DATE: October 29, 2014

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

FROM: Gregory C. Johnson, P.E.
Chief Operations Officer
Randel R. Van Portfliet, P.E.
Bureau Director of Field Services

SUBJECT: Bureau of Highway Instructional Memorandum 2014-11
Digital Electronic Signature (DES) Validation Procedures

What is Digital Signature Validation and why does it matter?
All signatures must be authenticated to determine the identity of the document signer(s) and it is the legal requirement that anyone receiving a signature from an external party must authenticate the signature on the document they receive (paper or electronic). While handwritten signatures have visual indicators that help us determine someone’s real signature, the digital signature process is much faster and more secure. However, digital signatures can also be falsely created by other parties and made to look very similar to the authentic digital signatures, so care must be taken to determine the true identity of the signers. The process to determine the authenticity of digital signatures is referred to as signature validation.

Validation is the process that authenticates the electronic signature on a document and compares it to the known validated signature on file.

In general, the electronic signature validation process occurs primarily in the background of the software and only requires us to take action the first time a signature is received. A valid digital signature proves that the message was created by a known sender; such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). This is accomplished by the use of an algorithm that creates unique encrypted codes associated with the digital signature for the user. In general, each digital signature has two main components. The first is a private key code that is encrypted into the signature which is essentially the user’s password used to affix their signature. The second component is called the public key code which is a unique complex code embedded into the signature that allows other parties to easily authenticate the true identity of the signer. Each digital signatures public code is unique to the digital signature, not the person, thus if you have
two digital signatures each has its own unique code, they are not the same. When a sender signs a document their private key remains with them, but the public key is embedded into the signature on the document. When the document is sent to the recipient, the recipient’s computer compares the unique public code in the signature to the list of known validated signature codes. If the codes match then the signature is considered valid and proves the signature was made by the sender. If the codes do not match, the software indicates the signature has not been validated. If this occurs the recipient is required to perform the validation process as described in the next section of this BOH IM. (Note the graphic process describing the validation process is presented in Attachment 1; e-Signature Validation Process Overview of this BOH IM.)

Effective immediately, the process for validating Digital Electronic Signature (DES) received by MDOT from any external party will be as follows:

1. **External Parties:**

   a. All external parties (non-MDOT/FHWA), intending to use DES on any documents to be submitted to MDOT, must submit form 5600 Statement of Digital Electronic Signature Validation to the local MDOT office for validation of the DES prior to (or concurrent with) the DES being used on any documents submitted to MDOT.

   b. Form 5600 must be submitted for each individual DES the first time the signature is used on a project. This can be submitted concurrently with a document; however, the document will not be accepted until the validation process has been completed.

   c. Most DES certificates expire after four (4) years from the initial date of the DES creation. It is the responsibility of the signature creator to maintain their DES and create a new DES when their current DES expires. Form 5600, once validated, will allow the use of the DES on other documents submitted to MDOT until the DES expires (including on other projects or in other offices).

   d. If the DES owner changes employment, position, responsibilities, forgets the DES password, or loses the DES file, this will require that a new form 5600 be submitted for the new signature.

2. **MDOT Office:**

   Any document received by MDOT containing a DES must be checked for proper validation prior to acceptance. This can be confirmed via the blue signature panel validation process at the top of the document in Adobe Acrobat (Figure 1).
If the digital electronic signatures on the document have already been authenticated, the software will clearly confirm this with the green checkmark as shown below in Figure 2.

If electronic documents come into the office with a non-validated DES, (figure 3 below),

then the office must determine the validity of the document signers. If the signature does not match the previously validated signature codes on file the office must reject the document until a new form 5600 is submitted and the DES can be validated. **It is the legal responsibility of the first person who receives any signature to verify the validity of the signature before accepting any documents.** After the signature has been validated and added to the trusted list of validated signatures, the software will re-validate and display the green check mark. The completion of the form 5600 is only required when a signature is first used, subsequent documents will be validated automatically for that user. It may take a while for the central office database updates to be distributed to all other users, so until that occurs a signer can send along a
copy of the fully completed form 5600 to the new office where they can manually add the validated signature to their trusted identities.

In the case of multiple signatures on the same document, the software clearly identifies the signatures that have not been validated as shown in figure 4 below.

![Image: At least one signature has problems.]

The software also automatically tracks all changes made to the document. This is important because by the very act of signing a document, the document has changed from the version the first person saw. Any major changes to the document that affect the integrity of the encrypted digital signatures will invalidate or delete the signatures, but minor changes like multiple signers will just be noted.

Should an office receive a document or form 5600 that requires them to validate the digital signature the process is simple and straightforward.

The validation process is detailed on form 5600 and the receiver must verify at least two (2) of the four (4) federal signature authentication requirements outlined below:

a. The name of the sender is the same name expected.
b. E-mail from a company domain e-mail address.
c. Direct contact with sender verifying they sent the document with signature.
d. Verification via another method with provided details.

The MDOT recipient of the document is then required to indicate which two methods were used to verify the signature is actually from the recipient and then confirm their validation efforts by placing their own digital signature on the form. This form is then routed to the central office for archiving and a copy of the completed form returned to the sender for their records or for submission to other offices until the central database is updated.
a. MDOT office staff that receives form 5600 will go through and complete the validation steps per the form instructions.

b. Once the DES is validated, the validating MDOT office staff will countersign form 5600.

c. MDOT office staff will then add the validated signature to their trusted identities. Instructions for manually adding a validated signature to your trusted identities can be found on the MDOT WIKI Construction Manual in Division 1 Supplemental Information, e-Sign section. [http://mdotwiki.state.mi.us/construction/index.php/E-Signature](http://mdotwiki.state.mi.us/construction/index.php/E-Signature)

d. MDOT office staff will then submit the completed form 5600 to MDOT-eSign@michigan.gov and also back to the submitting applicant.

3. MDOT-Central Office:

   a. MDOT Central Office staff will receive form 5600 via the MDOT-eSign@michigan.gov e-mail address. MDOT Central Office staff will then maintain these 5600 forms in a centralized server for archiving purposes, update export files of all previously validated DES, and send these validated DES out to MDOT staff periodically.

If you have any questions, contact MDOT-eSign@michigan.gov. Please share this information with consultants and local agencies within your area.
e-Signature Validation Process Overview

1. Signing a PDF
   - Digital signature added to document using private key code (password) and affixing the hidden “public” key

2. Transmittal
   - Public Key embedded in PDF document

3. Receipt/Validation
   - Public key code embedded in document is compared to list of codes of validated
   - If codes match, the Signature will have a green checkmark indicating the signer has been validated.
   - If the codes do not match, the identity of the signer is unknown and must be manually validated by the receiver of the document before acceptance.