

Tamil Nadu VAT Implementation, Validating Signature

User Guide – Validating Signature

April, 2016

Version 1.0

Notice

© 2016 Tata Consultancy Services Limited

This is a controlled document. Unauthorized access, copying, replication or usage for a purpose other than for which it is intended, are prohibited.

All trademarks that appear in the document have been used for identification purposes only and belong to their respective companies.



TATA CONSULTANCY SERVICES

Tamil Nadu VAT Implementation – Govt. ISU

Tata Consultancy Services Ltd

801/1001, Sakar-II, Near Ellisbridge, Off. Ashram Road,

AHMEDABAD – 380006

PF3020

Document Release Note

Notice No: TCS/TNVAT/Validating Signature for Digitally Signed Document/1.0

Customer: Department of Commercial Taxes, Tamil Nadu

Project: Tamil Nadu VAT Implementation

Document Details

Name	Version Number	Description
Blueprint - Validating Signature for Digitally Signed Document – Tamil Nadu VAT Implementation – Validating Signature for Digitally Signed Document	1.0	User guideline for Validating Signature for Digitally Signed Document/Notice/Certificate

Revision Details

Action Taken (add/del/change)	Previous number	page	New page number	Revision description

Change Register serial numbers covered:

The documents or revised pages are subject to document control.

Please keep them up-to-date using the release notices from the distributor of the document.

These are confidential documents. Unauthorized access or copying is prohibited.

Approved by:

Authorized by:

Date:

Date:

PF2060C

Document Revision List

Customer: Department of Commercial Taxes, Tamil Nadu

Project: Tamil Nadu VAT Implementation

Document Name: Blueprint – Validating Signature for Digitally Signed Document

Release Notice Reference (for release)

Revision Number	Revision Date	Revision Description	Page Number	Previous Page Number	Action Taken	Addenda / New Page	Release Notice Reference

Conten

1. Introduction.....	7
2. Validating the signature: For department/Dealer:.....	8
3. To validate the signature follow the below procedure.....	9
4. Conclusion.....	14

List of FiguresY

Figure 1 : Authority Signature	8
Figure 2 : Validate Signature	9
Figure 3 : Signature Validation status	9
Figure 4 : Signature properties	10
Figure 5 : Signer's Certificate	10
Figure 6 : Trust Settings	11
Figure 7 : Security Screen Pop up	11
Figure 8 : Certificate Details	12
Figure 9 : Validating Signature	13
Figure 10 : The Green tick mark indicating the digital signature is valid	13

1. Introduction

When you receive a signed document, you may need to validate its signature to verify the signer and the signed content. Depending on how you have configured your application, validation may occur automatically. Signature validity is determined by checking the authenticity of the signature's digital ID certificate status and document integrity.

Authenticity verification confirms that the signer's certificate or its parent certificates exist in the validating list of trusted identities. It also confirms whether the signing certificate is valid based on the user's Acrobat or Reader configuration.

Document integrity verification confirms whether the signed content changed after it was signed. If content changes document integrity verification confirms whether the content changed in a manner permitted by the signer.

This document will guide how to validate the signature in the digitally signed RC. Dealer should refer below screens to validate the Signature.

Also after right clicking the document, validate signature should come. Else please save the document and open the same again in folder. Then validate signature will come and can validate using below steps.

2. Validating the signature: For department/Dealer:

If dealer download the RC from Portal, the signature of Signing Authority will be as shown in the below figure for the first time users.

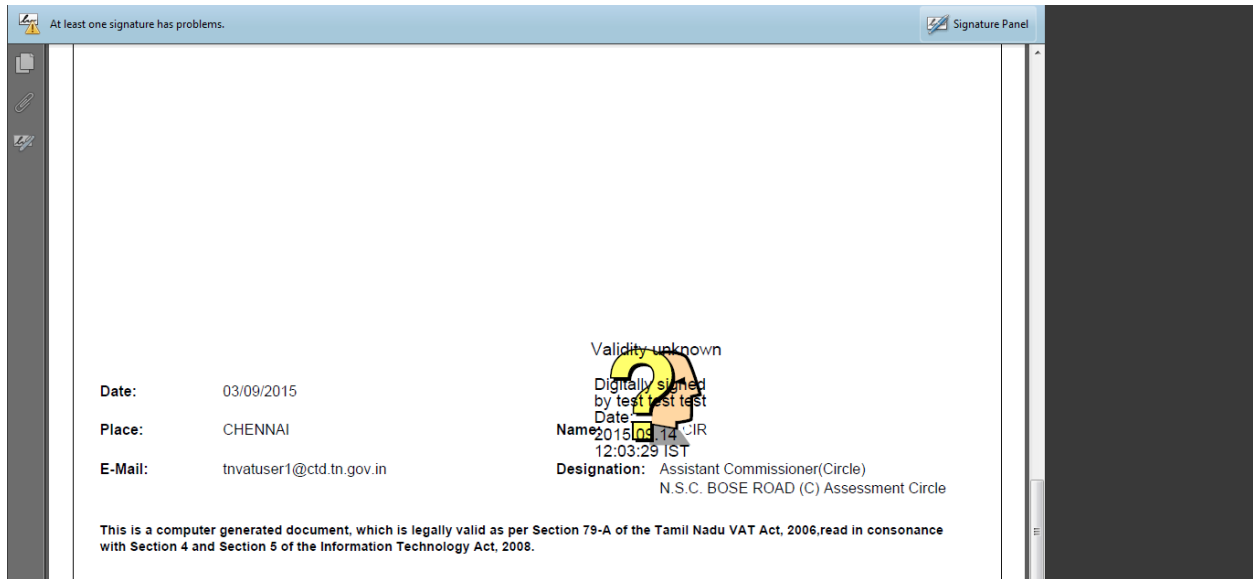


Figure 1 : Authority Signature

3. To validate the signature follow the below procedure

1. Step 1- Right click on the signature and select “Validate Signature” option.

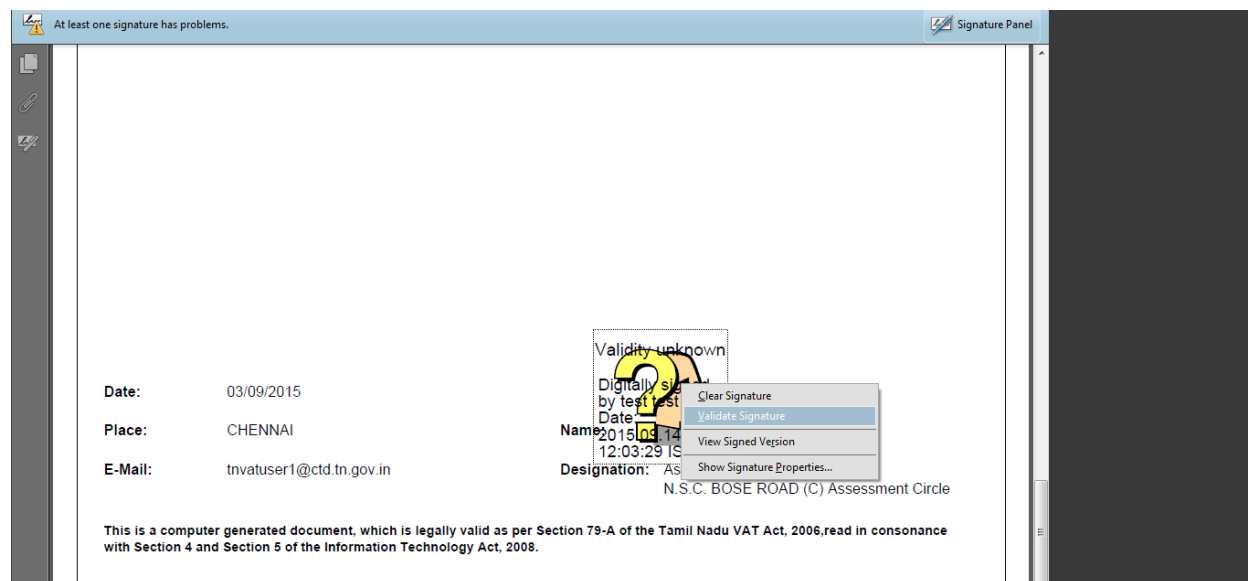


Figure 2 : Validate Signature

2. Step 2- After selecting the Validate Signature option a pop up will appear stating Signature Properties. Then click Signature Properties for further proceedings.

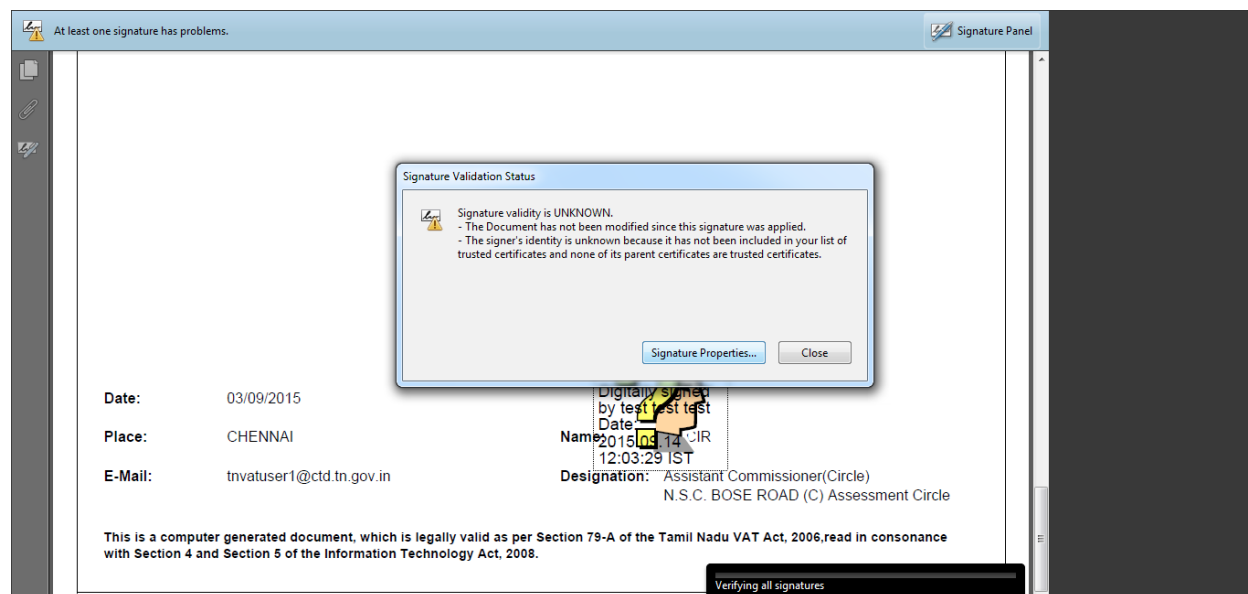


Figure 3 : Signature Validation status

3. Step 3-Once the Signature properties are clicked another pop up will appear, in which click “Show Signer’s Certificate”.

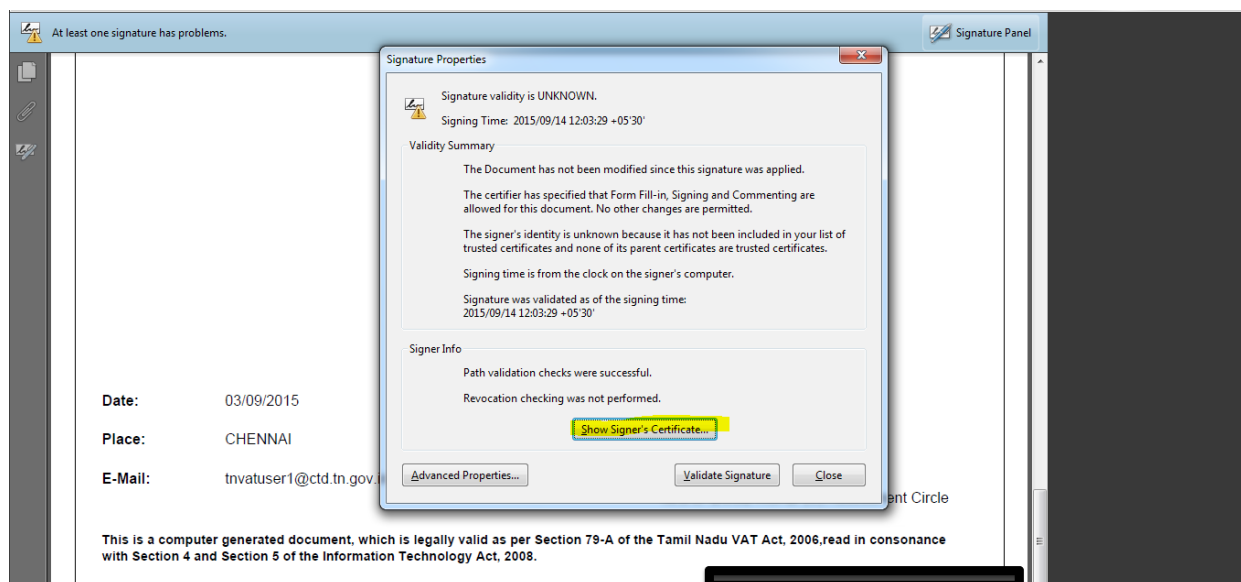


Figure 4 : Signature properties

4. Step 4- After selecting the above option a new dialog box will appear which allows you to view the details of a certificate .Once the dialog box opens go to “Trust” tab.

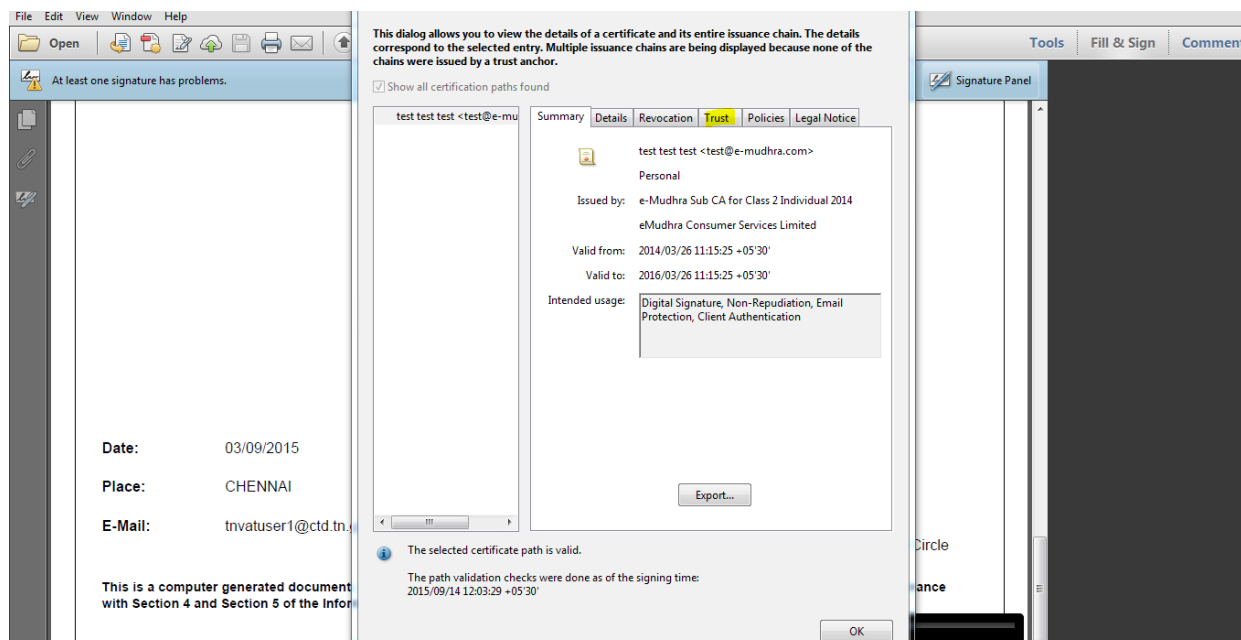


Figure 5 : Signer’s Certificate

5. Step 5- Next click on “Add to Trusted Certificates”.

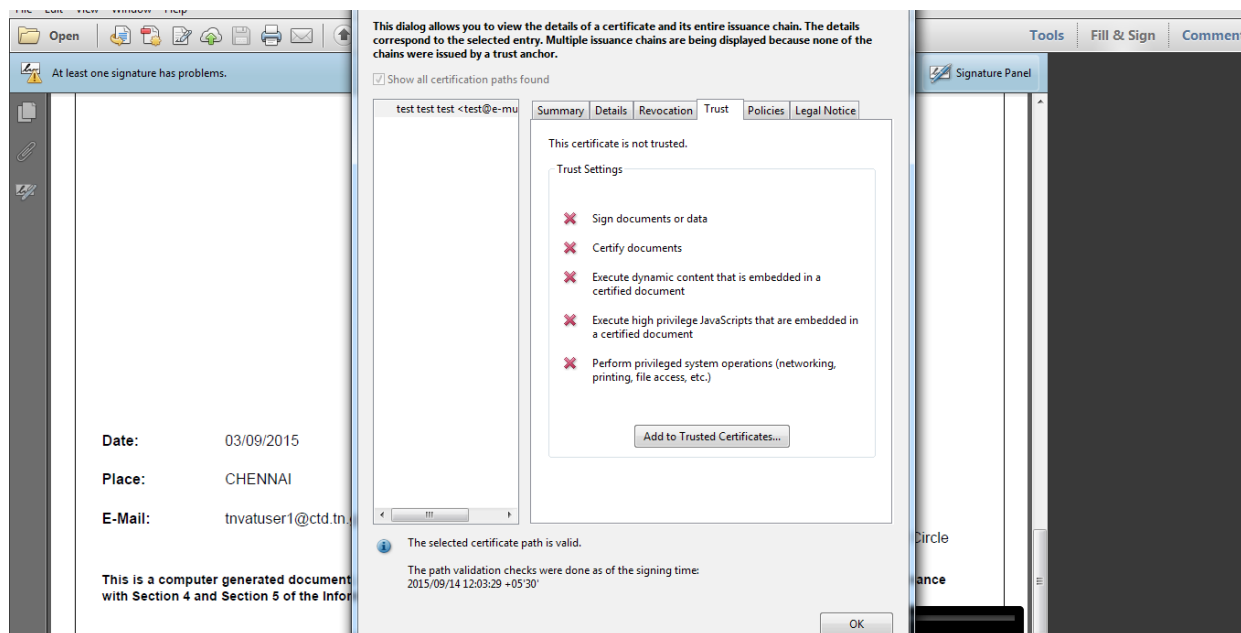


Figure 6 : Trust Settings

6. Step 6- After adding the certificate to the Trusted Certificate click on the OK button from the pop up appeared on screen.

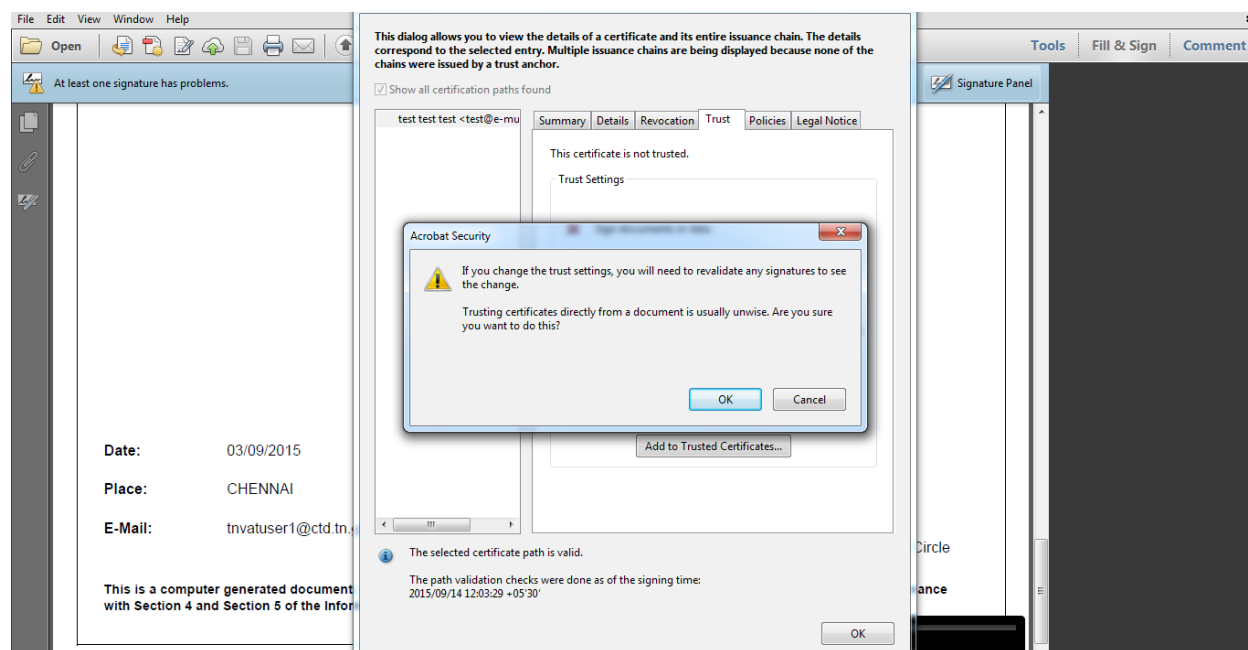


Figure 7 : Security Screen Pop up

7. Step 7- Once the adding process is completed tick the box stating that 'Use this certificate as a trusted root' and then click the Ok button.

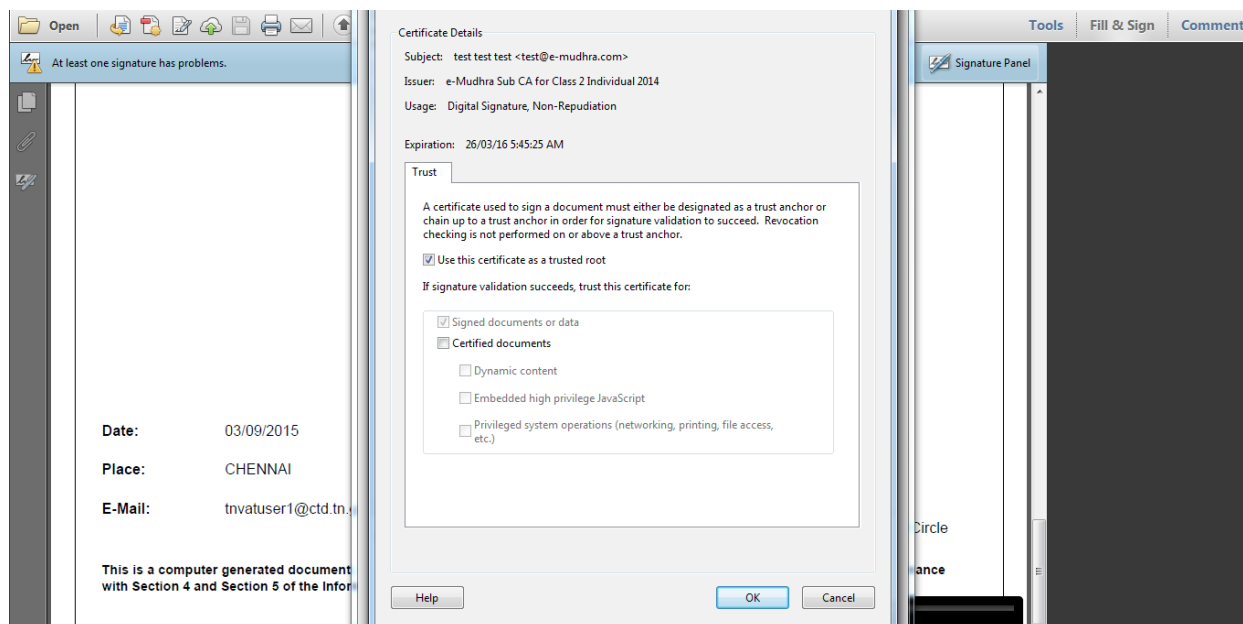


Figure 8 : Certificate Details

8. Step 8- After all the above process is being completed finally click "Validate Signature" and close.

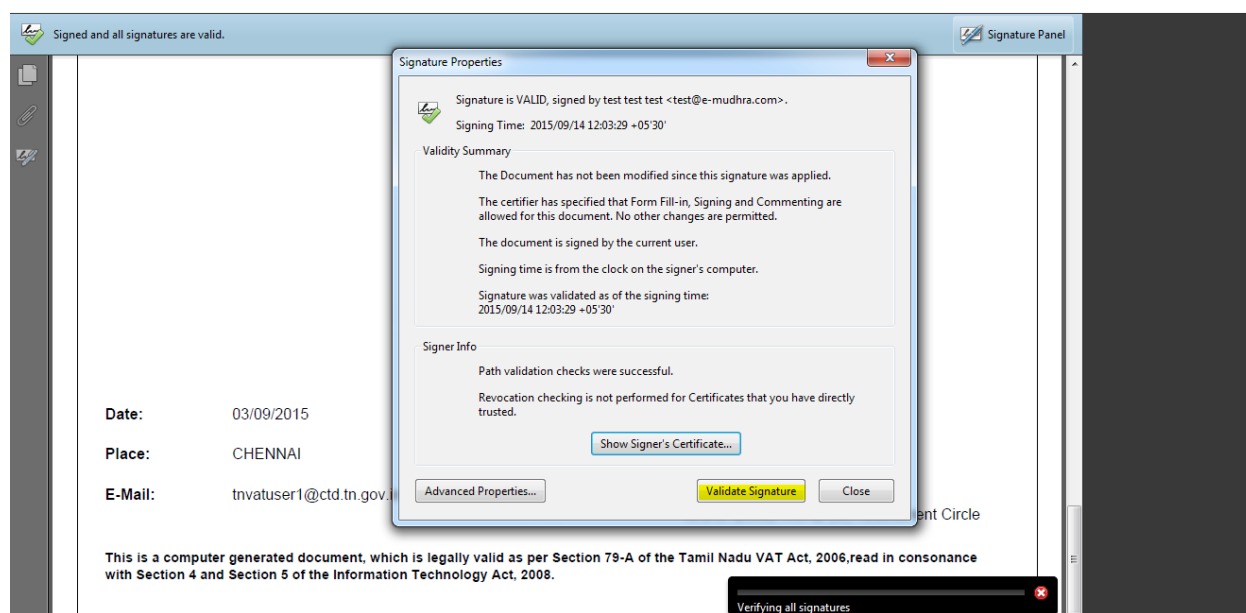


Figure 9 : Validating Signature

9. After the Validate Signature option is selected there a green tick mark will be shown. The Green tick mark as shown in the below figure should be there indicating that the digital signature is valid.

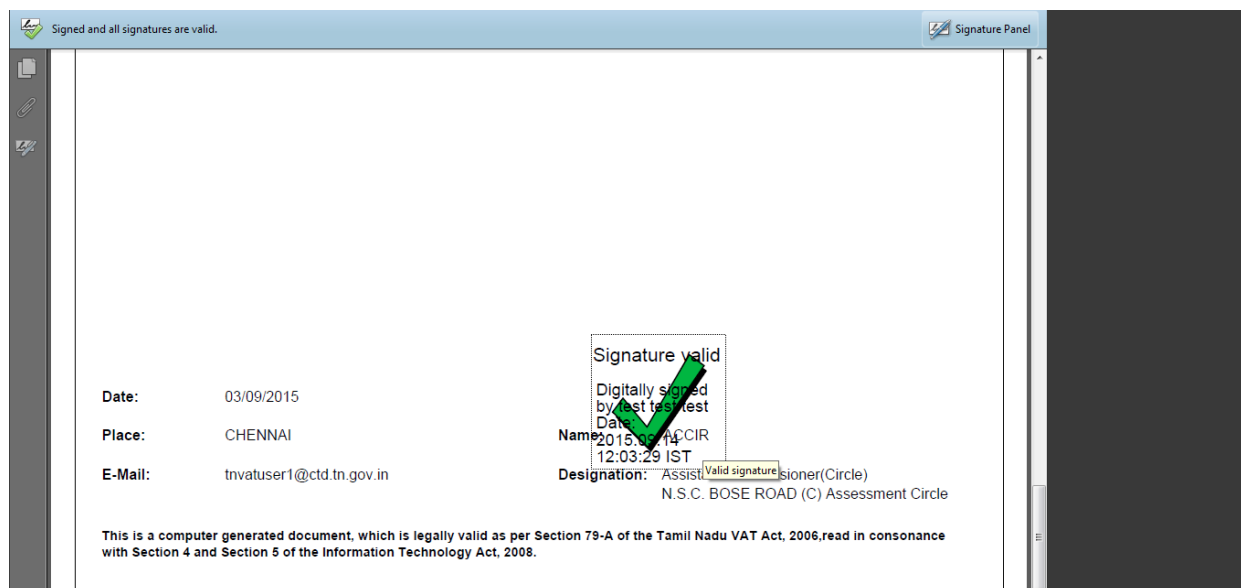


Figure 10 : The Green tick mark indicating the digital signature is valid

4. Conclusion

In this document we demonstrated how to validate signature. Signature should be validated for the first time in each system where the user downloads the documents. If once the signature is validated in a system for the subsequent downloads of document the signature will be validated automatically.