MDOT
Michigan Department of Transportation

OFFICE MEMORANDUM

DATE: February 28, 2012

TO: Region Engineers
Region Associate Operations Engineers
Region Construction Engineers
TSC Managers
TSC Construction Engineers

FROM: Gregory C. Johnson, P.E.
Chief Operations Officer

Randy R. Van Portfliet, P.E.
Bureau Director of Field Services

SUBJECT: Bureau of Highway Instructional Memorandum 2012-02
Digitally Encrypted Electronic Signatures

The Michigan Attorney General's office, in concurrence of the Federal Highway Administration, has issued a decision authorizing the Michigan Department of Transportation (MDOT) to use and accept digitally encrypted electronic signatures. These digital signatures are not scanned copies of handwritten signatures or faxed copies of a handwritten signature, but are a secure electronic "object" that is embedded into the electronic PDF document by the signer with their unique password, identity, and the date/time digitally encrypted into the electronic document.

Signatures are commonly used to authenticate documents. When you sign a paper document, you are authenticating its contents. Similarly, digital electronic signatures are used to authenticate the contents of electronic documents. These electronic signatures are unique to the signer and often provide enhanced verification of the signer's identity.

It has been legally acceptable to use digital electronic signatures for interstate and foreign commerce since passing the Electronic Signatures in Global and National Commerce Act (E-SIGN Act) on June 30, 2000, by the United States Congress. The act ensures the validity and legal effect of contracts entered into electronically and prevents these contracts from being treated differently from pen and paper equivalent contracts. This means that an electronic document with a validated digital electronic signature must be legally treated in the same manner as a paper document with an original handwritten signature.

To digitally sign a document, you must first have a digital identification (ID). This unique identifier can be obtained from various certification authorities, but MDOT will primarily use the Adobe Acrobat software. A digital signature can be placed anywhere on a document via the "Sign" toolbar icon in Adobe Acrobat software. Once a user has established their unique digital signature ID, digitally signing documents takes only seconds. The user must enter their unique

password in order to sign the document. The software will then embed their digitally encrypted electronic signature into the electronic PDF file. The electronic document is then a signed original and carries the exact same significance as a handwritten signature on a paper document.

Document Certification

The option of document certification should only be used when there is only going to be a single signature on a form or document. Certifying a document allows the document creator to ensure that no changes will be made to the document after signing. If any changes are made to a certified document after a certifying signature they will be very apparent and prevent anyone else from validating said document. Thus documents which require multiple signatures, like contract modifications, should never use the certify option. Certified documents would apply more to documents such as single signature letters and forms where the signer has to ensure that no data is changed, added or deleted from the original document.

Signature Validation

The use of a digital signature has the same legal validity as a traditional handwritten signature using ink on paper. However, since it is possible to create a digital signature ID with anyone's information in it, there are required signature validation procedures. Similar to how handwritten signatures must be verified, it is the responsibility of the recipient of an electronically signed document to confirm the identity of the signer/sender before the electronic signature may be considered valid. The federal government outlines a process for confirming signature identity that involves a minimum of two separate methods. The first (and typical) method is verification of the identity of the signer. If the document was supposed to be signed by a certain person and their name appears, then this requirement has been met. Secondly, it is common to identify the method/source of delivery. If the document arrives from the signers unique email address then the second validation method criterion has also been met. The following are questions/criteria to be answered by the person validating the electronic signature:

1. Did the document arrive from the signer's company/agency e-mail account or from an unknown email address?
2. Was it an electronic signature from the expected signer that has been previously validated?

Strange documents, new signatures not previously verified, documents from unknown email addresses, etc. should be verified by contacting the approver at their place of business (usually by telephone) to confirm the new digital ID and/or the document. Alternative approvers/signers of documents or unique delivery methods can always be pre-arranged. If approvers or delivery methods differ from the previously agreed upon people or methods, the recipient of the digitally signed document must contact the sender to validate their identity. When using electronic signatures, it is the responsibility of the recipient of the document to verify the electronic signature on the document before the document can be considered valid or provided to another entity for review and signature. These simple validation steps will significantly reduce any potential risks associated with electronic signatures.

Adobe Acrobat software has an integrated validation feature, therefore, once a user has validated (see Appendix) the sender of a digital signature, this sender will not need to be validated again. The effort required to validate electronic signatures will diminish as a users list of trusted digital signatures expands. Adobe Acrobat software also provides visual cues for validation. If the sender has not been previously verified, their digital electronic signature will have a grey colored question mark over it. Once a person's unique digital electronic signature has been validated and added to the trusted identity list, the Adobe Acrobat software will then always show a validated green-colored check mark next to that person's unique electronic signature. New or un-verified electronic signatures will continue to have a grey-colored question mark next to the sender's electronic signature until the validation step has been completed. The Adobe Acrobat software also allows you to share your previously validated electronic signatures with others through a simple e-mail process in the software.

One important issue to consider when utilizing digital electronic signatures is that any document that requires multiple signatures (i.e. contract modifications) must be either signed entirely in pen/ink on paper or signed entirely with all parties using electronic signatures. It is not possible to mix the two methods of signature as paper printouts of digital signatures are meaningless and scanning handwritten signatures into a PDF document is not currently acceptable to the Michigan Attorney General's office as a legal signature.

MDOT Electronic Signature Procedures

Digital electronic signatures will now be accepted wherever a signature is required on an MDOT document. The Michigan Attorney General's decision did not limit the types of documents MDOT may utilize digital electronic signatures on; however, it does require that new use of documents or processes be first cleared with their office. MDOT will continue to add new documents and processes to the growing list of those approved for electronic signature use; however, if a new document or procedure needs to be added, it should be submitted to the MDOT E-sign team in the Construction Field Services Division, Construction Contracts Unit. The use of electronic signatures throughout MDOT is encouraged and can lead to significant monetary, resource, and time savings for all involved. New forms, innovative ideas, and process improvements are encouraged to be submitted for approval.

Whether to sign by hand or electronically will continue to be optional for most documents; however, some documents or processes may eventually begin to require the use of electronic signatures due to the significant savings in material, time, and labor. Any changes to MDOT procedures that would require mandatory use of electronic signatures will be noted in the documented MDOT procedures.

MDOT currently only authorizes the use of the PKCS#12 Digital Signature ID. This international standard method of digital signature encryption requires the signer to enter their unique password each time they sign a document electronically. This method is also compatible with most common MDOT software such as Adobe Acrobat and Microsoft Office. Other types of digital IDs may also be approved in the future, but these IDs will be required to meet the minimum security and encryption protocols of the PKCS#12 IDs. Digital signature files are

transportable to other machines, but there is no password reset feature, so if you forget your digital signature password you will have to create a new digital signature. PKCS#12 digital signature IDs are good for a period of four years and the owner can change the password manually, but a user will not be prompted to change passwords until the ID expires.

MDOT is also working on integration of electronic signatures on portable devices. While Adobe Acrobat software does not currently support the use of electronic signatures on portable devices, there are several other software applications that do meet the MDOT security standards which allow regular PDF files to be digitally signed using portable devices. These applications and software are still being evaluated by the E-Sign team and the Department of Technology, Management and Budget for incorporation into MDOT processes. Until new portable device digital signature standard procedures are published, the use of these third party software applications will have to be submitted to the E-Sign team for evaluation on a case by case basis.

It is also important to note that for records retention and archiving purposes whenever digital electronic signatures are used on documents, the electronic file (adobe PDF file) is considered the legal original document. Printouts of documents containing digital signatures are only copies, so the electronic files containing digital electronic signatures must be retained and follow the relevant approved records retention procedures. Proper retention, archiving, and storage of the electronic files must be considered when using digital electronic signatures. MDOT will address the records storage issue through the requirement that all electronically signed documents must be placed in the project directory in the ProjectWise document management program.

Digital signatures are unique to each person. Under no circumstances may an electronic signature or password be used by another person. Signature authority may sometimes be allowed to be delegated to another party for certain procedures, but such delegation must be done by the designated party utilizing their own unique digital electronic signature on the document with the signature reason noting "Signed For *Persons Name*". If a person is found to have been committing fraud by using another person's digital electronic signature, the offending party will lose their electronic signature privileges and the case will be referred to the applicable authorities and/or the respective oversight group (pre-qualification committees, Attorney General, etc.). The fraudulent use of electronic signatures will be considered a significant violation and be subject to severe repercussions.

The use of PDF forms with pre-established fillable areas for electronic signatures on standard forms and documents is acceptable and encouraged for use within MDOT. The use of pre-established signature areas on other documents is not required. A significant advantage to using electronic signatures is that they may be placed on documents wherever the signer desires. When not using prepared forms with pre-established signature areas, the signer should take care to consider signature placement on the document with regard to clarity and readability. For instance, if the signer creates a signature placement box that is too small, the signature may not be readable, or if the signature placement box is drawn too large, it may encroach upon other areas of the document.

MDOT electronic signature instructions are attached to this BOH IM.

MDOT Style Guidelines for Use of Electronic Signatures

MDOT electronic signatures will need to conform to the following style guidelines:

Adobe Software digital signature option selections:

- Graphic options shall be:
  - "Name"
  - Or "Imported Graphic" (as outlined below)

- Configure text shall be configured as:
  - Uncheck the adobe "logo"
  - Required to include: ("Name", "Date", "Location" and "Reason")
  - Optional "Distinguished Name" (includes job title)
  - Optional for "labels"

- Text properties:
  - "left to right"

You may have multiple digital signature files configured for different purposes. It is even possible to configure a digital signature with an "Imported Graphic" (option noted above) containing an image of your scanned written signature or a scan of a professional license stamp. These are acceptable, but written signature images are not required and non-business related graphics are not acceptable.

Please share this information with consultants and local agencies within your area.

Gregory C. Johnson, P.E.

Digitally signed by Gregory C. Johnson, P. E.
DN: cn=Gregory C. Johnson, P.E., o=MDOT, ou=Executive, email=johnsong2@michigan.gov, c=US
Date: 2012.02.28 10:59:39 -05'00'

Chief Operations Officer

Bureau Director of Field Services

FHWA Approval 12-27-11

Attachment

BOFS:CFS:MA:lw

Index: Operations Review

cc:	CFS Division Staff	B. Wieferich	J. Adamini	APAM	MCA
	M. Chaput	C. Rademacher	L. Wieber	CRAM	MCPA
	B. O'Brien	P. Collins	ACEC	FHWA	MITA
	M. DeLong	D. Wedley	ACM	MAA	MML

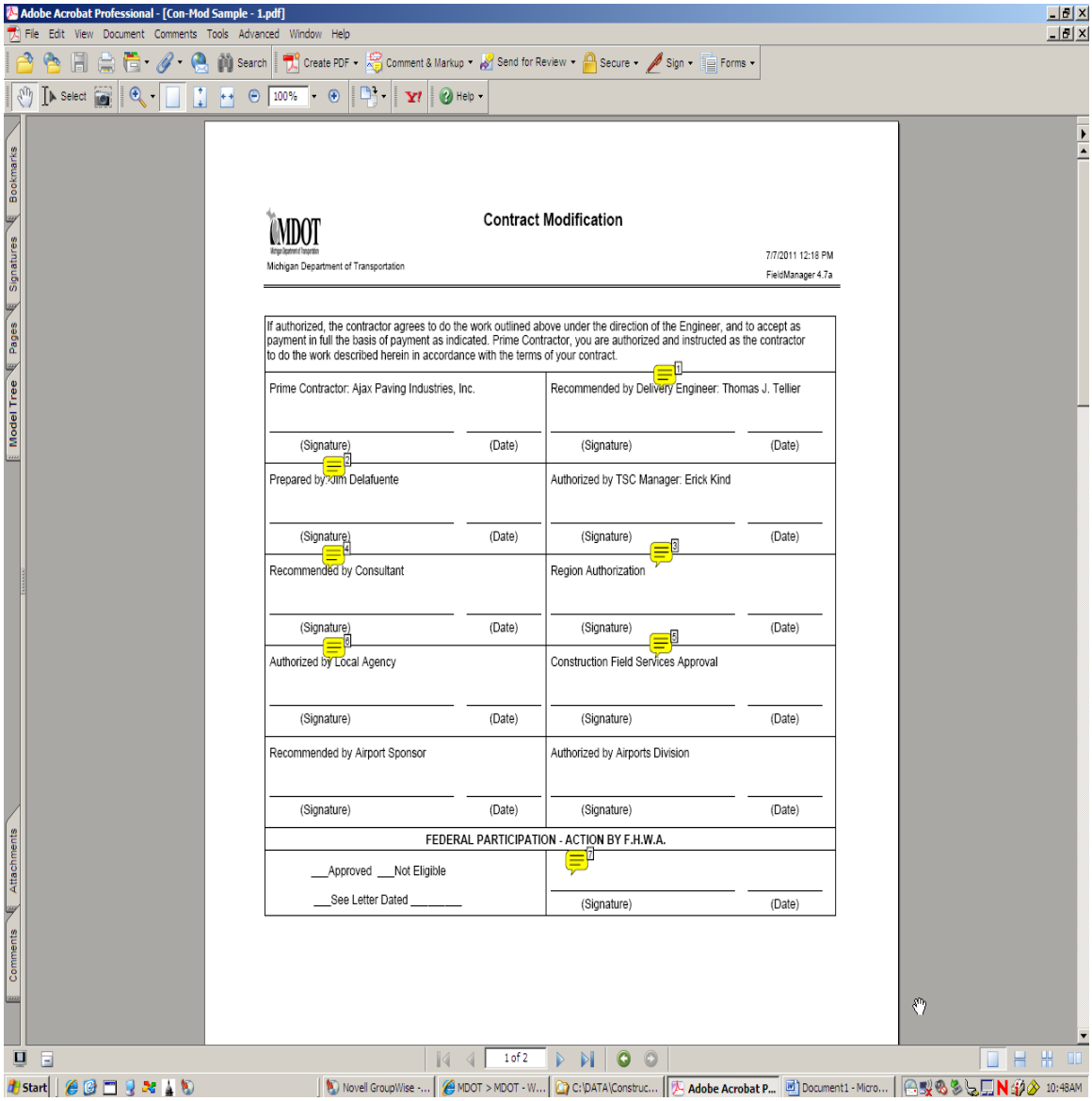
MDOT DIGITAL ELECTRONIC SIGNATURE INSTRUCTIONS

Updated February 2012

Table of Contents:

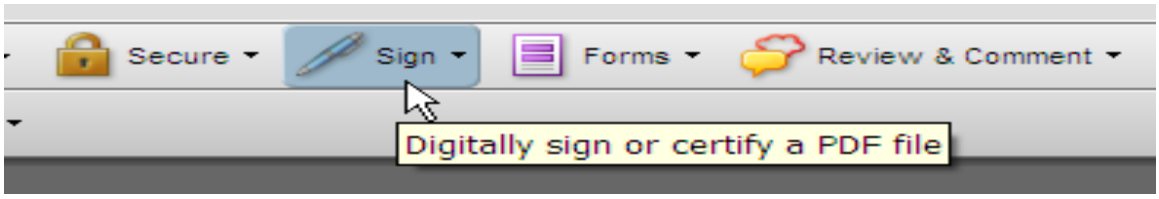
Step #1 – Document

Electronic document is received in a format that was scanned into a PDF file or printed to PDF that requires an electronic signature. Below is what an Adobe PDF file will look like. This one is a Field Manager Contract Modification approval.



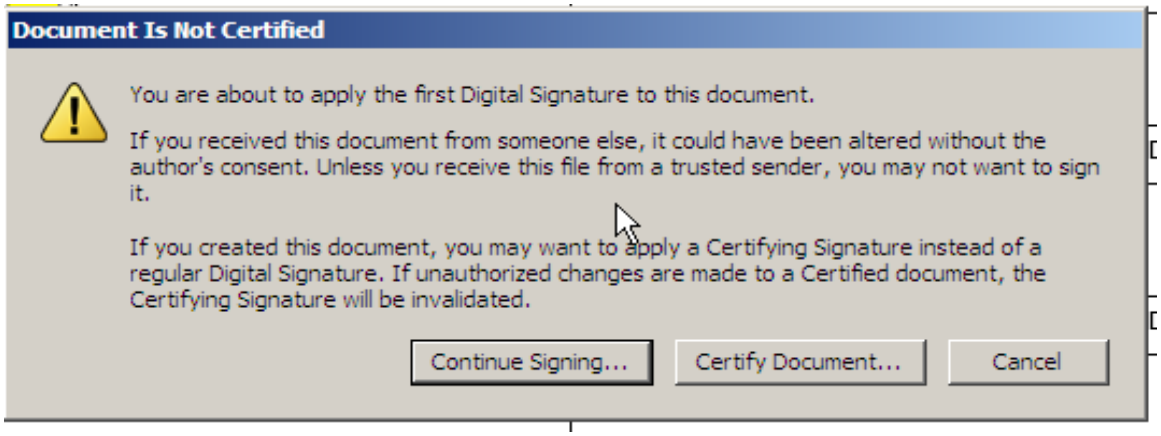
Step #2 – Signatures

After review and approval of document contents and when you are ready to sign the document, just go to the “Sign” icon in the upper right end of the adobe menu or use the pull down menus.



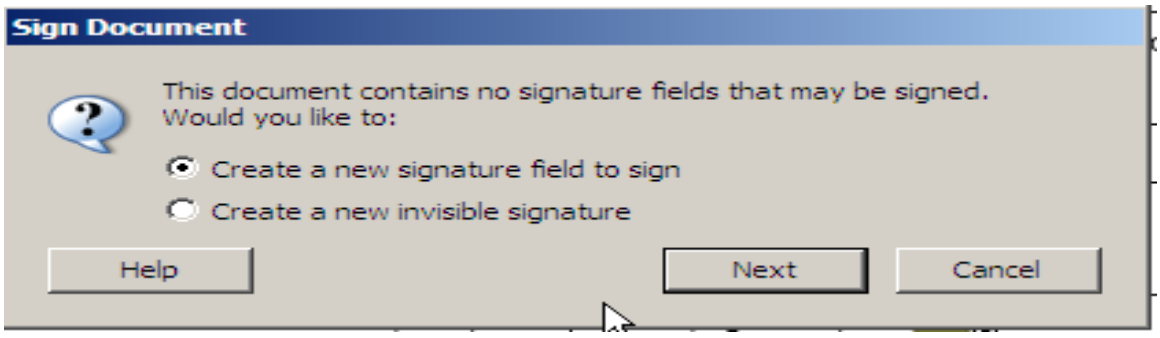
Step #3 – Document Certified

This question will not always appear, but if it does you are probably the first person to sign the document. If you choose the “Certify Document” option then any changes made to the document after that point (including another person signing) will remove your certifying signature. So in the case of a multiple signature document like a contract modification, use the “Continue Signing” option.



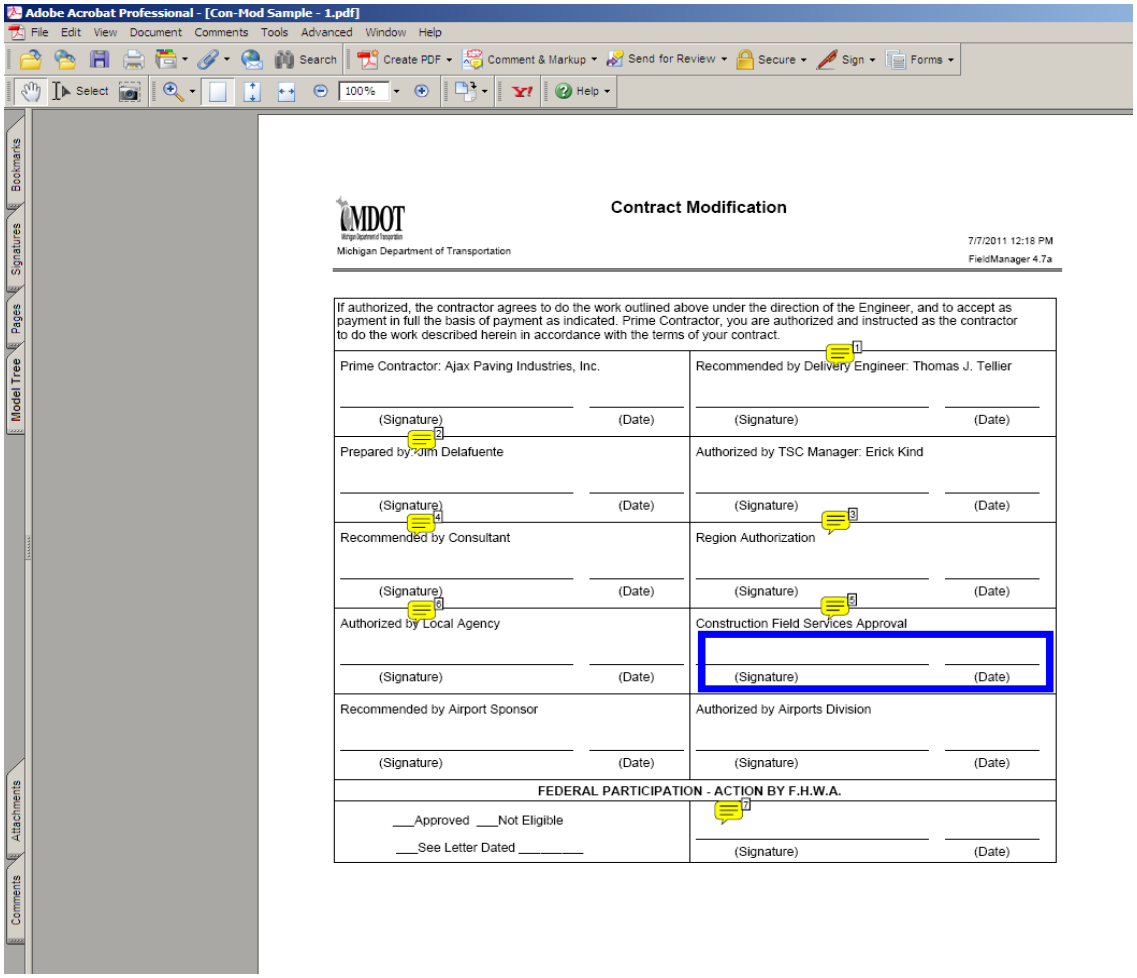
Step #4 – Signature Field

This choice relates to documents that may have been pre-setup with signature areas like standard forms or if you wish to manually indicate where you will sign the document.



Step #5 – Create Signature Field

Draw a rectangle box in the area you intend to place your signature.



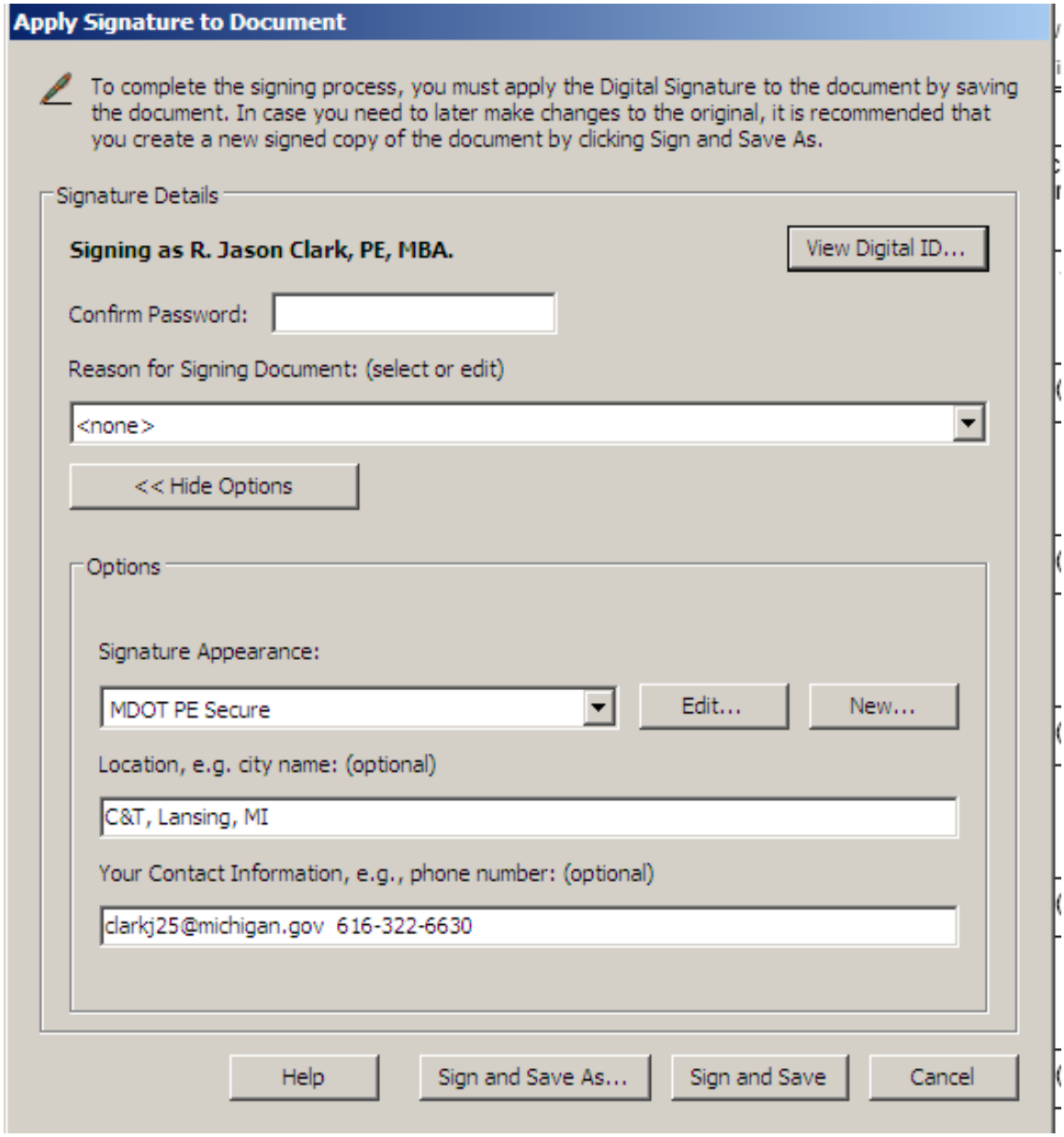
Step #6 – Choose Digital Signature

If you already have a digital signature, select it from the list and go to Step #7. If you do not have a digital signature already created, you will need to create one. (See Appendix A for setting up new digital electronic signatures.)

Step #7 – Apply Signature to Document

Enter your password, then type in your customized reason for signing the document (or use pull down menu for standard reasons). Next, confirm the contact info and then go to step #8 for more on signature appearance. (If signing for someone else, it is required to type *"signing for ??"* in the Reason for Signing Document area.)

Adobe Reader Version 7

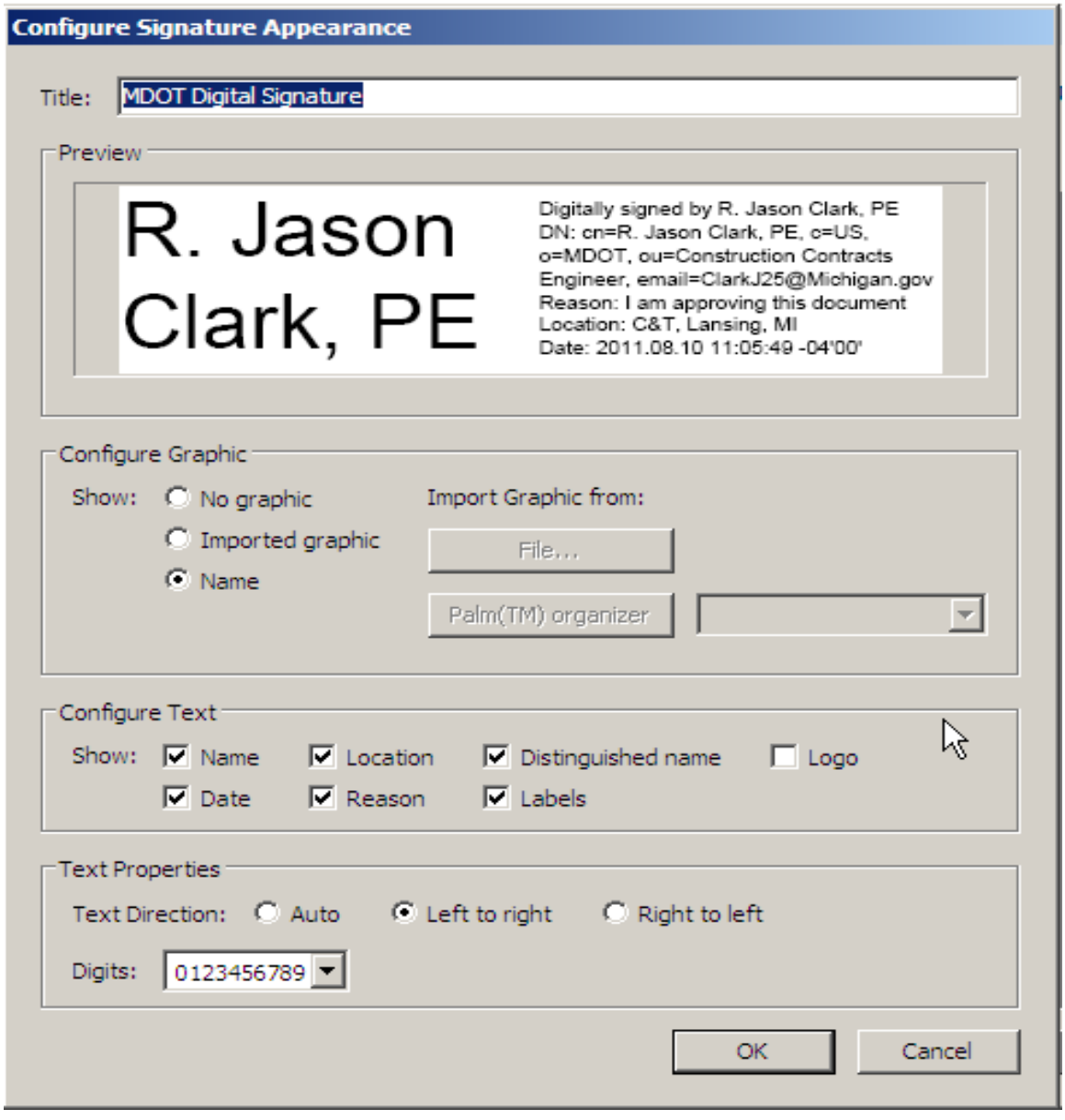


Adobe Reader Version 8

Step #8 – Signature Appearance

MDOT standards are still being developed, but for now all signatures must include the Configure Graphic option of “name” and the Configure Text options of “name”, “location”, “date”, and “reason”. Initial primary requirement is to be sure to uncheck the box next to “logo” which places a copyrighted Adobe logo on your signature if you do not uncheck that box.

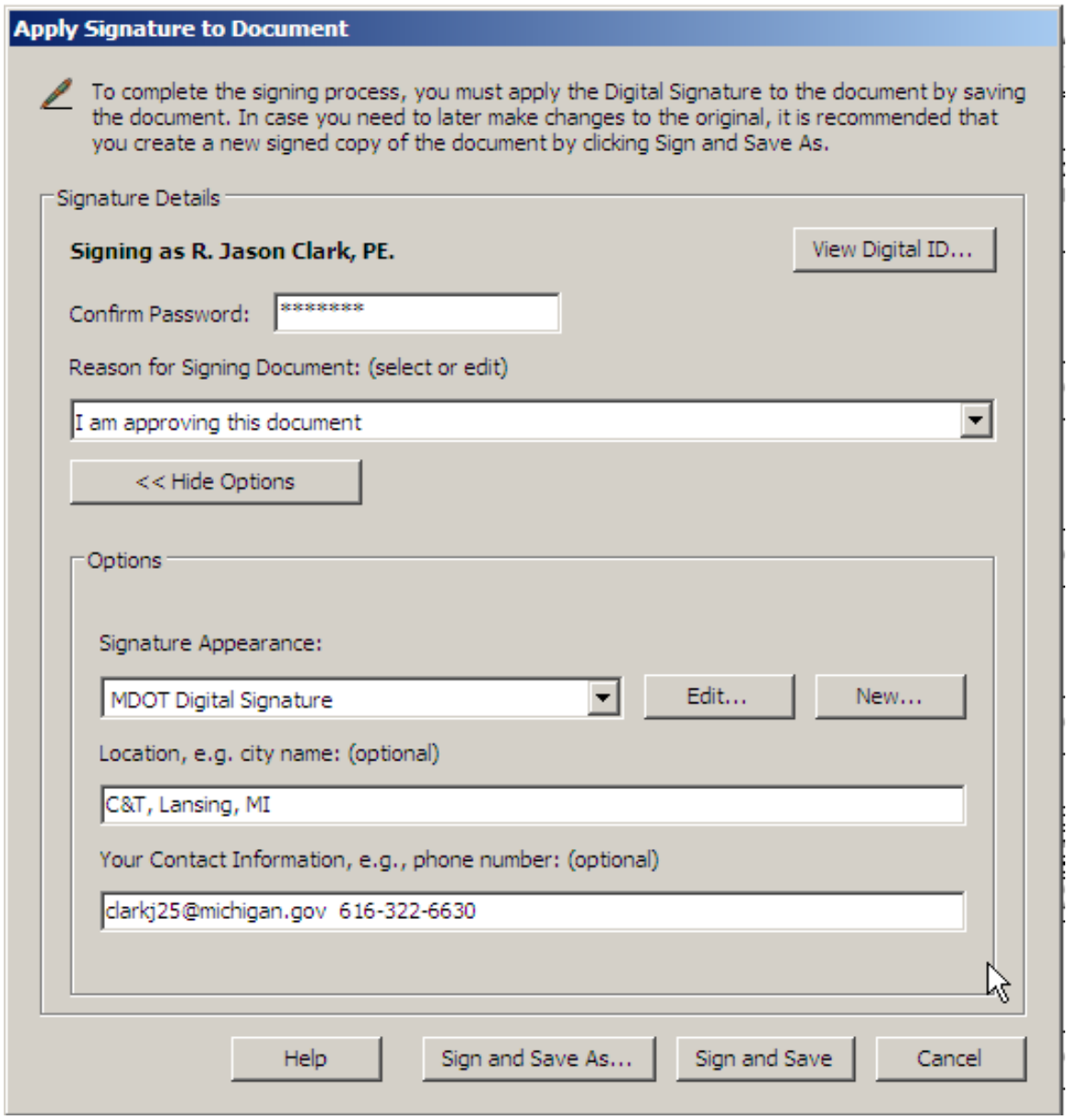
Adobe Reader Version 7



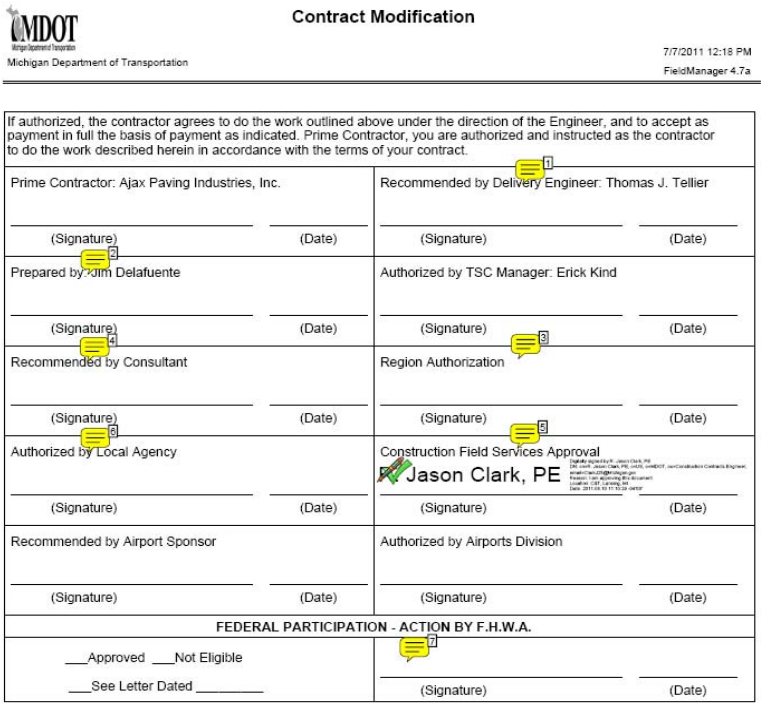
Adobe Reader Version 8

Step #9 – Sign Document and Save

Enter your password, confirm your information and then select either the “Sign and Save As” or the “Sign and Save” button.



Step #10 – Check Results and Validate



MDOT
Michigan Department of Transportation

Contract Modification

7/7/2011 12:18 PM
FieldManager 4.7a

If authorized, the contractor agrees to do the work outlined above under the direction of the Engineer, and to accept as payment in full the basis of payment as indicated. Prime Contractor, you are authorized and instructed as the contractor to do the work described herein in accordance with the terms of your contract.

Prime Contractor: Ajax Paving Industries, Inc. (Signature) (Date)	Recommended by Delivery Engineer: Thomas J. Tellier (Signature) (Date)
Prepared by: Jim Delafuente (Signature) (Date)	Authorized by TSC Manager: Erick Kind (Signature) (Date)
Recommended by Consultant (Signature) (Date)	Region Authorization (Signature) (Date)
Authorized by Local Agency (Signature) (Date)	Construction Field Services Approval R. Jason Clark, PE (Signature) (Date)
Recommended by Airport Sponsor (Signature) (Date)	Authorized by Airports Division (Signature) (Date)
FEDERAL PARTICIPATION - ACTION BY F.H.W.A.	
___Approved ___Not Eligible ___See Letter Dated _____	(Signature) (Date)

<u>Blow up of Digital Electronic Signature</u>

(Note how large your draw box can greatly affect final signature appearance. Also note date/time, reason, contact info, etc)

Construction Field Services Approval

R. Jason Clark, PE

Digitally signed by R. Jason Clark, PE
DN: cn=R. Jason Clark, PE, c=US, o=MDOT, ou=Construction Contracts Engineer, email=ClarkJ25@Michigan.gov
Reason: I am approving this document
Location: C&T, Lansing, MI
Date: 2011.08.10 11:10:29 -04'00'

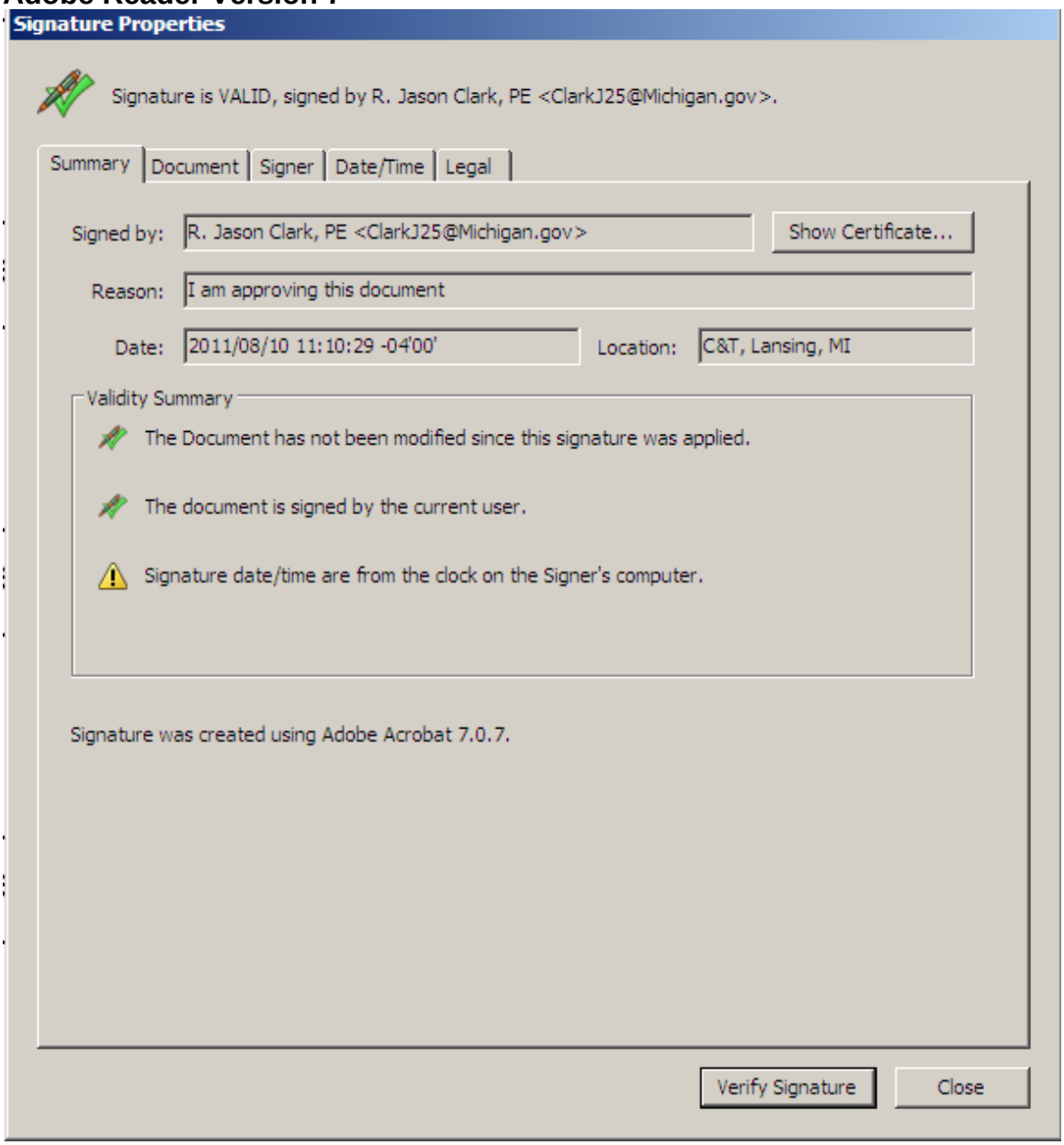
(Signature) (Date)

Appendix A – Signature Validation and Trusted Identities

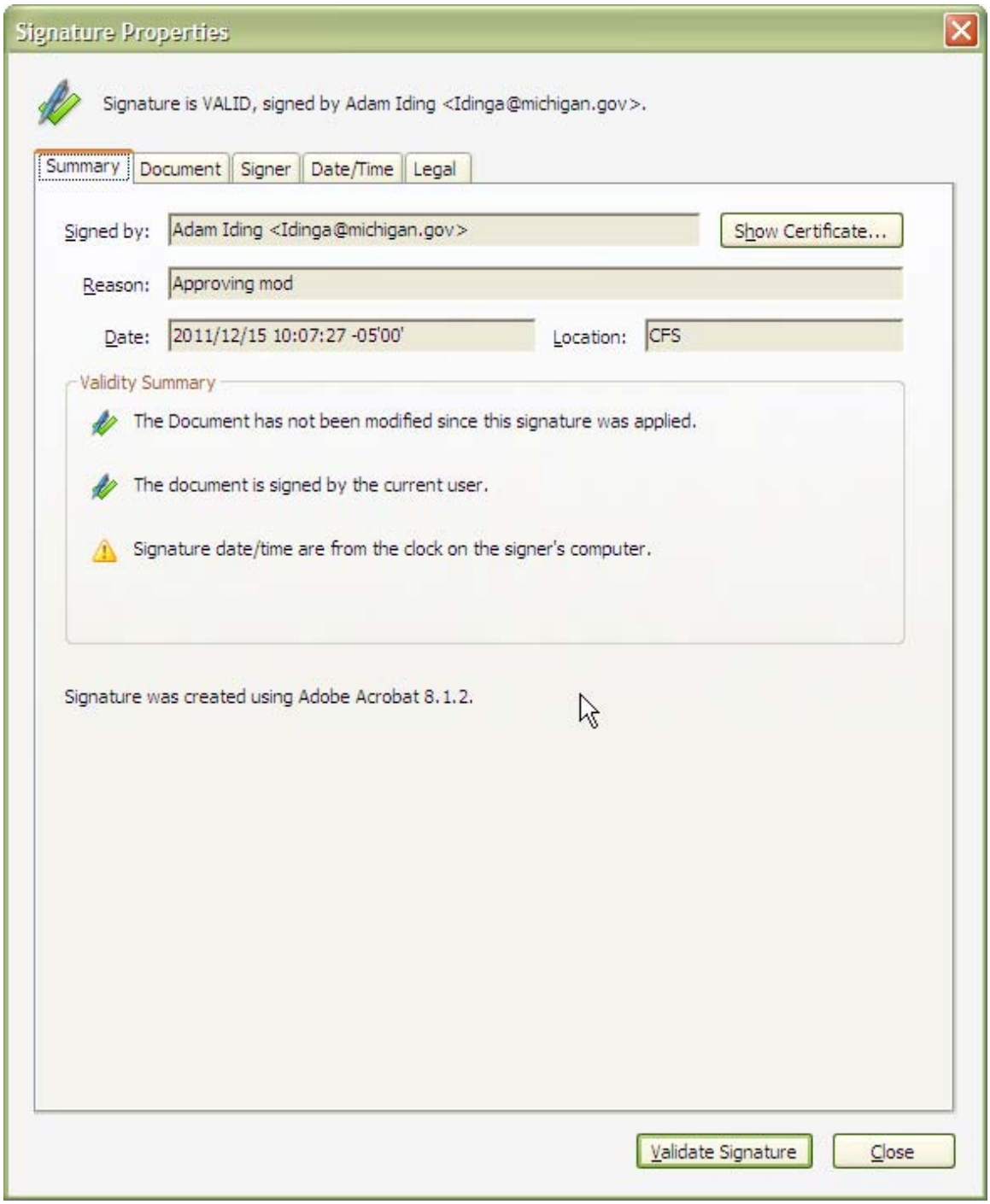
Step A – Validation – Right Clicking on a Signature Reveals

Right click on any digital electronic signature to see the validation info. This confirms the date/time were not altered (attempts to pre/post date), identity, changes to document since signing, etc. Another option in right clicking a signature is to view the document when it was signed (like track changes in MS word).

Adobe Reader Version 7



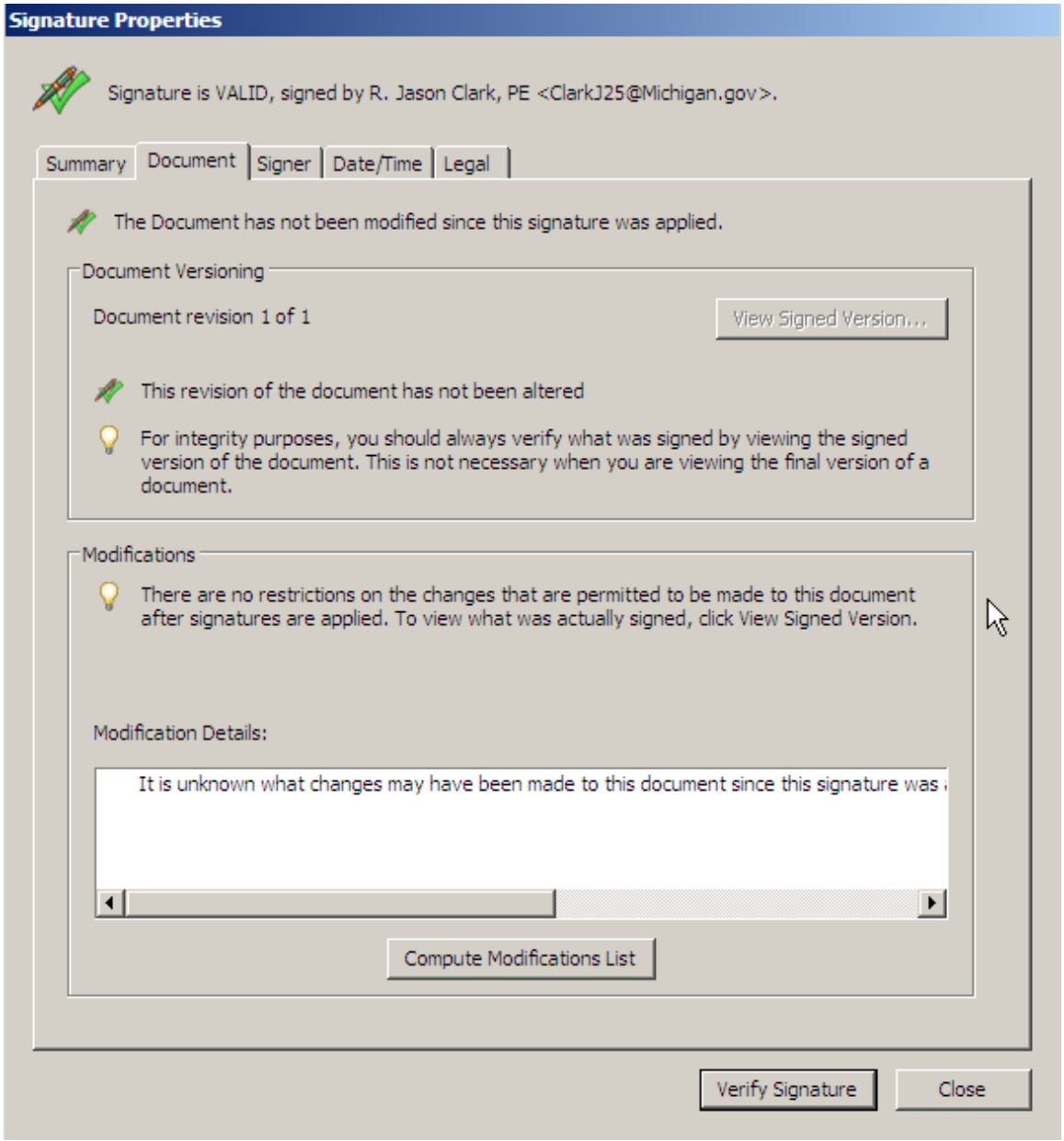
Adobe Reader Version 8



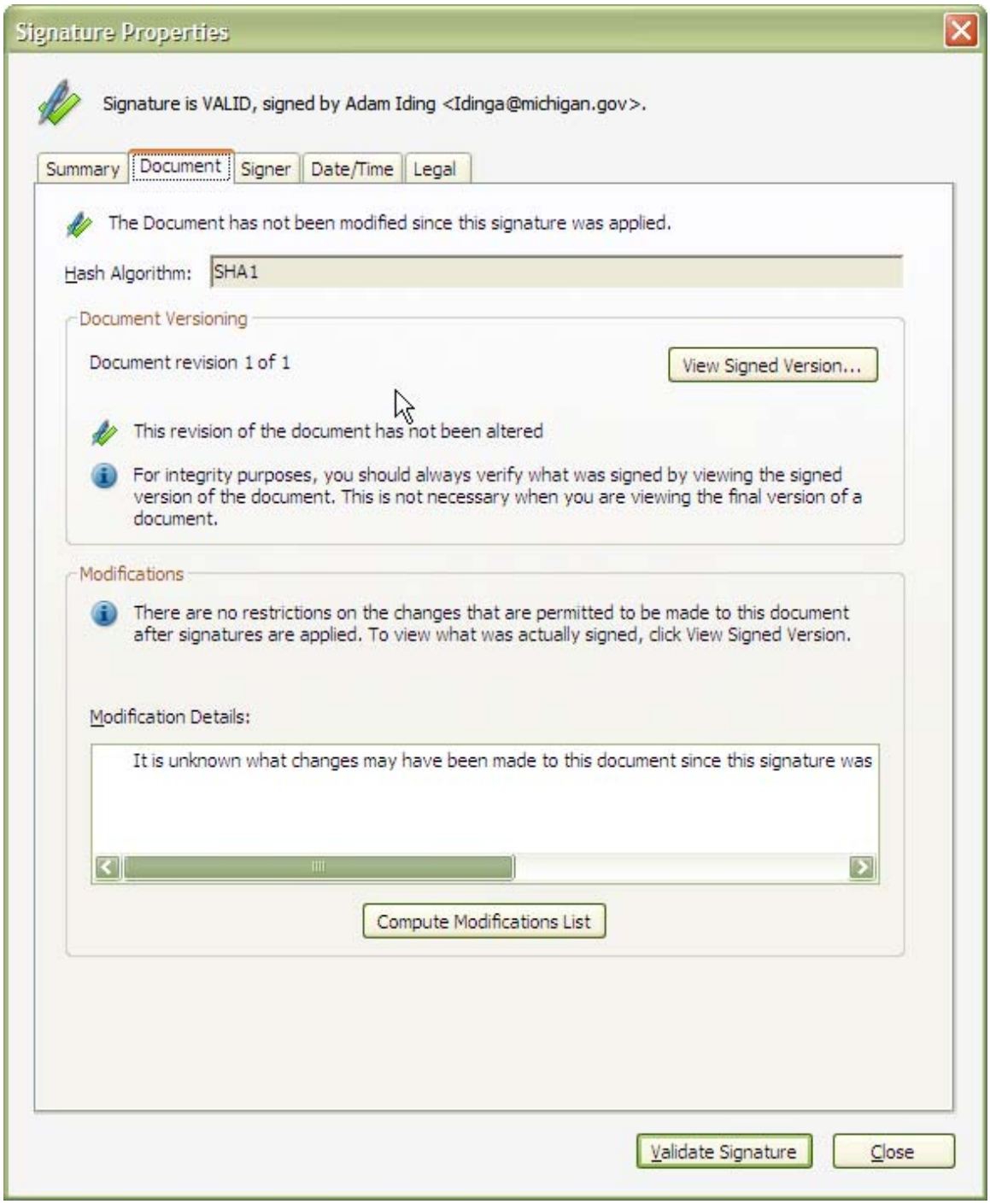
Step B – Validation – Document Properties

This allows you to back up through a "Track Changes" type log to view the version of the document when someone signed. (The addition of each signature technically alters the document so it is not completely unmodified; however, the underlying PDF image is unchanged.)

Adobe Reader Version 7

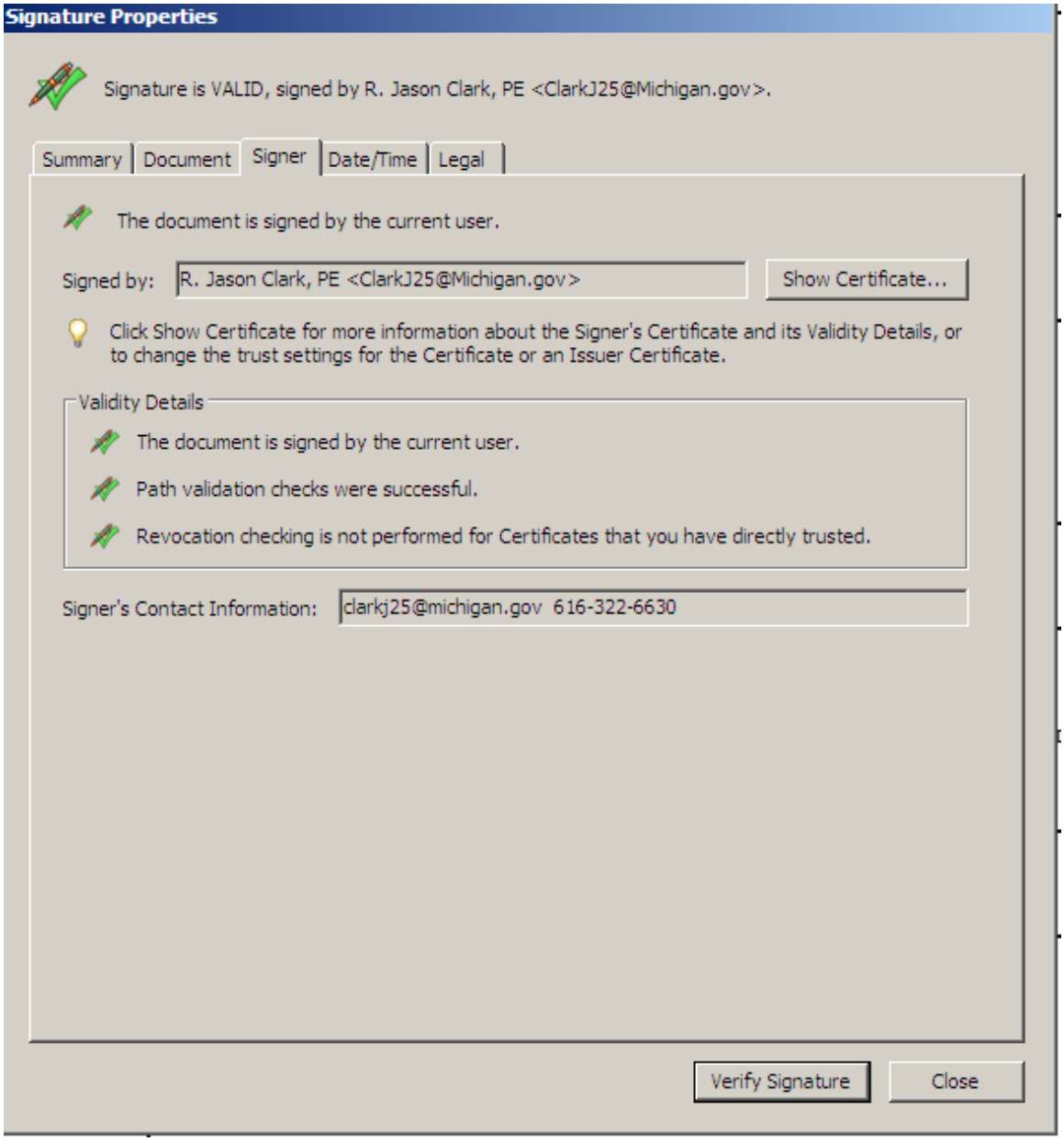


Adobe Reader Version 8

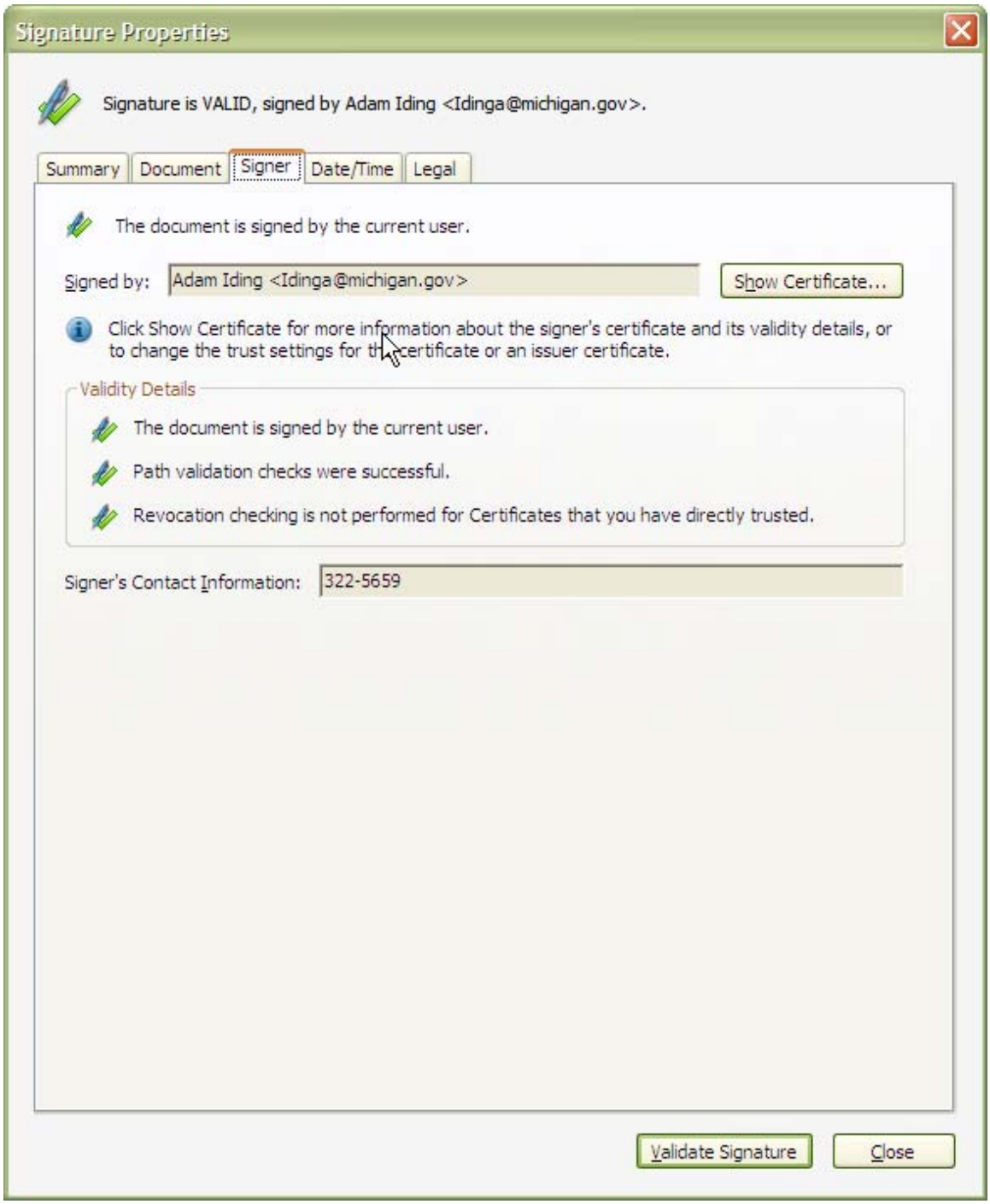


Step C – Validation – Details of Signer

Adobe Reader Version 7

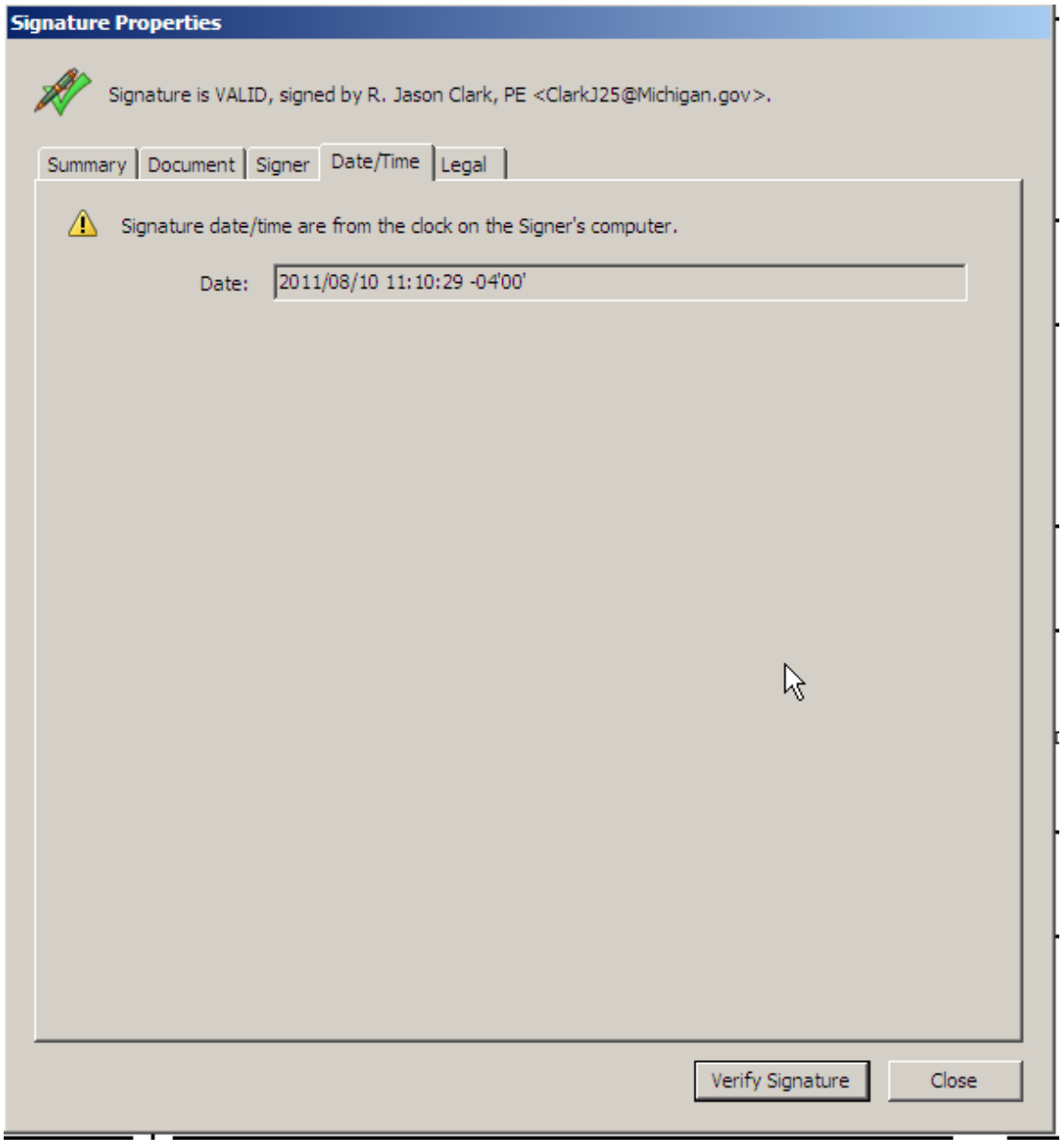


Adobe Reader Version 8

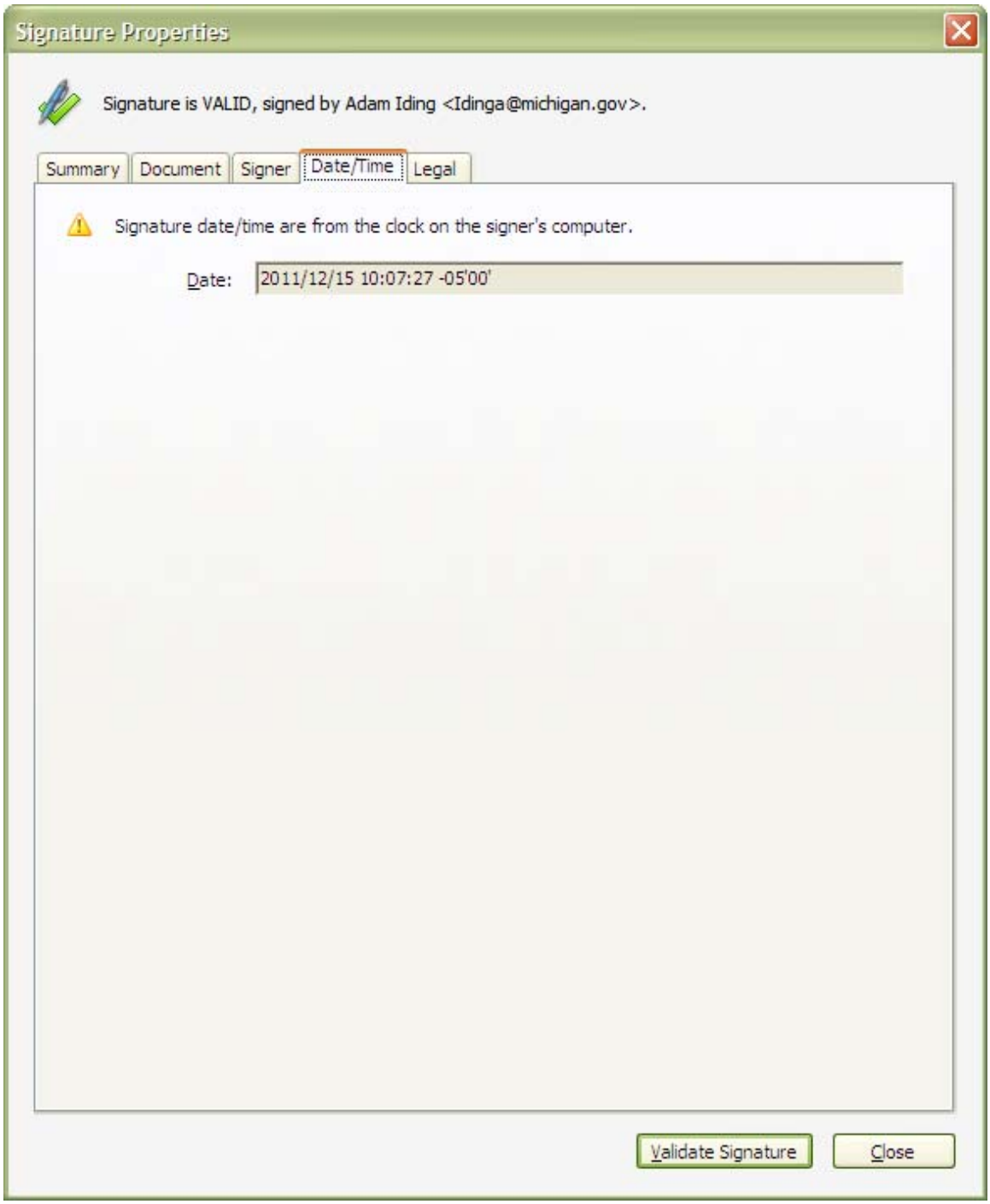


Step D – Validation – Date and Time Stamp Check (to prevent post/pre-dating document signatures)

Adobe Reader Version 7

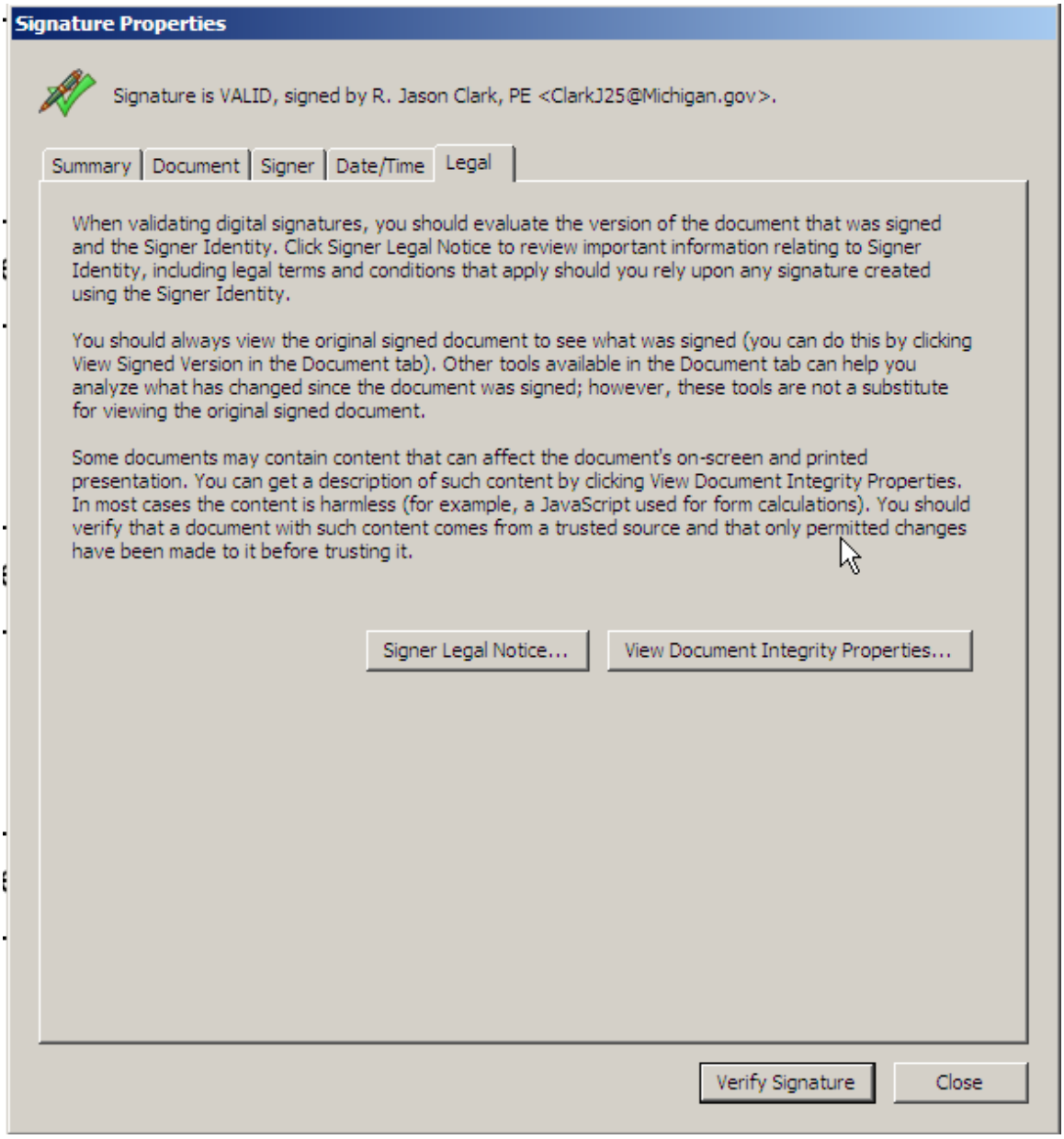


Adobe Reader Version 8

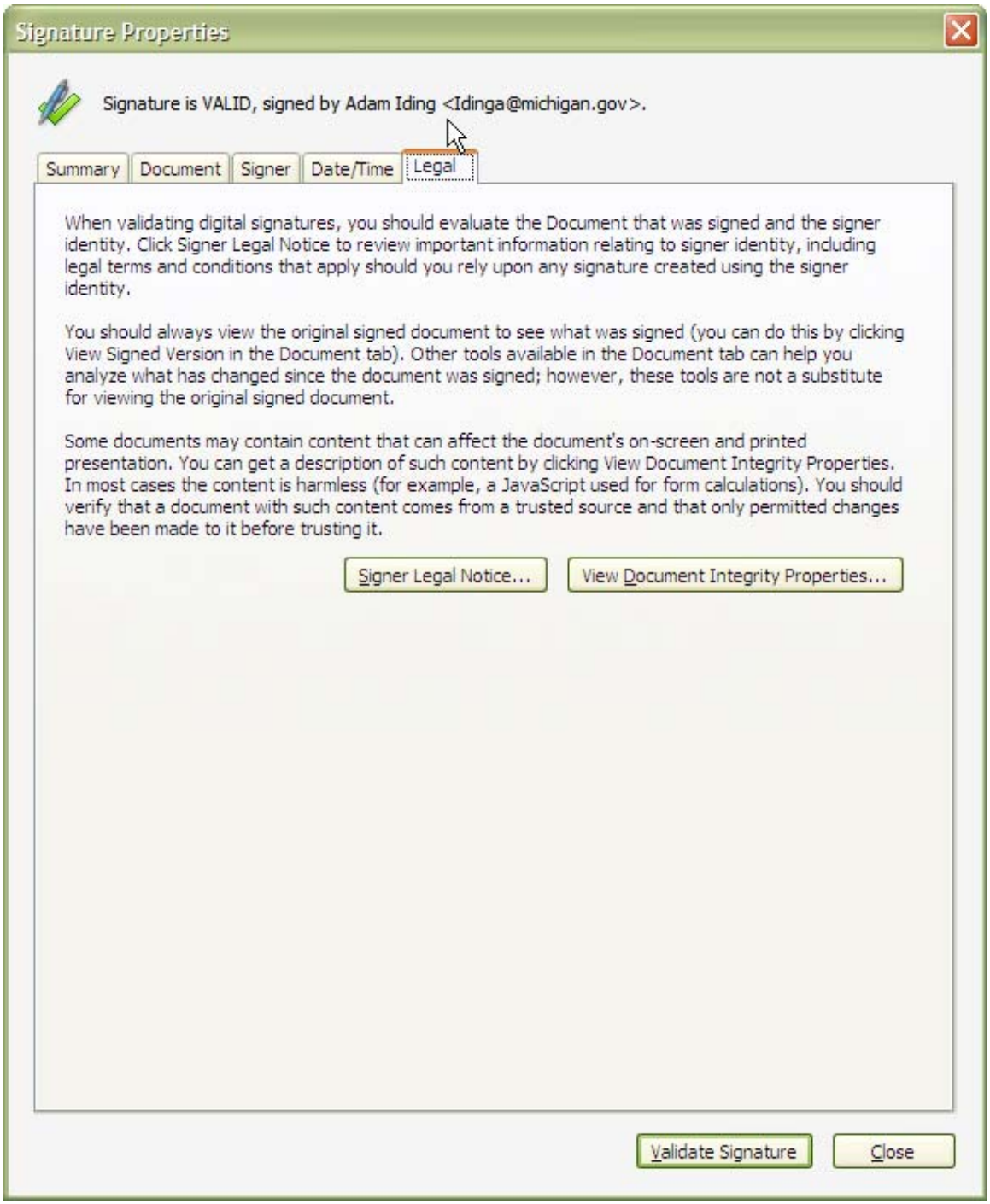


Step E – Validation – Legal Content

Adobe Reader Version 7



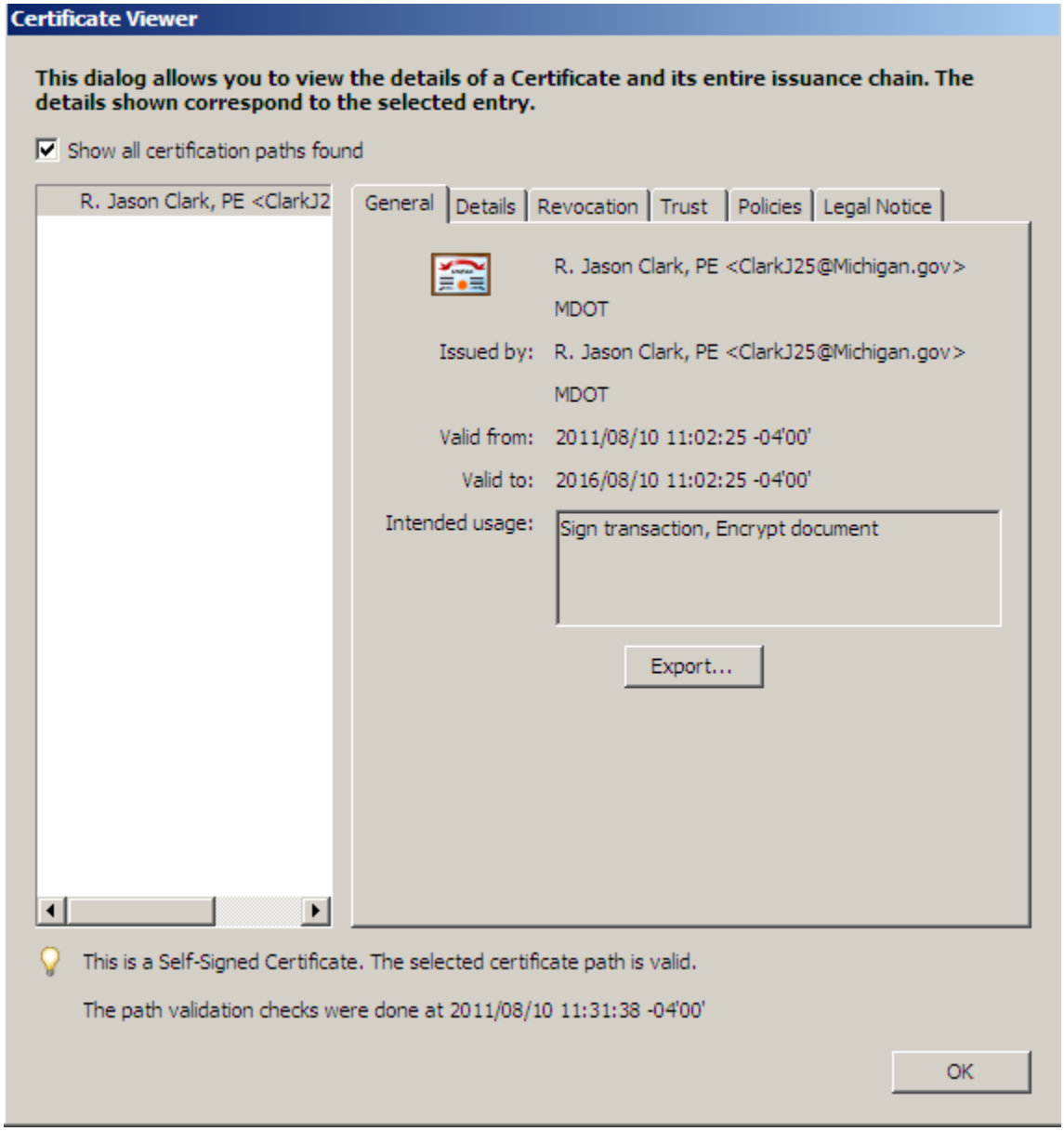
Adobe Reader Version 8



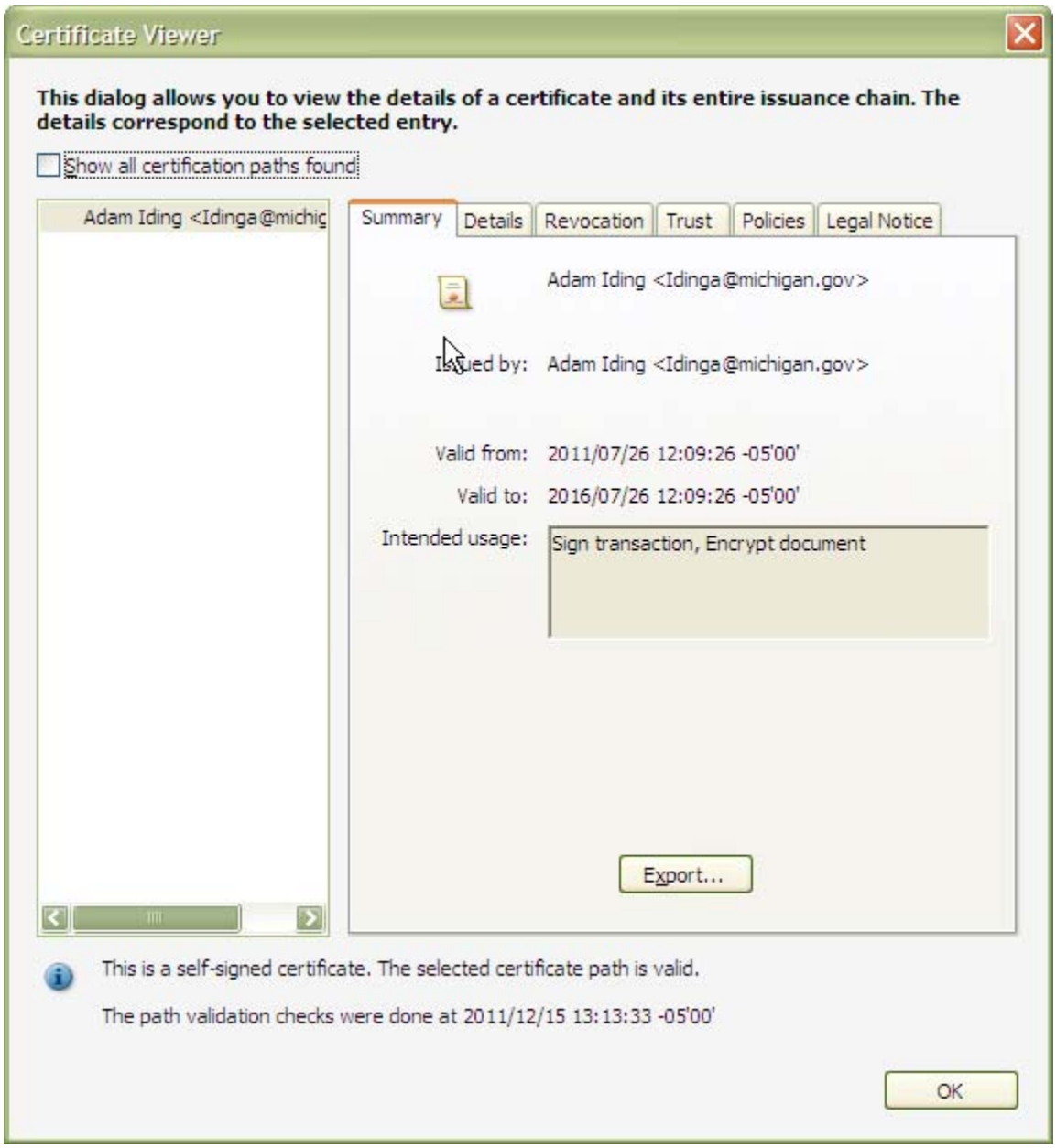
Step F – Validation – Signer – View Certificate

Under the “Signer” tab, clicking on “View Certificate” shows the details of the certificates of all the signers of the document to that point.

Adobe Reader Version 7



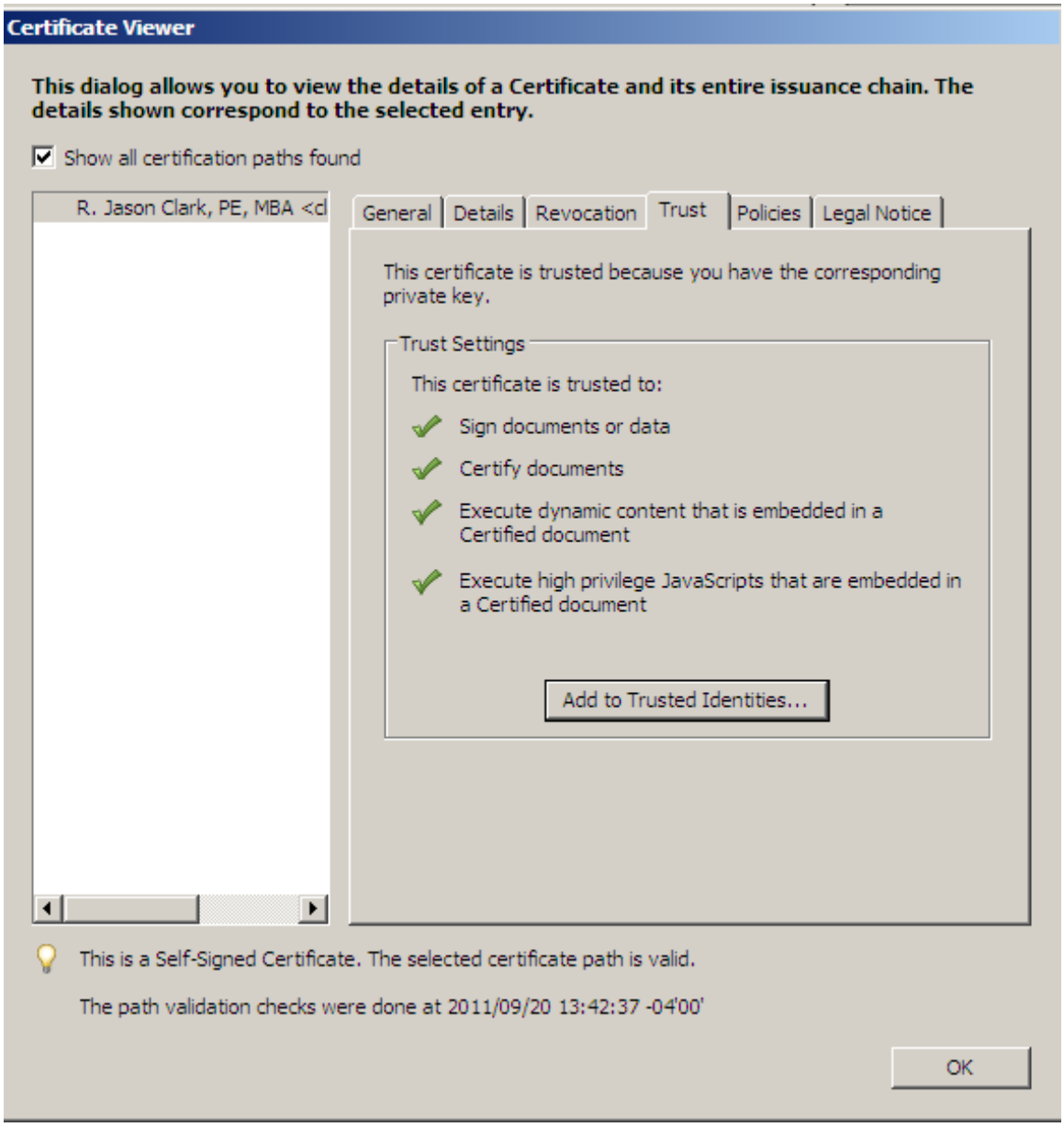
Adobe Reader Version 8



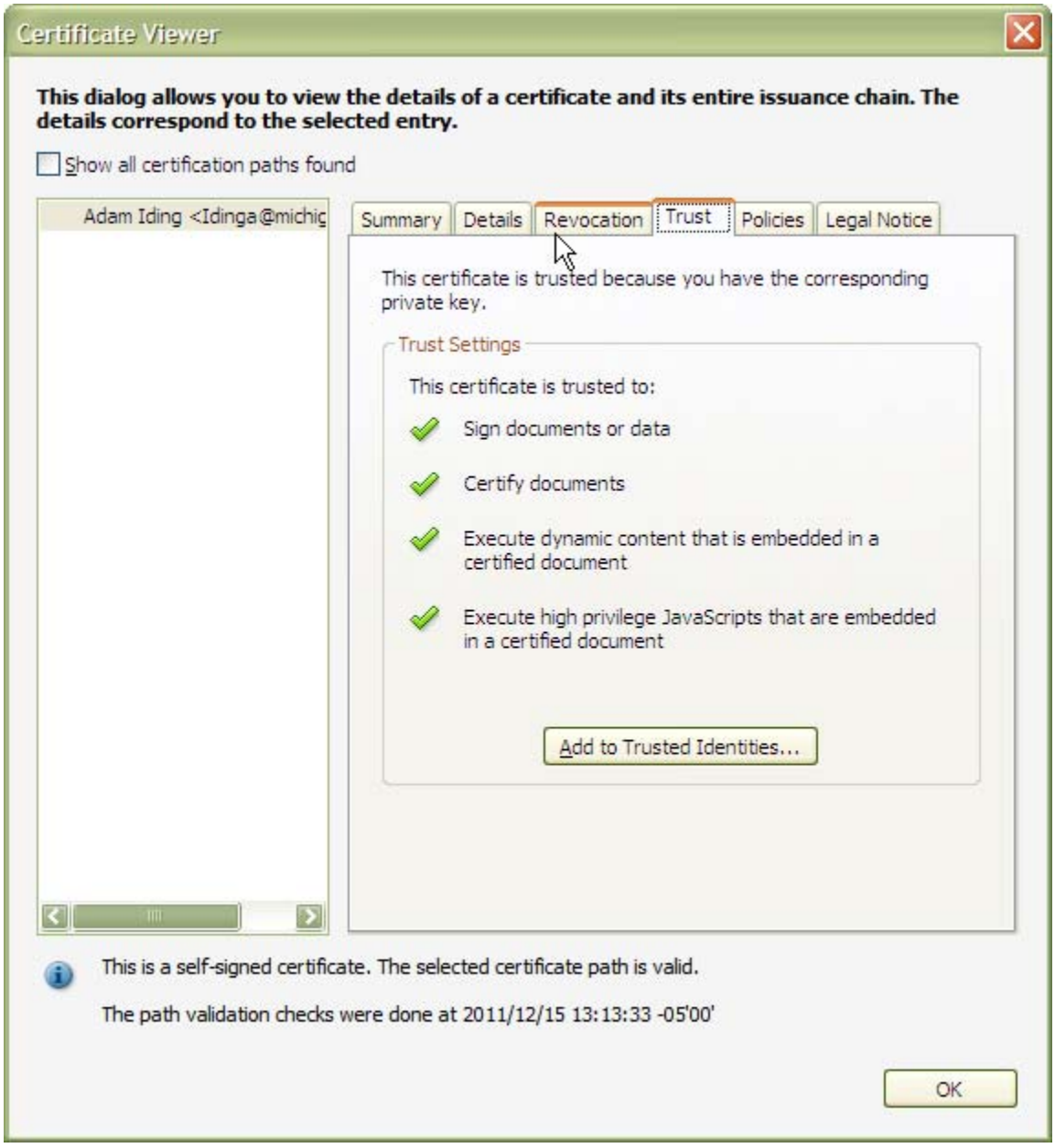
Step G – Validation – Signer – View Certificate – Trust

Under the "Signer" tab, clicking on "View Certificate" then on the "Trust" tab shows the details of the trusted identity and allows you to "Add to Trusted Identities" once you have validated the signature. This only needs to happen once per digital electronic signature.

Adobe Reader Version 7



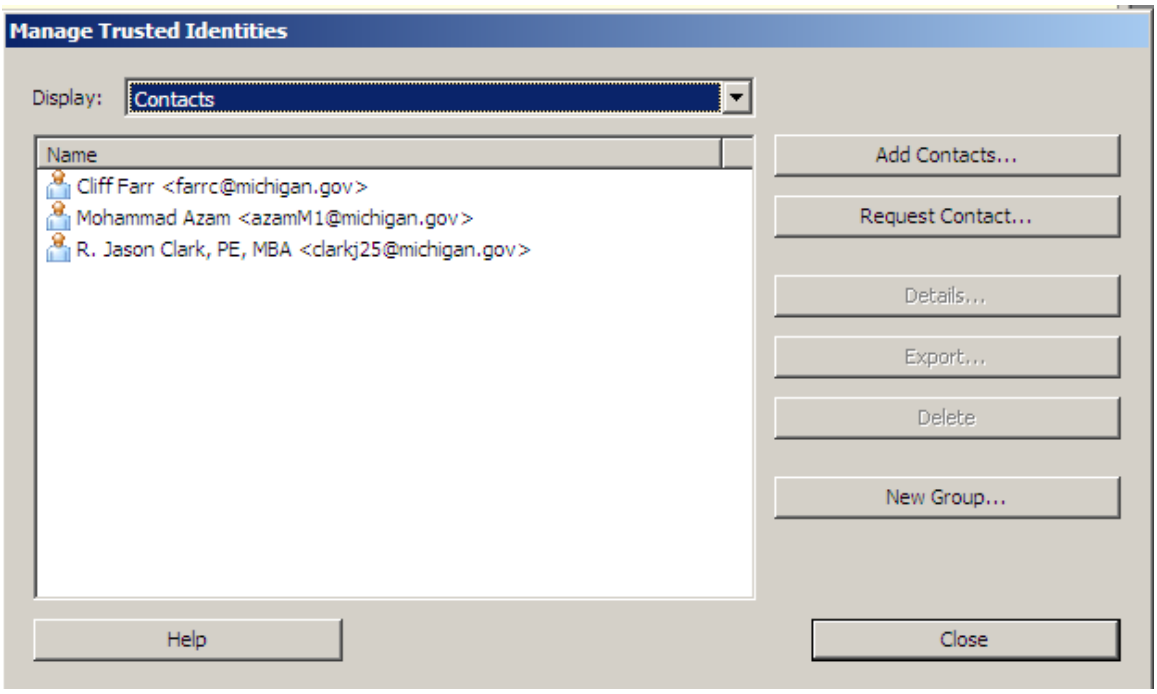
Adobe Reader Version 8



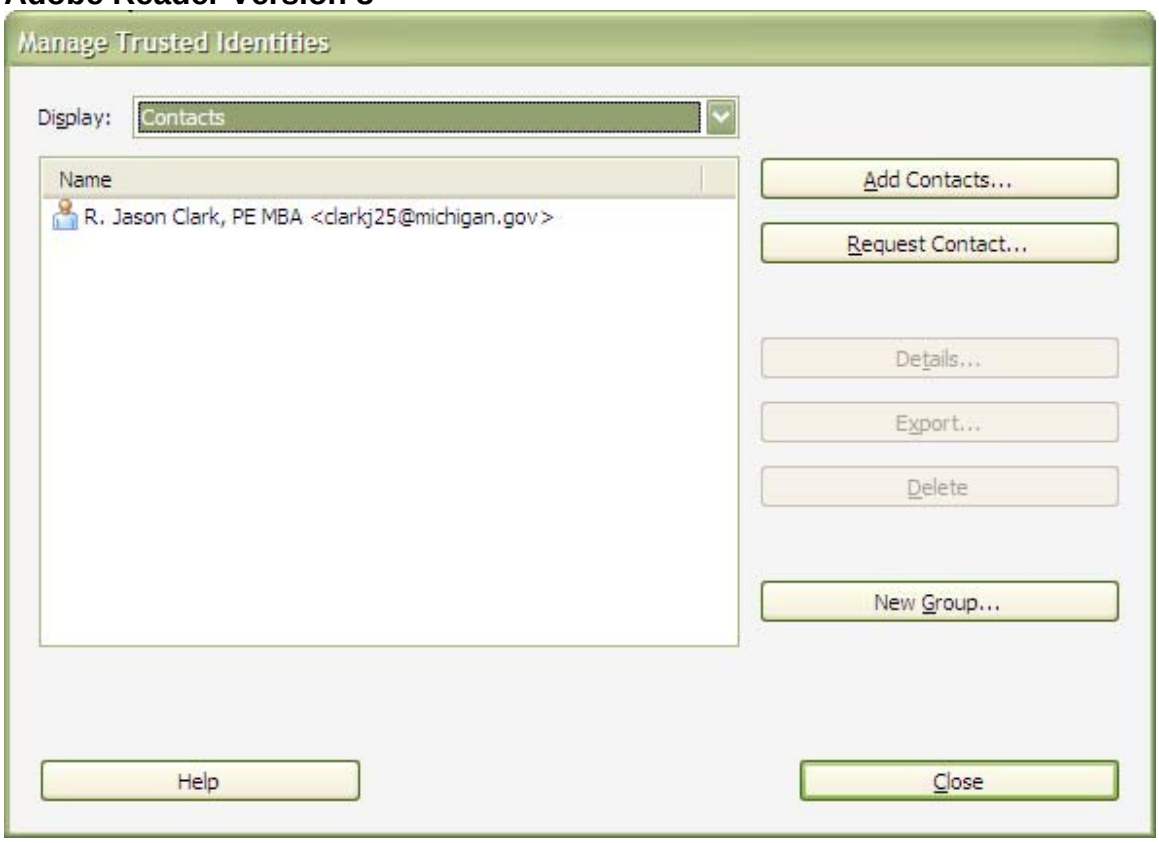
Step H – Advanced Tools Menu – Manage Trusted Identities

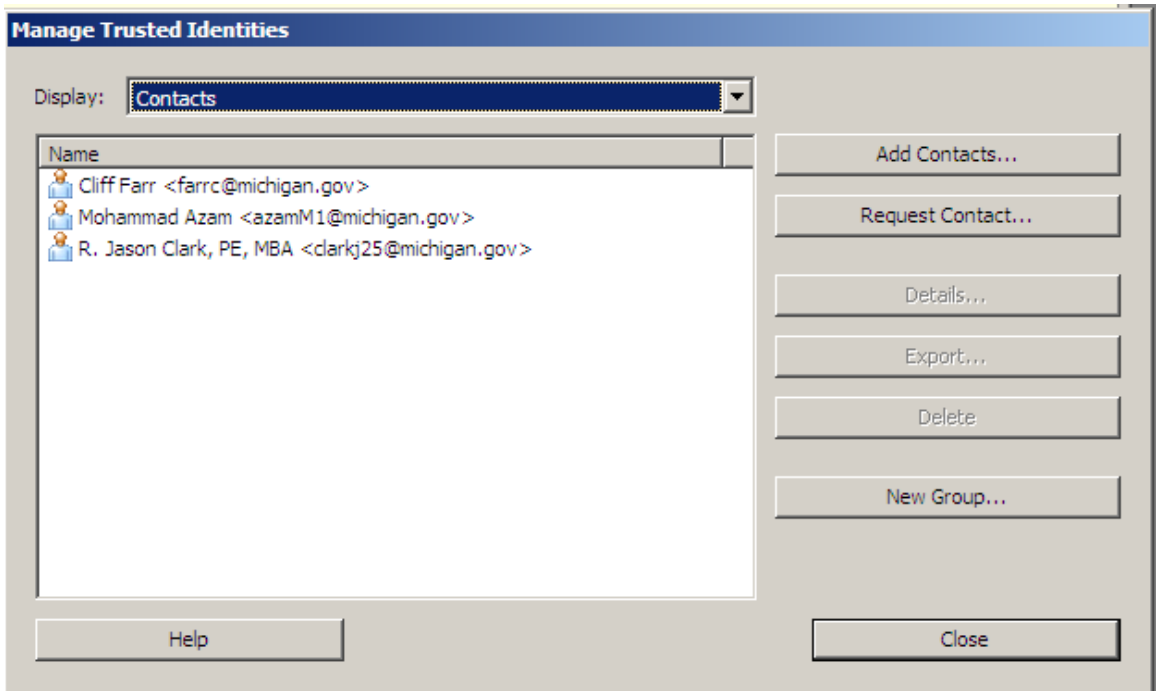
The “Advanced” menu pull down and “Manage Trusted Identities” shows all of the previously validated and trusted electronic signatures that have been received. You can also share your trusted contacts to another person (via email) using the “export” feature.

Adobe Reader Version 7



Adobe Reader Version 8

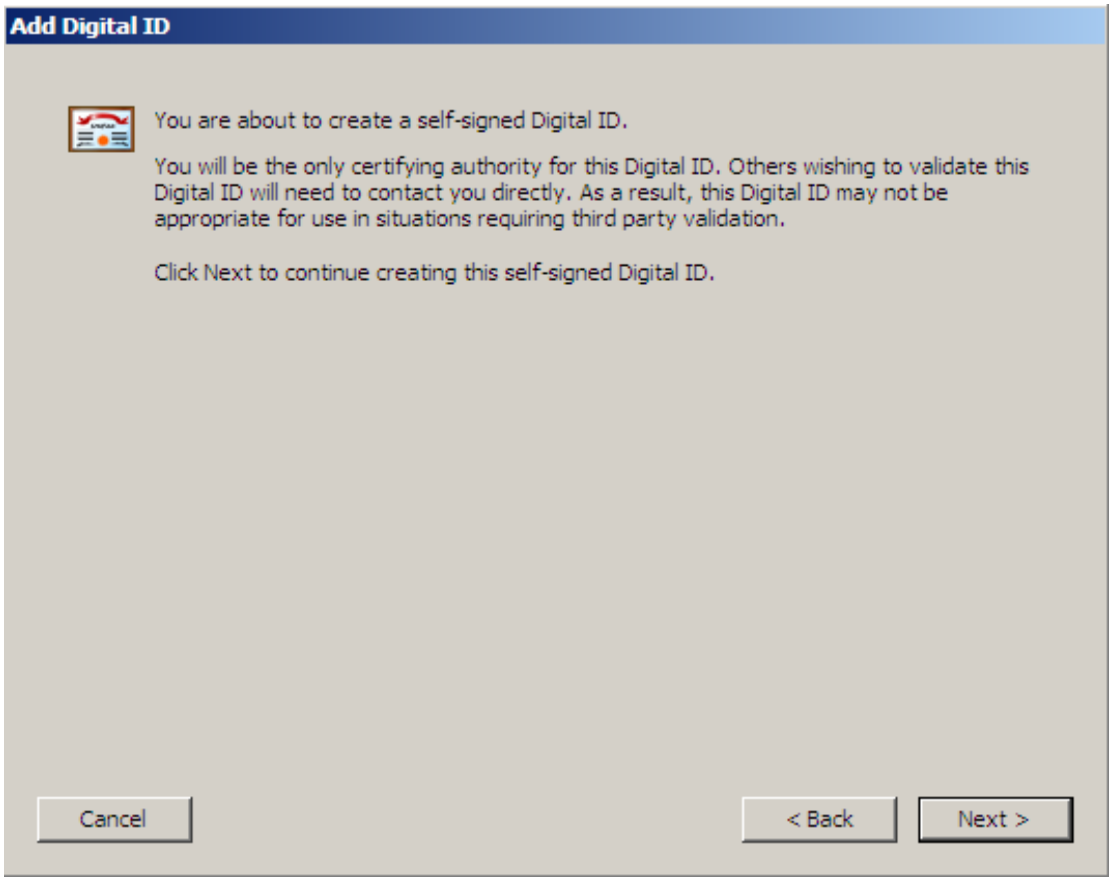




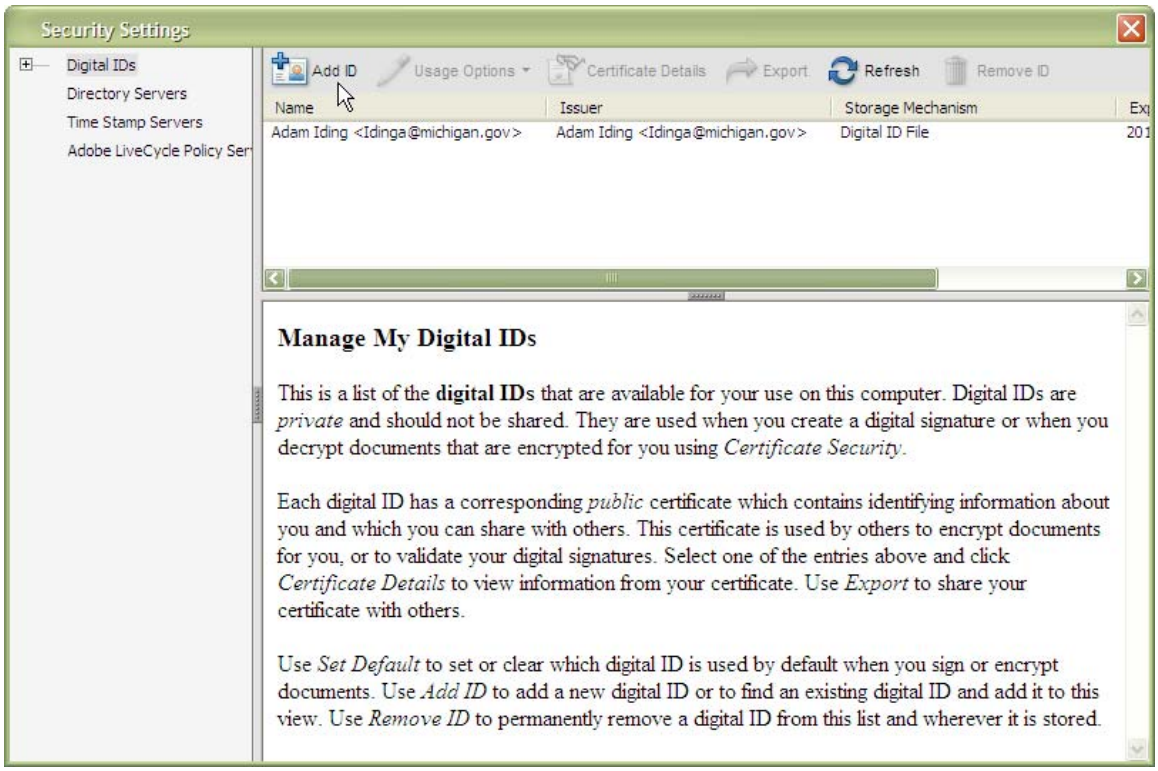
Appendix B – Setting up New Digital Electronic Signature for First Time

Step A – Add Digital ID

Adobe Reader Version 7

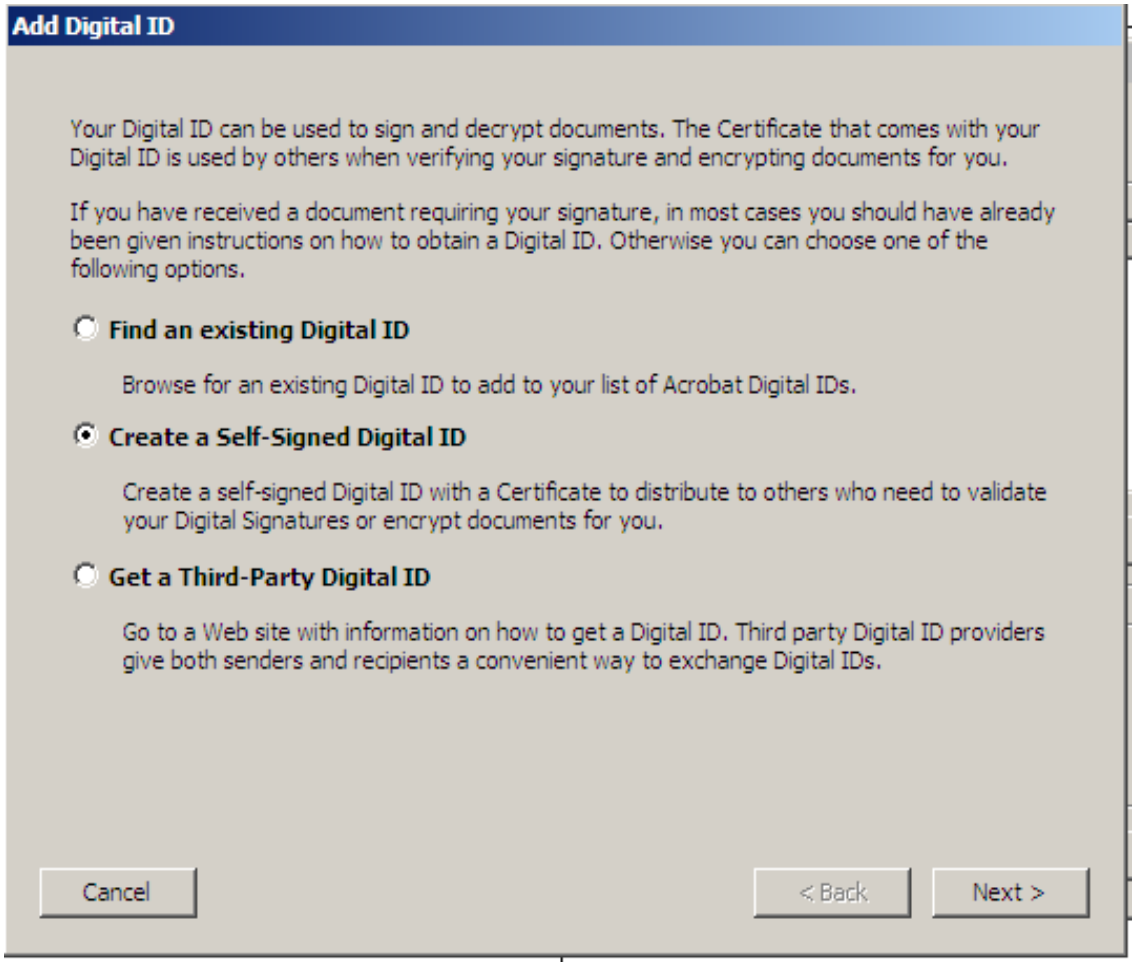


Adobe Reader Version 8

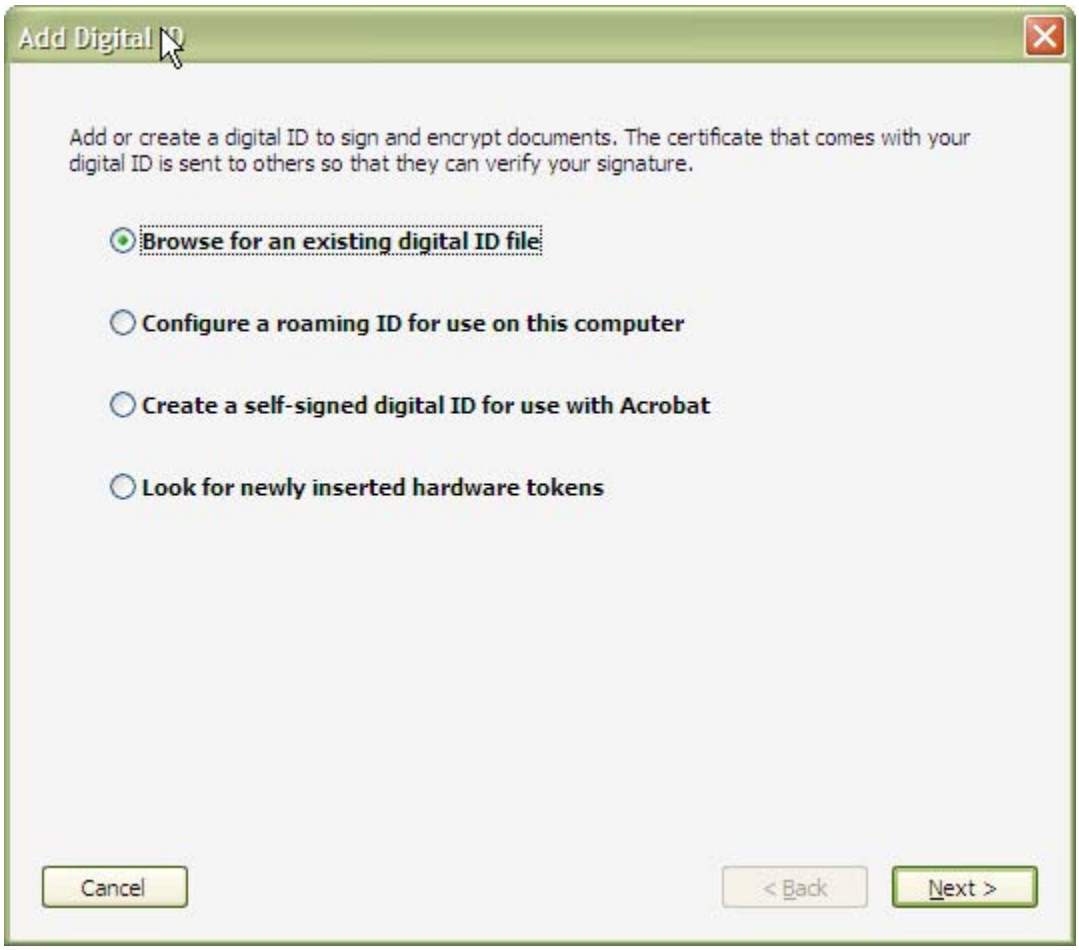


Step B – Select Type

Adobe Reader Version 7



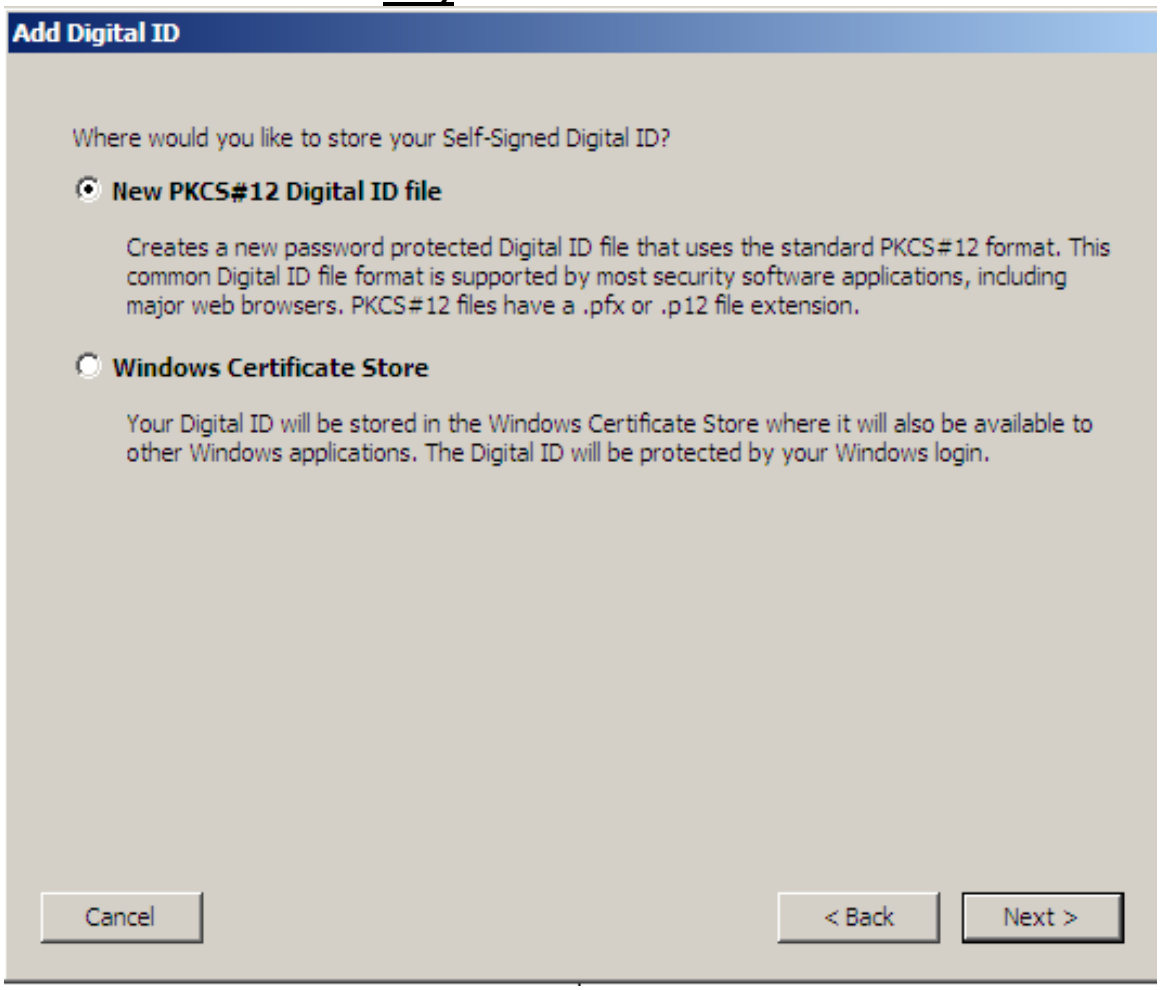
Adobe Reader Version 8



Step C – Storage Method

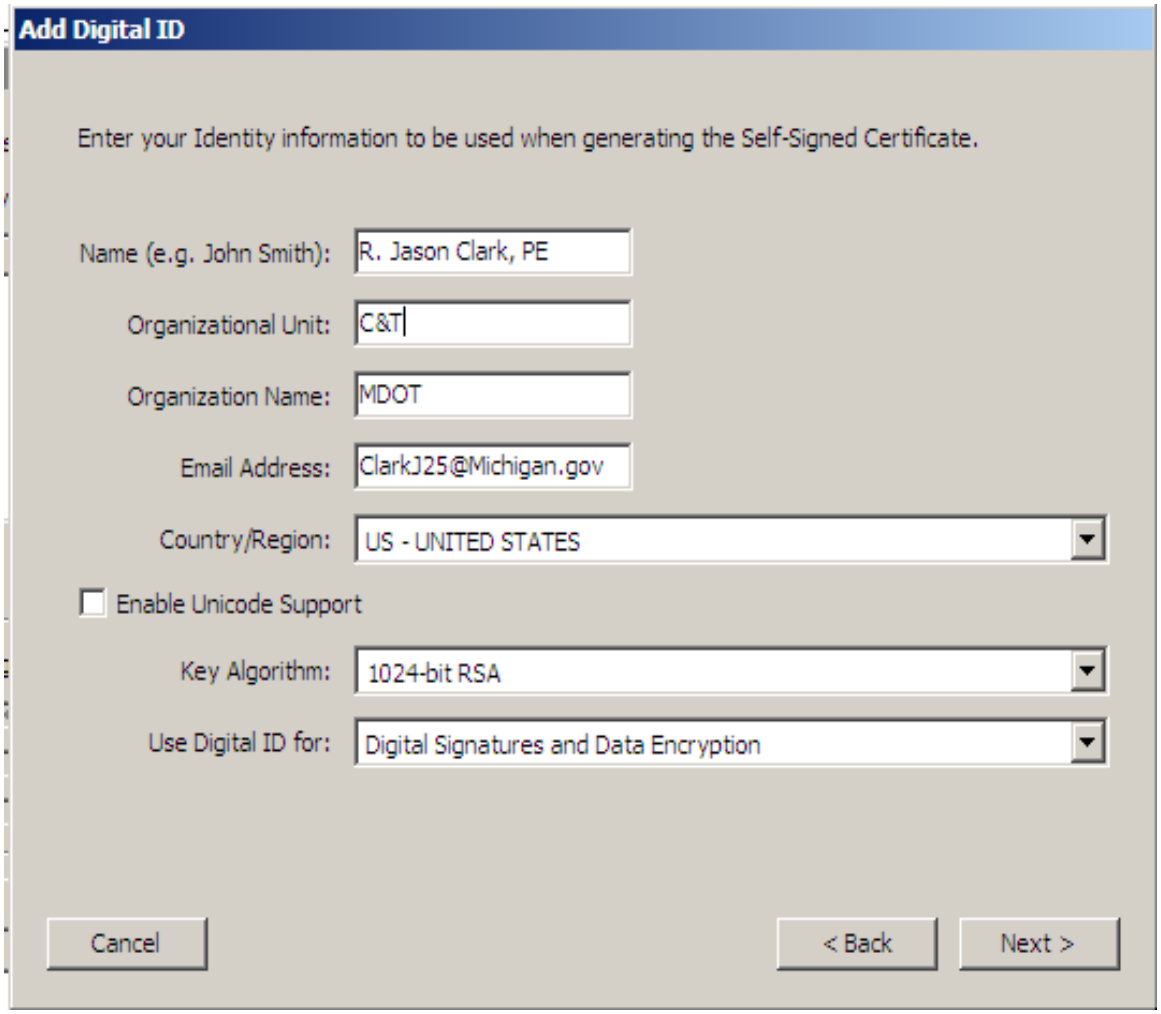
Choosing the "Windows Certificate Store" option does not require the use of a password each time to sign; it uses your computer log-on.

Adobe Reader Version 7 <u>Only</u>

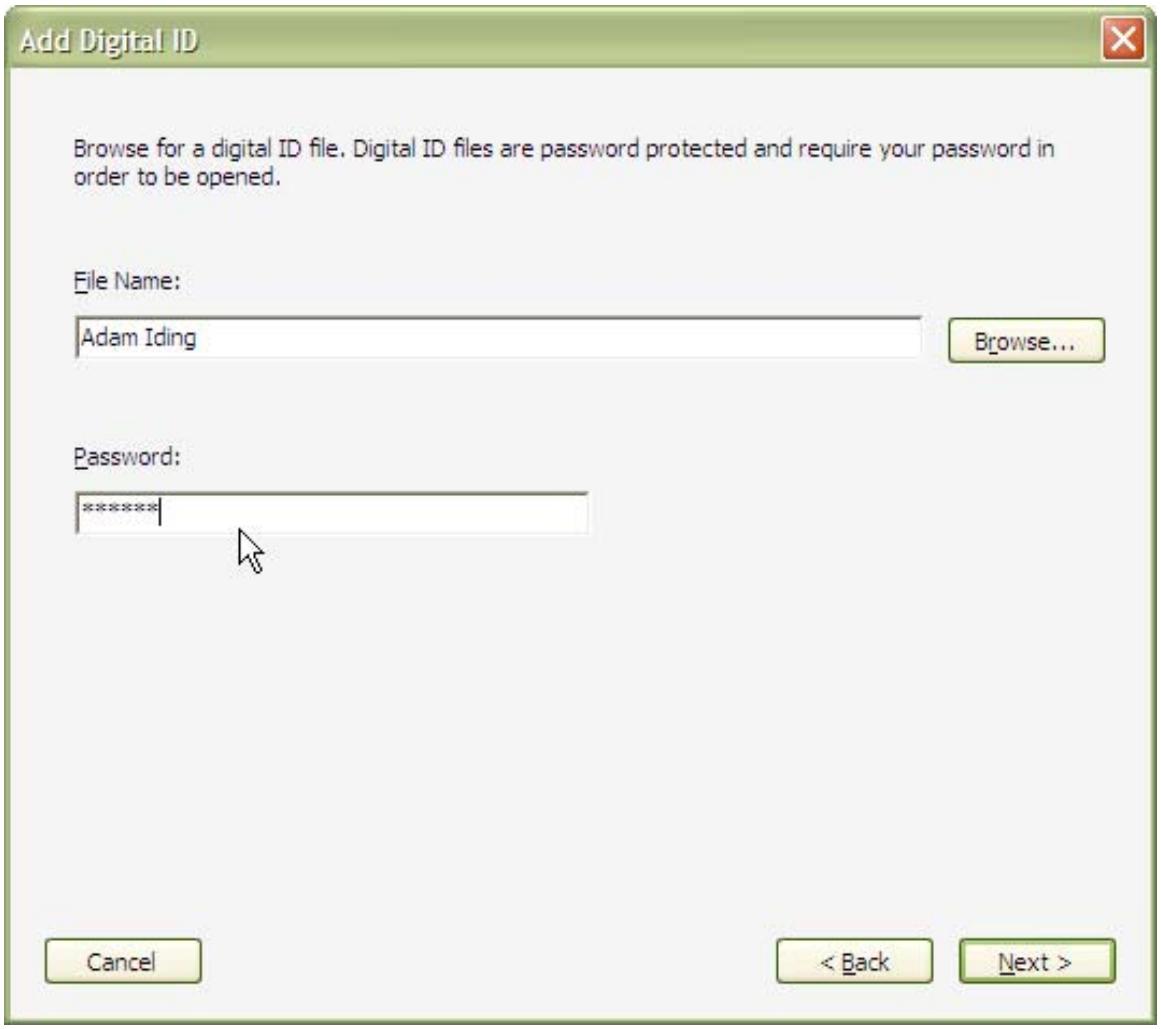


Step D – Enter Your Info

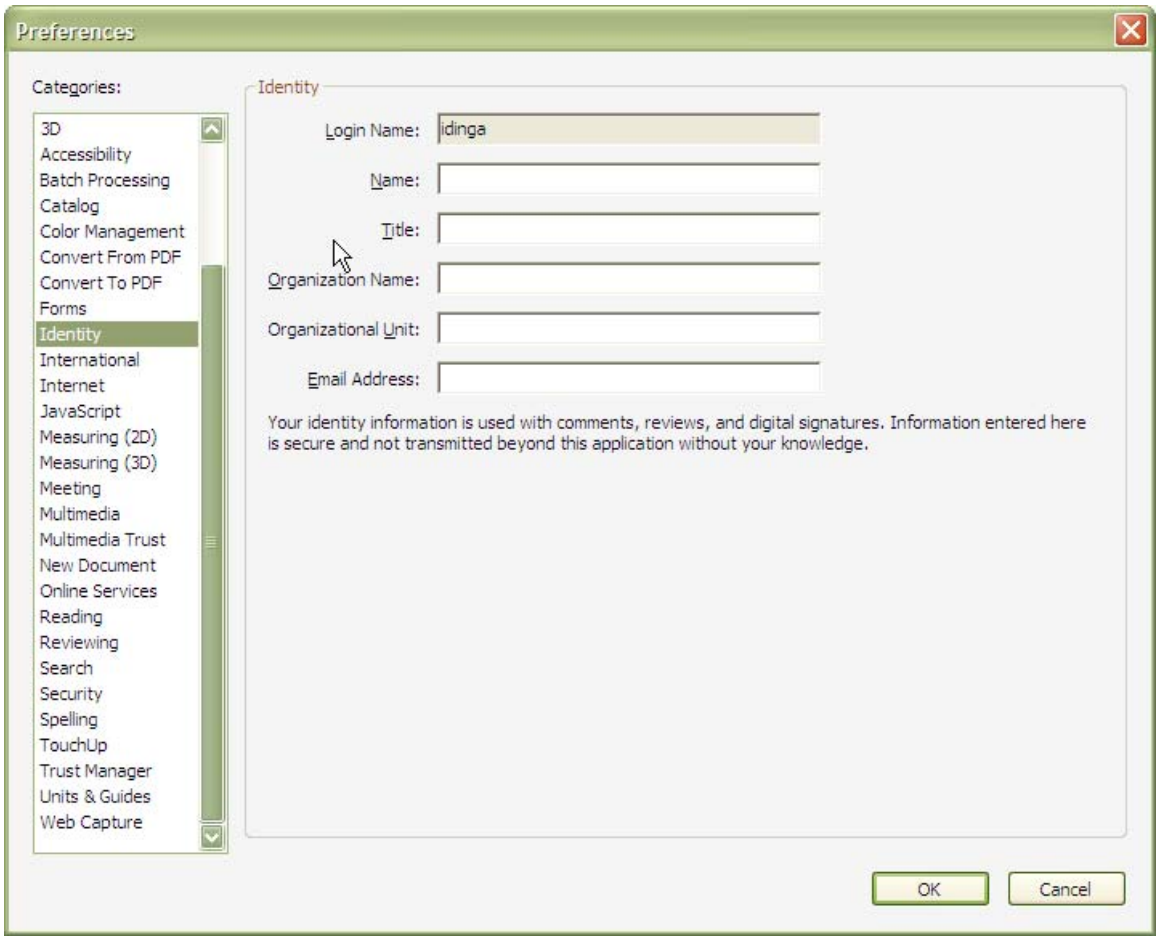
Adobe Reader Version 7



Adobe Reader Version 8 (Step 1): Finish this step and move on to Step 2 to enter your information.



Adobe Reader Version 8 (Step 2): Choose Edit, then Preferences, select Identity on the left under Categories, and then click OK.



Step E – Setup Password

After your password has been setup, go back to Step #7 and start using e-sign.