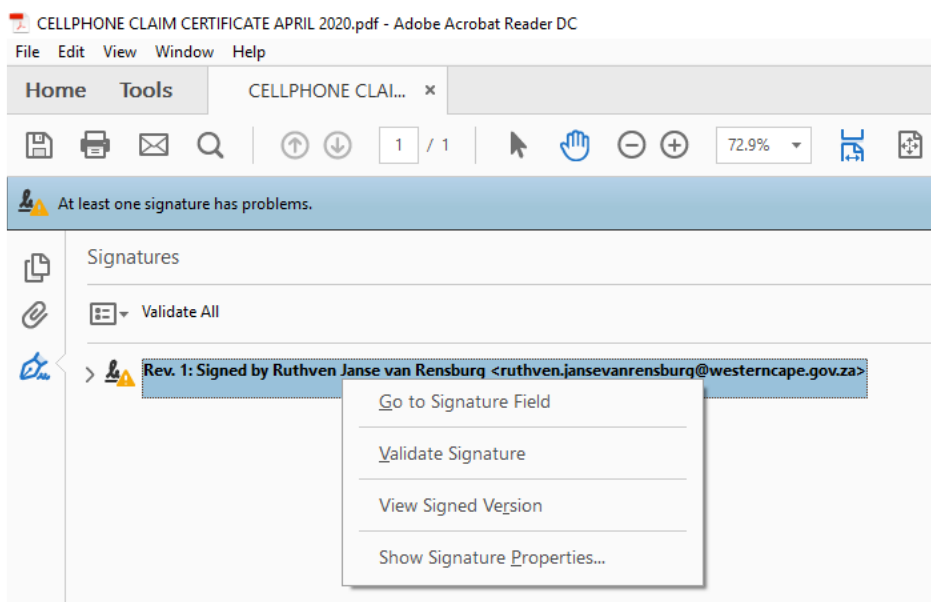
- a. When a pdf document with an electronic signature is received and the signature/s have not been added as a trusted signature, Adobe will indicate in the left corner that the signature/s has a problem and in the right corner give access to the Signature Panel:



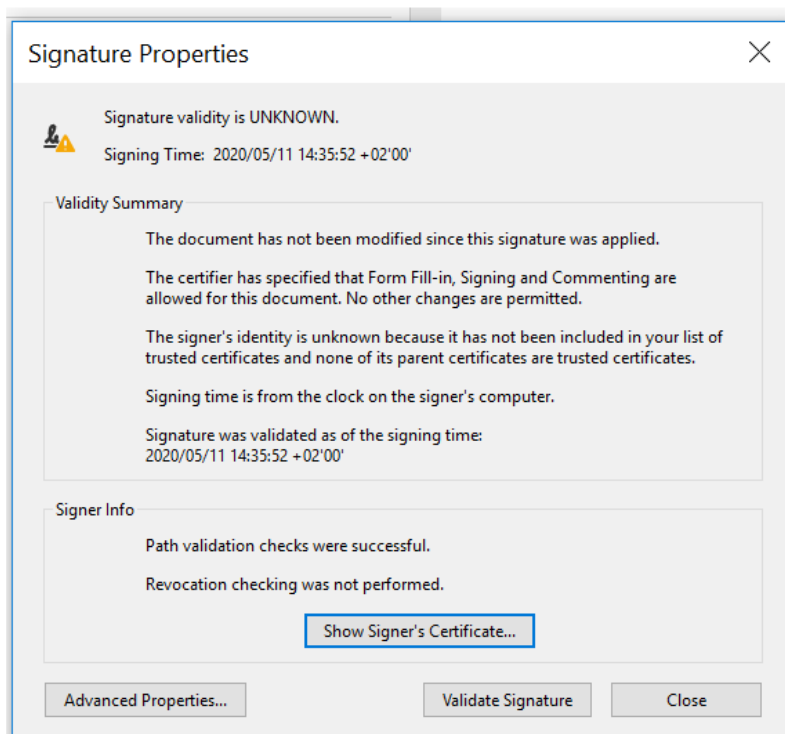
- b. Open the Signature Panel, and the detail relating to the validity of the signature will be presented:



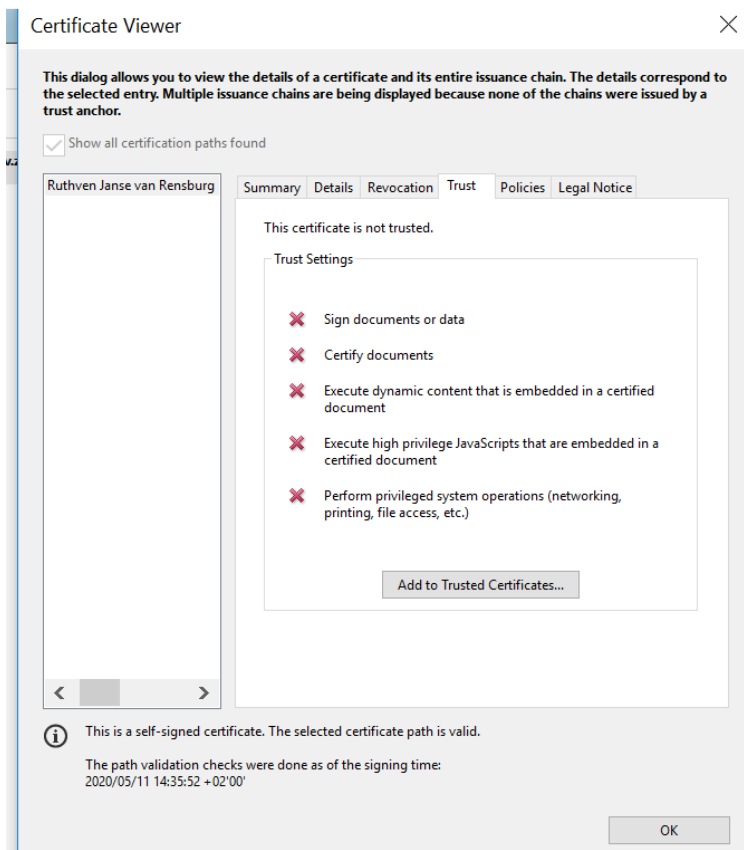
- c. The receiver then has to make sure that the signature was received from a trusted, authentic source, which in could include phoning/contacting the person/s. This is a once-off exercise per signature and once the particular signature is validated, will not be required again. It will also indicate when a signature from trusted people are then received from other sources than the computer where the trusted signature was created from.
- d. Once satisfied that the signature is from an authentic source, the following steps must be followed:
 - i. Right click on the signature and select "Show signature properties"



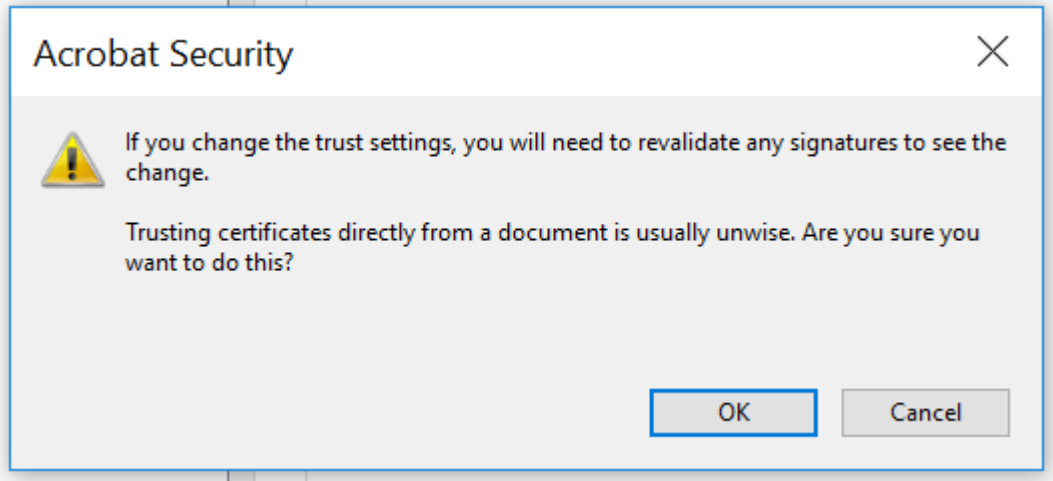
ii. Select "Show signer's certificate"



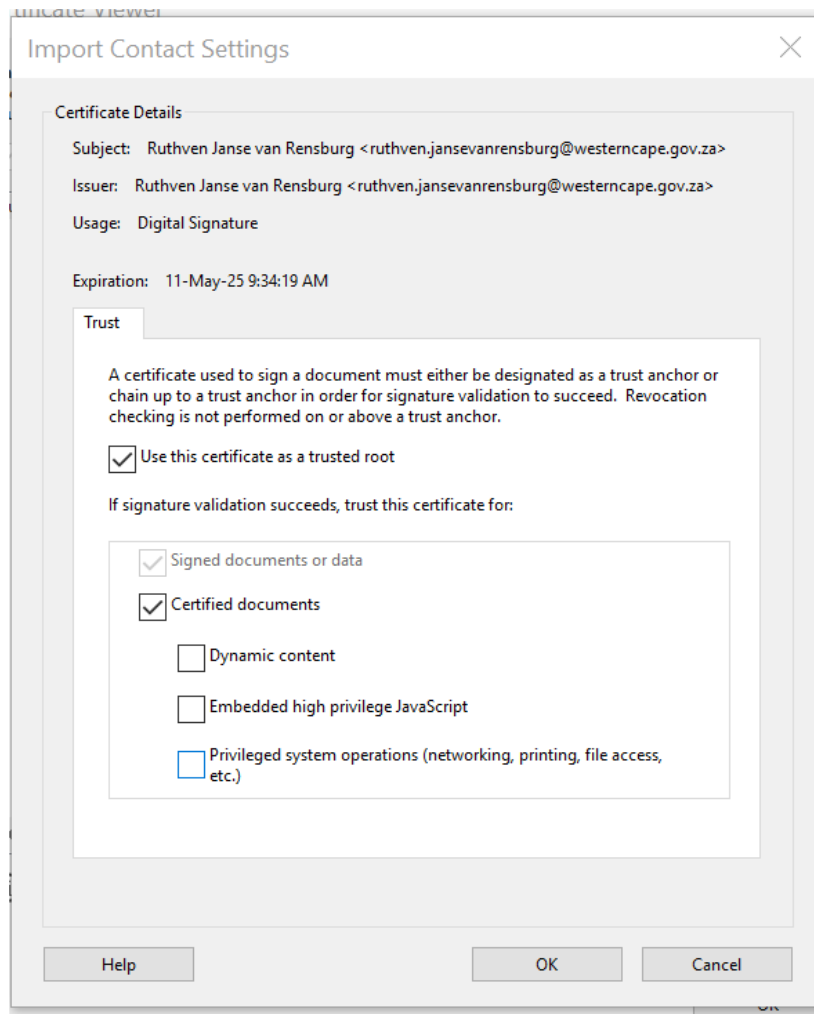
iii. Select the "Trust" tab and click on "Add to Trusted Certificates"



iv. Click "OK"

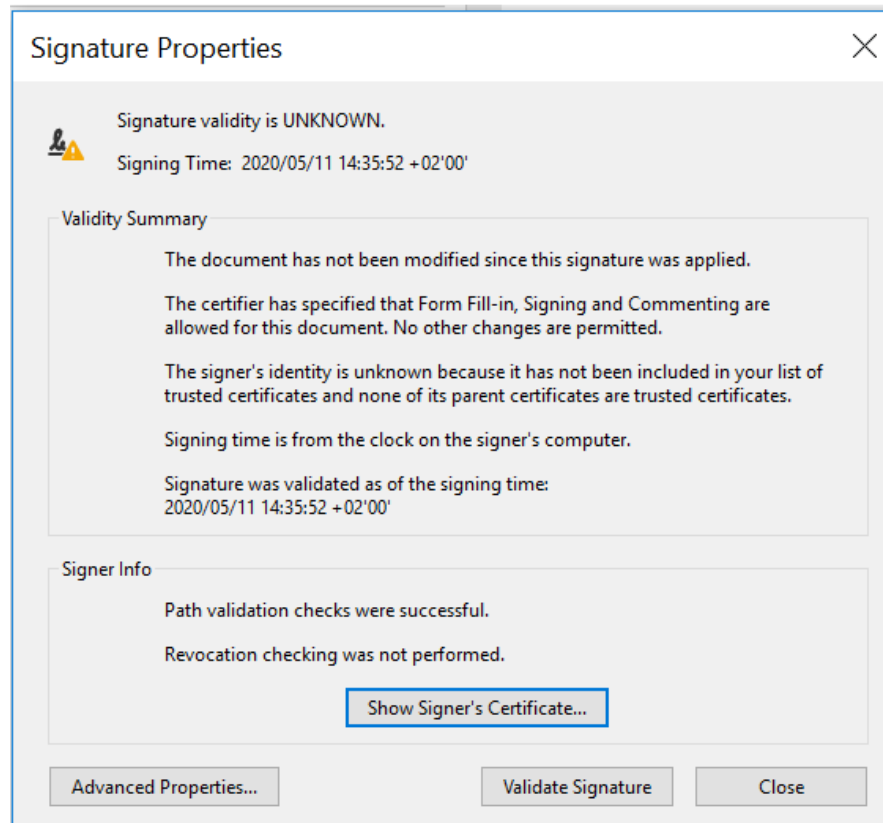


v. Place a check in "Use this certificate as a trusted root" and "Certified documents" and click "OK"

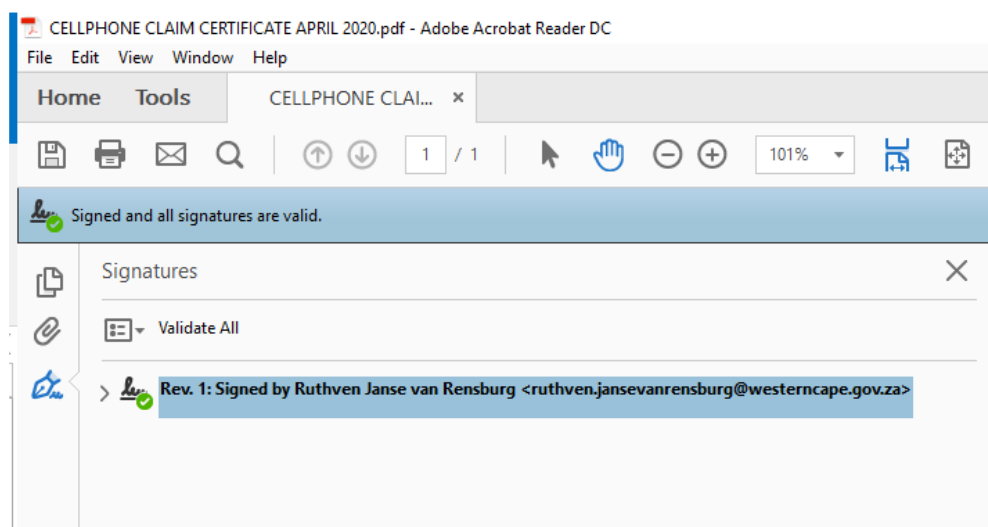


vi. Click "OK" on next screen

vii. Click on "validate signature" on next screen

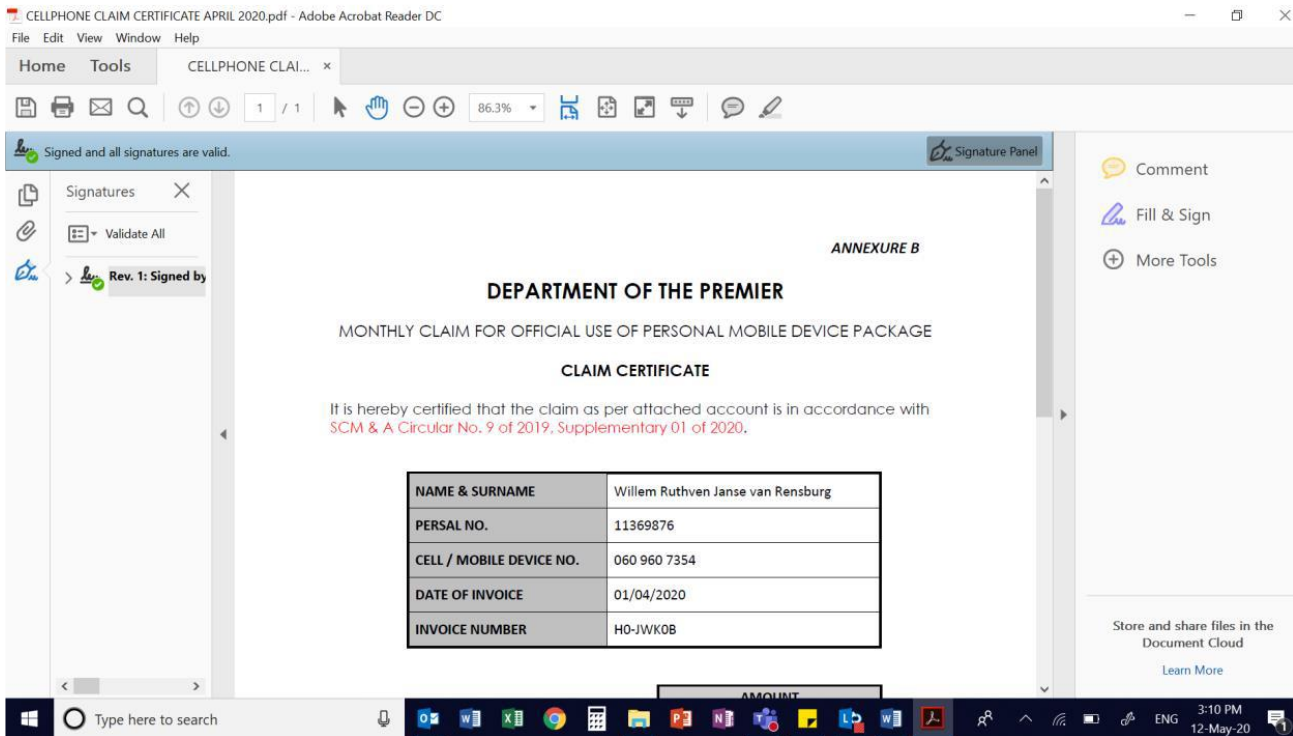


viii. The signature is now validated (green ticks) and each subsequent signature from the same person using the same machine is authenticated by Adobe and will appear as trusted.

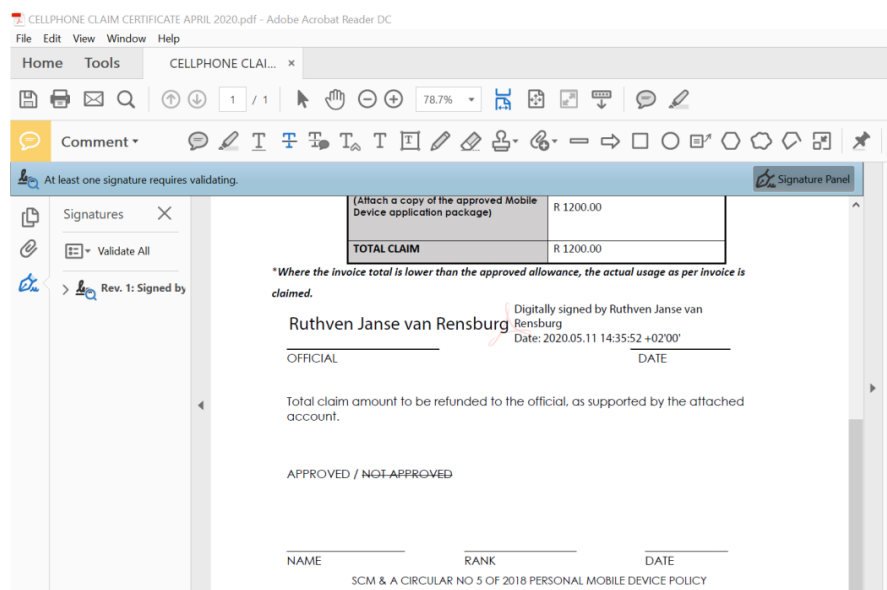


Annexure C – indication of agreement and appending of comments on pdf documents

- a. To indicate your support, recommendation or approval of a pdf document, open the document and go the required portion. Select “Comment” from the Tools menu



- b. Select the “Strikethrough Text” tool and delete the irrelevant portion before appending your signature.



- c. Should you want to add comments to the document, select the “Add Text Box” tool, draw a textbox on a suitable space in the document and add your comments before appending your signature.

CELLPHONE CLAIM CERTIFICATE APRIL 2020.pdf - Adobe Acrobat Reader DC

File Edit View Window Help

Home Tools CELLPHONE CLAI... x

78.7%

Comment

At least one signature requires validating. Signature Panel

(Attach a copy of the approved Mobile Device application package)	R 1200.00
TOTAL CLAIM	R 1200.00

**Where the invoice total is lower than the approved allowance, the actual usage as per invoice is claimed.*

Ruthven Janse van Rensburg Digitally signed by Ruthven Janse van Rensburg
Date: 2020.05.11 14:35:52 +02'00'

OFFICIAL _____ DATE _____

Total claim amount to be refunded to the official, as supported by the attached account.

APPROVED / NOT-APPROVED

I noted that:
X
X
X

NAME _____ RANK _____ DATE _____

SCM & A CIRCULAR NO 5 OF 2018 PERSONAL MOBILE DEVICE POLICY