Digital Plan Room FAQs

What is a Certificate Authority?
A Certificate Authority (CA) (or Certification Authority) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified.

Why isn't my digital signature passing validation
A certificate authority (CA) is a trusted entity that issues electronic documents to verify the identity of a digital entity. The CA that issued the certificate with which these signatures were signed is not trusted by the agency because it does not meet the professional board rules security standards. Self-signed documents are not accepted per the Florida Administrative Code 61G15-23.003. The new requirement states that you must have your own identity, digital seal and signature validated by a 3rd party Certificate Authority. Local Engineers, Architects, and Surveyors are using Entrust, GlobalSign, IdentTrust, TrustFactory and VeriSign.

DocuSign, is a secure signing service and is **not** recognized as a third-party certificate authority, or an SSL/TLS certificate which provides root certificates or private keys. If you research these authorities, you will see that DocuSign is more of a loan style signing service. It may have been accepted in the past in error, but the Digital Plan Room is designed to verify that proper certificates are being used.

Plans are signed, but I am receiving a message that they have been modified since they were signed.
Per the Florida Administrative Code (FAC), the digital signature is invalidated if any data in the document is changed after the signature has been added to the document. To resolve this error: remove the signature field from the document and re-sign the document.

Why am I receiving a message when validating plans that the root certificate cannot be trusted?
Self-signed certificates can no longer be accepted in accordance with FAC. The new requirement states that you must have your own identity, digital seal and signature validated by a Third-Party Certificate Authority (CA). Some design professionals have successfully used CoSign, DigiCert, Entrust, Exostar, GlobalSign and IdenTrust, as an example. (Note: These authorities are not being promoted by Charlotte County, nor are they the exclusive authority accepted.) For more information on digital signatures, please see the County's "Digital Seal and Signature Requirements" policy. If you are receiving this message and you are using a valid Third-Party CA, please contact our office.

Signature Date is in the Future.
The signature date on the document is in the future. A timestamp was not applied to the signature and the clock on your computer is set to a future date. Re-sign the document and include a valid timestamp.

Revocation checks could not be completed.
The system was unable to validate the certificate with the CA. The CA system may be down, or there was an error communicating with the CA. If the problem persists, please contact your CA.

File is not signed.
A digital signature is required for this document type. Please add a valid digital signature to the file. For instructions and information regarding digital signatures, please see the County's "Digital Seal and Signature Requirements" policy.

Certificate was expired at the date of signature.
The certificate with which these signatures were signed has expired. Each certificate has an expiration date. Make sure that the certificate is valid before signing the file. To resolve, please contact your CA.

Certificate was issued after signing date.
The certificate with which this signature was signed was not valid at the time the file was signed or there is an issue with the timestamp. Verify the certificate is valid before signing the file by contacting your CA. It is possible that the CA may need to re-issue your certificate.

Invalid certificate on signing date.
The certificate with which this signature was signed was not valid at the time the file was signed or there is an issue with the timestamp. Verify the certificate is valid before signing the file by contacting your CA. It is possible that the CA may need to re-issue your certificate.

FAQs – Plan Submittal

Why are my plans taking so long to process during the upload process?
File processing speed will vary depending on the file size and number of sheets. It is ok to navigate to other items while the plans are being processed. You will receive an email with a link when the file processing is complete.

What is an issue versus a condition?
Issues are code related concerns that must be corrected by correcting the appropriate drawings. Conditions are concerns that can be corrected in the field by the inspection staff and are similar to drawings.

What do I need to submit when I am uploading revised plans?
When submitting revised plans, provide written responses to each issue on the record and upload only the corrected sheets. Corrected sheets must still have third party verified digital signatures in order to upload the corrections. It is no longer necessary to resubmit the entire plan set.

Can I make mid-cycle changes and upload new plans?
The plan review cycle must be completed before new plans can be uploaded. Mid-cycle uploads are not permitted. At the conclusion of the plan review cycle, you will receive notification that the plan review cycle is complete.

An unexpected error occurred.
This error could signal an error on the Digital Plan Room server or an issue with the computer or connection used to submit it. Please try resubmitting a second time and if the problem persists, please contact our office.