Table of Contents

Section 1: State Board of Professional Engineers and Land Surveyors Rules

1.1: 13:40-8.1A DIGITAL SIGNATURES AND SEALS ............................................................... 1

Section 2: Overview .................................................................................................................. 2

Section 3 Glossary of Terms .................................................................................................. 2

Section 4: How Authentication Works .................................................................................... 2

Section 5: Digital Signing and Sealing Plans-Example 1 ....................................................... 4

5.1: Bluebeam REVU Digital Signature and Seal Setup ......................................................... 4

5.2: Bluebeam Signature and Seal – Demonstration ............................................................. 7

Section 6 Digital Signing and Sealing Plans-Example 2 ....................................................... 10

6.1: Adobe Signature and Seal Setup ...................................................................................... 10

6.2: Adobe Signature and Seal – Demonstration ................................................................. 15
The NJ Board of Professional Engineers (PE) and Land Surveyors adopted rules for digital signatures and seals in November of 2015. Any electronic plans submitted to the Division of Land Use Regulation, where a signed and sealed plan is required, shall comply with the NJ Administrative Code governing the State Board of Professional Engineers and Land Surveyors. As a point of reference, below is the section of PE rules applicable to digital signatures and seals:

**N.J.A.C. 13:40-8.1A DIGITAL SIGNATURES AND SEALS**

a) A digital signature and seal shall carry the same weight, authority, and effect as a handwritten signature and impression-type seal when the following criteria are met:

1) The digital signing and sealing process satisfies the requirements of the Digital Signature Standard (DSS) established by the National Institute of Standards and Technology, FIPS PUB 186-4, Digital Signature Algorithm Validation System, (2014), which is hereby incorporated by reference, as amended and supplemented. This standard may be obtained at the following website: [http://www.NIST.gov/](http://www.NIST.gov/). The digital signature and seal must be:

i) Unique to the licensee;

ii) Verifiable by a trusted third party or some other approved process as belonging to the licensee;

iii) Under the licensee’s direct and exclusive control; and

iv) Linked to a document in such a manner that the digital signature and seal is invalidated if any data in the document is changed. Once the digital signature and seal are applied to the document, the document shall be available in read-only format if the document is to be digitally transmitted.

b) A licensee who digitally signs and seals a document shall maintain a digital copy of the electronically transmitted document that has also been digitally signed and sealed for future verification purposes in accordance with N.J.A.C. 13:40-3.4(b).

c) The pictorial representation of the digital signature and seal shall be readily available to the Board upon Board request and shall be produced in a manner acceptable to the Board. It shall contain the same words and shall have substantially the same graphic appearance and size as when the image of the digitally transmitted document is viewed at the same size as the document in its original form.

d) Licensees are responsible for the use of their private digital keys. A lost or compromised key shall not be used and the licensee shall cause a new key pair to be generated in accordance with the criteria described in (a) above. A licensee shall take all reasonable steps to ensure that a compromised key is invalidated and shall inform all affected clients that the digital key has been compromised.
Digital Signature and Seal

Section 2- Overview:

All drawings to be uploaded to DEP Online services that would normally be professionally signed and seal, must be digitally signed by a professional engineer using an authenticated digital signature that can be verified. Digital signatures that meet the requirements of the PE rule are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed plan can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. As a state agency, the Division of Land Use Regulation (DLUR) is not authorized to recommend any third-party entity or software. Any reputable software provider should provide documentation that their product meets the Digital Signature Standard (DSS) established by the National Institute of Standards and Technology, FIPS PUB 186-4, Digital Signature Algorithm Validation System, (2014).

This document will serve as a guide to the technical terms and the steps needed add a seal and digital signature to an electronic plan.

Section 3- Glossary of terms:

Public Key Infrastructure (PKI): A framework that is established to issue, maintain and revoke public key certificates.

Digital Signature: Digital signatures allow an individual to keep their entire workflow online, eliminating the need for paper documents. A digital signature is the online equivalent of a notarized signature; In this case the Certificate Authority (CA) serves as the notary in terms of verifying your identity.

A digital signature is constructed from several components:

1. Digital Certificate – A digital certificate is a method of verifying your identity when used to certify documents. A digital certificate allows a document to be checked for changes or modifications to a document post certification. A digital certificate is issued by a Certificate Authority, unique to the user and under the licensee’s direct and exclusive control.

   a. Certificate Authority – A certificate authority is a third-party entity that is only used to verify the signer’s identity and ensure that no changes have been made to the document after certification. Certificate Authorities generally issue a digital certificate using either a Hardware Key (USB or SmartCard) or through the Certificate Authority’s software.

   b. Trusted Timestamp – Trusted Timestamping is the process for securely keeping track of the creation and modification time of a document. This will be issued with your digital certificate when obtained from a Certificate Authority.
2. **Professional's Seal and Signature** – A digital version of the professional's seal and signature. Be sure to keep a copy of your digital seal and signature used. See note*.

*NOTE: The pictorial representation of the digital signature and seal shall be readily available to the Board upon Board request and shall be produced in a manner acceptable to the Board. It shall contain the same words and shall have substantially the same graphic appearance and size as when the image of the digitally transmitted document is viewed at the same size as the document in its original form.

**Section 4: How the Authentication Works**

Using a digital signature to sign a document allows your PDF software to validate the file. This validation will ensure no changes have been made to document after your signature has been placed on it and validate your identity as having signed the document.

Before you begin these are items you will need to complete this guide:

1. Digital version of your Professional Seal.
2. Digital/Pictorial version of your signature
3. Digital ID/Digital Certificate issued by a Certificate Authority
4. PDF software capable of utilizing Public Key Infrastructure (PKI) standards
As a state agency, the Division of Land Use Regulation (DLUR) is not authorized to recommend any third-party entity or software. This software below is currently utilized by DLUR and is meant to be an example only.

Section 5: Digital Signing and Sealing Plans-Example 1

Bluebeam REVU Digital Signature and Seal Setup

Introduction: This portion of the guide will show you how to setup your digital ID for signing and sealing documents if you were issued a digital certificate. If your Certificate Authority issued you a Digital ID skip to Step 5 of this section.

Digital ID’s created using Bluebeam Certificates are self-signed and are NOT ACCEPTED. You must use a digital certificate obtained through a separate Certificate Authority.

1. Tools>Signature and click digital ID’s. Then Click the “+” symbol

2. Select “Browse for existing Digital ID file” and click Next
3. Find your Digital ID. The location will depend on the how the Certificate Authority gave you it. Commonly implemented on hardware devices that need to be inserted and can be found here, under Devices and drives.

4. Enter the password for your digital ID

5. You should now see your digital ID listed here.
6. Highlight your digital ID and Click Manage Appearances

7. Click the ‘+’ symbol to create a new appearance. Copy the following settings. For File choose the file location of your digital stamp.
Bluebeam Signature and Seal – Demonstration

1. Open the PDF to be stamped.
2. Select Tools>Signature and Click Sign Document.

3. Draw a 3x3 Rectangle in the upper corner and then click Cancel. *This box will be left blank. It is to be used by NJDEP to place their approval stamp on the document*

4. Repeat Step 2 – Click Tools>Signature and Click Sign Document.
5. Draw a rectangle in the space designated for your stamp. Choose the digital ID we setup above. Login with your password, and select the settings shown here:

6. Click Ok and save your document with a new name.
7. From the top bar select Window>Panels>Signatures. A toolbar will appear on the left side of the screen showing the signature present. A successful certification will look like this:

**NOTE:** Ensure there is still a signature box available in the upper right corner for NJDEP’s stamp to be placed on the document.

8. Confirm the signature pane shows the document as certified.
Again, as a state agency, the DLUR is not authorized to recommend any third-party entity or software. This software below is currently utilized by DLUR staff and is meant to be an example only.

Section 6: Digital Signing and Sealing Plans-Example 2

Adobe Signature and Seal Setup

Introduction: This portion of the guide will show you how to setup your digital ID for signing and sealing documents if you were issued a digital certificate. If your Certificate Authority issued you a Digital ID skip to Step 5 of this section.

You must use a digital certificate obtained through a Certificate Authority using this method.

1. From the top toolbar click Edit>Preferences. Under Identities & Trusted Certificates click More.

2. Click ‘Add ID’ from the top bar and select ‘My existing digital ID from:’ and select the option relevant to how the Certificate Authority gave it to you.
3. Select the file path or device that contains your digital ID and enter your password.

4. Click Next and then Finish. You should now see your digital ID list here:
5. Close this window and Under Creation & Appearance click More:

6. Under Appearances click New:
7. Under ‘Configure Graphic’ Select ‘Imported graphic’ and select the file location of your stamp. Copy the rest of the settings shown here:
If your Certificate Authority requires you to set a Timestamping server follows these steps. Otherwise this guide is complete.

8. Return to the previous screen and under Document Timestamping select More:

9. From the top bar click New and enter the Time Stamp Server info given to you by your Certificate Authority:

10. Highlight the new Time Stamp Server you’ve just created and click ‘Set Default’ from the top bar.
As a state agency, the Division of Land Use Regulation (DLUR) is not authorized to recommend any third-party entity or software. This software below is currently utilized by Land Use Staff and is meant to be an example only.

Adobe Signature and Seal – Demonstration

**NOTE:** Adobe Reader does not support leaving a signature box for NJDEP.

1. Open the PDF to be stamped.
2. From the right tool bar click ‘More Tools’

3. Click ‘Prepare Form’
4. Select ‘Add a digital signature’ from the top bar:

5. Draw a 3x3 Rectangle in the upper corner and leave this blank. *This box will be used by NJDEP to place their stamp on the document.*

6. Draw a Rectangle where your stamp will be placed:
7. Click on ‘Close’ in the upper right corner:

8. Select ‘Certify with Visible Signature’:

9. Select the Digital ID we selected earlier and click ‘Continue’.
10. Select the appearance we created earlier ‘Stamp and Signature’, enter your digital ID password and ensure ‘Permitted Actions After Certifying’ is set to ‘Form fill-in and digital signatures’.

11. Save the document with a different name.
12. Confirm the document has been correctly certified by left clicking your stamp and clicking ‘Signature Properties’.