

21M-100

Digitally Signing Electronic Contract Documents

Design Manual Chapter 21 Automation Tools Instructions Originally Issued: 07-17-18 Revised: 10-31-22

Digital contract documents must be digitally signed (locked) with a verifiable digital certificate to ensure integrity of the contents of the digital files. By Iowa Administrative Code <u>193C.6.1(9)</u>:

"Secure electronic signature. An electronic signature as defined in or governed by Iowa Code chapter 554D meets the signature requirements of this rule if it is protected by a security procedure, as defined in Iowa Code section 554D.103(14), such as digital signature technology. It is the licensee's responsibility to ensure, prior to affixing an electronic signature to an engineering or land surveying document, that security procedures are adequate to (1) verify the signature is that of a specific person and (2) detect any changes that may be made or attempted after the signature of the specific person is affixed."

The Iowa DOT has chosen a private certificate authority to provide a digital certificate that meets the criteria of IAC 193C.6.1(9) and Iowa Code <u>554D.103(14)</u>. Any digital certificate used by the Engineer of Record or their representative needs to meet the Iowa code requirements. The Engineer of Record or their representative in their organization will lock the files with a digital signature after the Engineer of Record approves of the final content within the files. The Engineer of Record will apply their Engineering seal and signature for the digitally locked documents through Appendix A of the Special Provision for Digital Contract Files.

Files that will be digitally signed (locked) are specified in the Special Provisions for Digital Contract Files:

- LandXML files
 - Proposed Geometry file(s).
 - Proposed surface files of grading (subgrade embankment) and top of grade (top of pavement & side slope embankment).
- DGN files
 - Three dimensional line string lines of break lines of proposed surfaces.

The Engineer of Record should include the names of all locked digital files in Appendix A of the Special Provisions for Digital Contract Documents that was under their direct supervision. For example, if the Engineer of Record did not oversee the existing ground terrain model, the Engineer of Record will not sign for that file; however, it would still be provided to the customer for information only.

Digitally Signing (Locking) LandXML Files

The utility to be used to digitally sign XML files can be accessed from the Office of Design folder (W:\Highway\Design\Office of Design\).

The utility is called FDOTXMLSigning.exe:

| Drganize 🔻 Burn New fold | ler . | | | | · | |
|----------------------------------|--|--------------------|-------------------|-------|-----|--|
| organize + Burn New fold | · | | | | 8 • | |
| 🔆 Favorites | Name | Date modified | Туре | Size | | |
| 🧮 Desktop | 퉬 Design Resources | 5/17/2016 1:37 AM | File folder | | | |
| 🗼 Downloads | 퉬 Print Servers | 5/31/2016 11:00 AM | File folder | | | |
| 🖳 Recent Places | _MicroStation V8 Tools | 4/29/2009 7:59 AM | Shortcut | 2 KB | | |
| | AutomationNewsletter | 2/25/2010 12:42 PM | Shortcut | 1 KB | | |
| 肩 Libraries 💦 🔪 | Contract Modifications | 5/18/2012 10:04 AM | Shortcut | 2 KB | | |
| Documents | 🛞 Cost Estimating | 1/26/2012 6:57 AM | Shortcut | 1 KB | | |
| a) Music | Delete RSC | 1/18/2013 1:55 PM | Shortcut | 2 KB | | |
| Pictures | DOT Employee Directory | 5/31/2016 10:13 AM | Internet Shortcut | 1 KB | | |
| 🛃 Videos | FDOTXMLSigning.exe | 6/7/2016 9:20 AM | Shortcut | 2 KB | | |
| | Porms | 2/17/2015 2:56 PM | Internet Shortcut | 1 KB | | |
| 🖳 Computer | 🔁 IDMS | 5/13/2009 8:35 AM | Shortcut | 1 KB | | |
| 🏜 Local Disk (C:) | 武 Kill Excel | 1/22/2010 12:24 PM | Shortcut | 1 KB | | |
| 雸 thamski (\\ntdfs\HomeFolde | Kill MicroStation | 11/12/2008 7:09 AM | Shortcut | 1 KB | | |
| 🚽 u (\\dot.int.lan\atscore) (U:) | 🔊 Kill MSforms Exd | 1/8/2015 10:07 AM | Shortcut | 2 KB | | |
| 🚽 (W)DataStor (\\ntdfs) (W:) | 🔒 Lock Computer | 1/13/2010 1:08 PM | Shortcut | 3 KB | | |
| 🚽 atscore (\\dot.int.lan) (Z:) | 👜 OpFin Menu Installation Instructions.doc | 8/16/2002 2:17 PM | Microsoft Word 9 | 28 KB | | |
| | Printers | 7/14/1997 1:27 PM | Shortcut | 1 KB | | |
| 📭 Network | 🛃 ProjectWise Training | 8/31/2012 8:12 AM | Shortcut | 3 KB | | |
| | 🛃 Safety Committee | 1/12/2005 2:10 PM | Shortcut | 1 KB | | |
| | 🖳 Service Survey.doc | 10/26/2005 8:18 AM | Microsoft Word 9 | 56 KB | | |
| | A Shall Latterr | 8/1/2011 12:22 DM | Internet Shortcut | 1 KR | | |

External users can download the program from the <u>https://iowadot.gov/design/automation-tools</u> under the Programs zip file <u>link</u>.

- Cell libraries (ZIP file)
- Color tables (ZIP file)
- Configuration (ZIP file)
- Cost estimating (ZIP file)
- Dgnlib (ZIP file)
- Documentation (ZIP file)
- GeoPak (ZIP file)
- gINT (ZIP file)

- IowaRCS (ZIP file)
- Macros (ZIP file)
- Printing (ZIP file)
- Programs (ZIP file)
- Resource files (ZIP file)
- Seed files (ZIP file)
- Survey (ZIP file)

Upon opening the utility, it will remember the last digital certificate used to sign files. The first time you use it, you will have to select the correct digital certificate for signing files.

| SFDOT XML Signing | |
|------------------------|--|
| File Options Help | |
| Sign Verify Results I | og |
| Choose Certificate | Apply Signature Show Certificate |
| Use XML Spy compatib | ility mode. |
| Certficate Information | |
| 📩 Issuer name | IdenTrust ACES CA 1 |
| 🔄 🔄 Subject name | Thomas M Hamski |
| Signing algorithm | sha256RSA |
| 🖉 Valid Date | 9/28/2015 |
| 🖉 Expire Date | 9/27/2017 |
| Service Provider | Microsoft Enhanced Cryptographic Provider v1.0 |
| | |
| • | 4 11 |
| | |
| Ready | |

Click the **Choose Certificate** button to select the appropriate certificate for signing.

| SFDOT XML Signing | |
|------------------------|--|
| File Options Help | |
| Sign Verify Results | Log |
| Choose Certificate | Apply Signature Show Certificate |
| Use XML Spy compatib | ility mode. |
| Certficate Information | |
| 📩 İssuer name | Iden Trust ACES CA 1 |
| 🔄 🔄 Subject name | Thomas M Hamski |
| Signing algorithm | sha256RSA |
| 🔮 Valid Date | 9/28/2015 |
| Expire Date | 9/27/2017 |
| Service Provider | Microsoft Enhanced Cryptographic Provider v1.0 |
| | |
| | |
| Ready | |

Digital Certificates

Select the digital certificate used for digital signature

Windows Certificate Store

Store Location: CurrentUser

Store Name: My

Ŧ

•

Current Only

Ŧ

X

Store location: Current User

Store name: My

Certificates: Your IdenTrust certificate

If your certificate is not visible in the dialog, refer to 21M-101 for instructions on exporting your certificate from Internet Explorer.

Certificates: Iden Trust ACES CA 1 Show PFX Digital Certificate File Select Show Save Password: Certficate Information lssuer name IdenTrust ACES CA 1 Subject name Thomas M Hamski sha256RSA Signing algorithm Valid Date 9/28/2015 Expire Date 9/27/2017 Service Provider Microsoft Enhanced Cryptographic Provider v1.0 ٠ 111 Þ

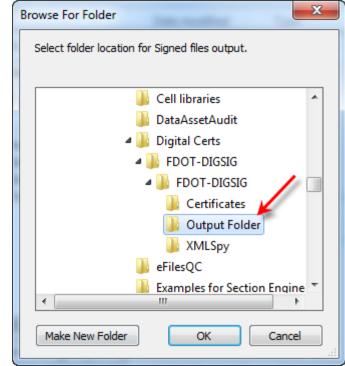
OK

Cancel

After selecting the appropriate certificate, an output folder must be selected. This is done by clicking on the Options menu and selecting Output Folder.

| | A FDOT XML Signing | | | | | | | | | |
|---|--------------------|---------------------|---------------------|-------------------------------------|--|--|--|--|--|--|
| | File | Options Help | | | | | | | | |
| | Sign Output Folder | | | | | | | | | |
| | Name | Output Suffix | • | Subject | | | | | | |
| | 🔘 XN | 1LFile4.xml | Thomas M Hamski | Iden Trust ACES CA 1 | | | | | | |
| | 🔘 XN | 1LFile3.xml | Thomas M Hamski | Iden Trust ACES CA 1 | | | | | | |
| | 🔿 XN | 1LFile2.xml | Thomas M Hamski | Iden Trust ACES CA 1 | | | | | | |
| | 🔘 XN | 1LFile1.xml | Thomas M Hamski | IdenTrust ACES CA 1 | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | - | | | • | | | | | | |
| | | | | | | | | | | |
| | Output | folder - W:\Highway | Design\AutomationSe | ection\Personnel\Tho _{.::} | | | | | | |
| C | _ | | _ | | | | | | | |

Select the appropriate folder to place the signed XML files. This utility is not integrated with ProjectWise. All locations must be on either the local computer or a network drive location.



To sign XML files *Click* on the **Apply Signature** button.

| SFDOT XML Signing | | | | | | | |
|--|--|--|--|--|--|--|--|
| File Options Help | | | | | | | |
| Sign Verify Results | Log | | | | | | |
| Choose Certificate | Apply Signature Show Certificate | | | | | | |
| Vise XML Spy compatit | bility mode. | | | | | | |
| Certficate Information | | | | | | | |
| 📩 Issuer name | IdenTrust ACES CA 1 | | | | | | |
| Subject name | Thomas M Hamski | | | | | | |
| Signing algorithm | sha256RSA | | | | | | |
| 🗳 Valid Date | 9/28/2015 | | | | | | |
| 🗳 Expire Date | 9/27/2017 | | | | | | |
| Service Provider | Microsoft Enhanced Cryptographic Provider v1.0 | | | | | | |
| | | | | | | | |
| | · · · · · · · · · · · · · · · · · · · | | | | | | |
| Output folder - W:\Highway\Design\AutomationSection\Personnel\Tho,;; | | | | | | | |

Select the files to be signed. Multiple files can be signed at once. The files to be signed must be outside of ProjectWise because the signing program is not ProjectWise integrated.

| Organize 🔻 New fold | 21 | | | |
|--------------------------|--|-----------------------------------|-------------------|------|
| | Name | Date modified | Туре | Size |
| 🔆 Favorites | | | | 0.20 |
| E Desktop | XMLFile1_Signed.xml | 5/16/2016 10:08 AM | XML Document | |
| 🗼 Downloads | XMLFile2_Signed.xml | 5/16/2016 10:08 AM | XML Document | |
| 🖳 Recent Places | XMLFile3_Signed.xml | 5/16/2016 10:08 AM | XML Document | |
| | XMLFile4_Signed.xml | 5/16/2016 10:08 AM | XML Document | |
| 🥱 Libraries | 46-1697-044_CoordinateGeometry_Signed.xml | 9/29/2015 11:23 AM | XML Document | 4 |
| Documents | 46-1697-044_CoordinateGeometry2.xml | 10/10/2014 1:06 PM | XML Document | 4 |
| 🖻 🎝 Music | 46-1697-044 Subgrade_model_Signed.xml | 10/6/2014 7:16 AM | XML Document | 3,22 |
| Pictures | XMLFile4.xml | 9/23/2014 3:20 PM | XML Document | |
| Videos | XMLFile3.xml | 9/23/2014 3:19 PM | XML Document | |
| | XMLFile2.xml | 9/23/2014 3:19 PM | XML Document | |
| 🖳 Computer | XMLFile1.xml | 9/23/2014 3:18 PM | XML Document | |
| 🛛 🏭 Local Disk (C:) | 46-1697-044_CoordinateGeometry.xml | 7/7/2013 5:57 AM | XML Document | 4 |
| 🖻 坖 thamski (\\ntdfs) | 46-1697-044_Subgrade_model.xml | 7/7/2013 5:57 AM | XML Document | 3,22 |
| ⊳ 🖵 u (\\dot.int.lan\a | \mu Certificates | 5/17/2016 1:51 PM | File folder | |
| ▷ 🖵 (W)DataStor (\\n | MLSpy | 5/17/2016 1:51 PM | File folder | |
| ▷ 💭 atscore (\\dot.int * | ۰ (III) III III III III III III III III | 1 | | • |
| Elle a | ame: "XMLFile4.xml" "XMLFile3.xml" "XMLFile2.xml" "XMLFile1.xml" | | XML Files [*.xml] | |

Enter your certificate's password.

| Signing data v | with your private exchange | key 🔀 |
|----------------|--|-------------------------------|
| | An application is requestin | g access to a Protected item. |
| | | |
| | Password for: CryptoAPI Private Key | Remember password |
| | | |
| | ОК | Cancel Details |

The utility has now applied your digital certificate to the XML files.

| S FDOT XML Signing | 1000 | | | | | | | |
|-------------------------|-----------------|---------------------|--|--|--|--|--|--|
| File Options Help | | | | | | | | |
| Sign Verify Results Log | | | | | | | | |
| Name | lssuer | Subject | | | | | | |
| 🖉 XMLFile4.xml | Thomas M Hamski | IdenTrust ACES CA 1 | | | | | | |
| 🛇 XMLFile3.xml | Thomas M Hamski | IdenTrust ACES CA 1 | | | | | | |
| 🛇 XMLFile2.xml | Thomas M Hamski | IdenTrust ACES CA 1 | | | | | | |
| 🛇 XMLFile1.xml | Thomas M Hamski | IdenTrust ACES CA 1 | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| < > | | | | | | | | |
| All XML files signed. | | | | | | | | |

3D DGN Files

MicroStation files can only be signed one at a time. Open the files to be signed one at a time and repeat the following steps.

| 🚮 Dra | wing | v 💽 🔽 | | à 🛧 - 🔶 : | 1 🔒 🕻 | • 🔝 🗖 | | (| C:\Users\tha | mski\Onel | Drive - Iow | va Departr | ment of Transp | ortation | Desktop\PV |
|------------|----------------------|-----------------------|-----------|--------------|-------|--------------|--------------|------------|----------------|-----------|-------------|----------------|----------------|-----------------|---------------------|
| File | Home | View Annotate | Attach | Analyze | Curve | s Con | straints | Utilities | Drawing | Aids (| Content | Mesh | Collabora | ate H | lelp |
| | (x) | MDL Applications | <u></u> | | | | Record | d ■ Stop | | | P | 72 🤹 To Ta | æ | * | |
| OLE | Named Expressions | ; 🏺 Connect to Browse | r Display | Convert Capt | ure 🐻 | 🔠 Open | DynamicX | (SMoc 🔨 🥖 | VBA Manager | Commit | Initialize | 7 | Signatures Si | gnature Cell | Coordinat System |
| | l | Utilities | | Image | | | Mac | cros | Fa | Desig | gn History | r Gi | Securi | ty | Geo |
| Explorer | | | | | | - 4 × | View | 1. Default | | | | | | / | |
| 🛛 🛛 🔀 File | | | | | | * | ⊡ ▼ (| 9 ≩ + . | ⊒ ,⊕ ,⊝ | P 🗔 < |) 🔊 🖪 |) () (| <u> 🔍 🔁</u> | | |
| 😝 Ite | ms | | | | | * | | , I I | - • • | | | _ | - 0+ | | |
| 🗑 Re: | sources | | | | | * | ß | Element S | election | _ | × | (| | | 0 |

Digital signatures in MicroStation are accessed from the **Drawing Workflow > Utilities Ribbon Tab > Signatures.**

| 📕 Digital Signatures | | | | | | | | | | | | _ _ X |
|----------------------|----------|---------|---------|--------|-------|------|-------------|--------|----------|------|--------|--------------|
| 🚺 🖪 🔆 🗙 🖗 🖻 | Ē | | | | | | | | | | | |
| Hierarchy | Verified | Trusted | Current | Source | Scope | Refs | Certificate | Signer | Location | Date | Expiry | Purpose |
| Herato | Ventied | Trusted | Current | Source | Scope | Refs | Certificate | Signer | Location | Date | Expiry | Purpose |
| | | | | | | | | | | | | |
| Click on Add File Si | anatur | | on | | | | | | | | | |

Click on Add File Signature button.

Click on the magnifying glass next to Certificate field.

| Add File Sig | nature |
|--------------|---------------------|
| Certificate | ٩ |
| Signer: | thamski |
| Location: | HDC18070 |
| Purpose: | |
| Expiry: | YYYY/MM/DD |
| | Dependent Signature |
| | Include References |
| | OK Cancel |

| Select your IdenTrust certificate to apply to the file | Certificates | | | | | | | | |
|--|------------------|----------------------|------------|------|--|--|--|--|--|
| and Click OK. | Issued To | Issued By | Expiration | Key? | | | | | |
| | 🛤 Thomas M Hamsk | Iden Trust ACES CA 1 | 2017/09/27 | R | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | 1 | | | View | | | | | |
| | | | | | | | | | |
| | | <u>0</u> K | Cancel | | | | | | |

Click **OK** to apply the digital signature.

| Add File Signature | | | | | | | |
|--------------------|--------------|---------------------|--|--|--|--|--|
| | Certificate: | Thomas M Hamski | | | | | |
| | Signer: | thamski | | | | | |
| | Location: | HDC18070 | | | | | |
| | Purpose: | | | | | | |
| | Expiry: | YYYY/MM/DD | | | | | |
| | | Dependent Signature | | | | | |
| | | Include References | | | | | |
| | | OK Cancel | | | | | |

You will be prompted to enter your digital certificate's password. *Click* **OK**.



| rchy | Verified | Trusted | Current | Source | Scope | Refs | Certificate | Signer | Location | Date | Expiry | Purpose |
|------|----------|----------|----------|--------|-------|------|-------------|--------|----------|------------------|--------|---------|
| | I | v | v | | 4 | | Thomas | | HDC18070 | 2016/06/08 09:12 | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

The Digital Signatures dialog will now show that the file has been digitally signed. Close the file.

Note: Do not save settings or modify the file in any way or the digital signature will be invalidated.

The file should now be set to read only. In windows Explorer right click on the file and select **Properties.**

| 🕼 test signature. | dan | 6/8/2016 9:14 AM | Bentlev N | licroStati |
|-------------------|-----|--|-----------|------------|
| | | Open with MicroStation V8i (SELECTseries 3) Print with MicroStation V8i (SELECTseries 3) Open with | | |
| | ۵ | Scan for threats | | |
| | | Restore previous versions Send to | • | |
| | | Cut Copy | | |
| | | Create shortcut Delete | | |
| | | Properties Properties | | |

On the General tab under Attributes, check the **Read-only** check box and *Click* **OK.**

| 1/2 test signature.dgn Properties | | | | | | | | | |
|-----------------------------------|---|--|--|--|--|--|--|--|--|
| General Secu | rity Custom Details Previous Versions | | | | | | | | |
| JU. | test signature.dgn | | | | | | | | |
| Type of file: | Bentley MicroStation Design (.dgn) | | | | | | | | |
| Opens with: | MicroStation V8i (SELE) Change | | | | | | | | |
| Location: | W:\Highway\Design\AutomationSection\Personnel | | | | | | | | |
| Size: | 69.0 KB (70,656 bytes) | | | | | | | | |
| Size on disk: | 72.0 KB (73,728 bytes) | | | | | | | | |
| Created: | Wednesday, October 15, 2014, 10:37:36 AM | | | | | | | | |
| Modified: | Today, June 08, 2016, 9:14:13 AM | | | | | | | | |
| Accessed: | Wednesday, October 15, 2014, 10:37:36 AM | | | | | | | | |
| Attributes: | Read-only Hidden Advanced | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | OK Cancel Apply | | | | | | | | |

Chronology of Changes to Design Manual Section:

021M-100 Digitally Signing Electronic Contract Documents

10/31/2022

Revised

Updated page 8 for the location of the digital signature tool for ORD Connect.

7/17/2018 NEW

New.