NCDOT eSignature Policy

NCDOT requires a digital signature solution in which the "root" digital certificate is provided by a certificate authority that meets assurance and trust requirements by Adobe. Documents with these certificates become automatically trusted by Adobe as this facilitates the ability to validate the signature. More information about Adobe's Approved Trust List and current members of that list can be found at http://helpx.adobe.com/acrobat/kb/approved-trust-list2.html.

The benefit of a solution described above is the ability for anyone to open a digitally signed PDF and observe a signature validity confirmation across the top of the file that indicates all signatures are signed and valid.

The State of NC and NCDOT have selected Docusign as our solution provider and it uses a root certificate from one of the Adobe Approved Trust List members. As such, all Docusign signed PDFs are publically verified and automatically trusted by Adobe.

Professional Engineering Firms and other external NCDOT partners that provide digitally signed materials to NCDOT must also meet these requirements. For digitally signed professionally sealed documents, the submitter is also responsible for ensuring compliance with relevant Board rules pertaining to digital signatures.

It should be noted that all digitally signed documents received by NCDOT should meet the requirements outlined herein. If NCDOT observes any indication that one or more signatures is invalid when opening the PDF, the PDF will not be accepted by NCDOT.

December 2014

Also, some vendors offer the ability to apply an additional password security to the document. Do not apply this additional password security as this prohibits NCDOT's ability to merge these documents into a combined PDF that can be used for viewing purposes only. Any documents that are received with this additional password security will not be accepted.

Updated: September 2015