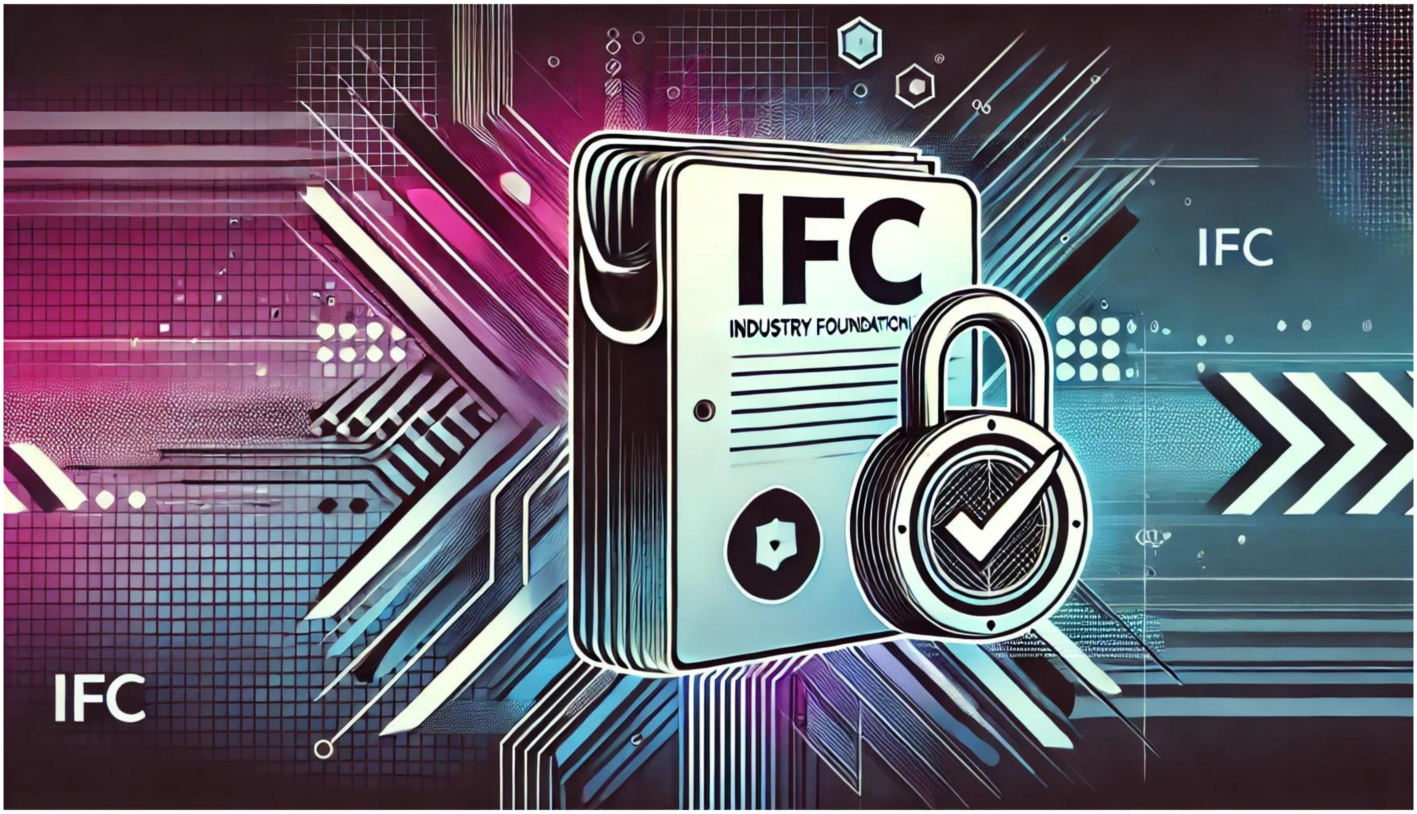
IFC DIGITAL SIGNATURE proof of concept report

DIGITALLY SIGNING IFC AND IFCZIP FILES

Completed:
May 6th, 2025

Prepared by
Constantinescu Ștefan
Peer-reviewer
Theodorou Dimitrios
Ifc originator
Vlăsceanu Dan



BIMTECH the home of BuildingSMART Romania buildingSMART Romania

Literature review

https://technical.buildingsmart.org/standards/IFC/IFC-formats/

https://www.buildingsmart.org/wp-content/uploads/2024/09/20240828_Denver_ImplementerAssembly_day1.5_Implementers-Forum.pdf

https://www.buildingsmart.org/wp-content/uploads/2025/03/IFC-Mandate_2025.pdf

Technical details provided by Digital Signature Company, DigiSIGN:

P7m (.p7m or application/pkcs7-mime): This format, defined by the PKCS#7 standard, contains the original data (for example, a document) together with the digital signature. It is a "detached signature" format.

P7s (.p7s or application/pkcs7-signature): This format, also based on PKCS#7, contains only the digital signature, separate from the original data. It is likewise a "detached signature" format.

XML (.xml or application/xml): XML (Extensible Markup Language) is a markup language designed to be both human and machine-readable. In the context of electronic signatures, XML serves as the basis for the XAdES (XML Advanced Electronic Signatures) format. In XML signature files, the signed data and signature information (including the certificate, signature algorithm, any timestamps, etc.) are stored in an XML structure.

PKCS#7 is a foundational standard for cryptographic message syntax.

CAdES (CMS Advanced Electronic Signatures) is an extension of CMS (which itself is based on PKCS#7), optimized for advanced electronic signatures with strong long-term validation support (even after the signing certificate has expired). Typically, it stores both the data and the signature in binary form.

XAdES is an extension of XML-DSig, providing advanced electronic signatures in XML format, with flexibility in managing the signed data and support for long-term validation

Introduction

The scope of this report is to understand if digitally signing IFCs can be a method for securing the authenticity of the file in relation to public authorities in the context of using IFC files as a deliverable for digital building permits and for digital archiving purposes. This does not limit the encrypting or archiving use cases in any way, the method could also be used as a way to ensure contractual agreements have been met between private parties or even public and private interactions.

Significance

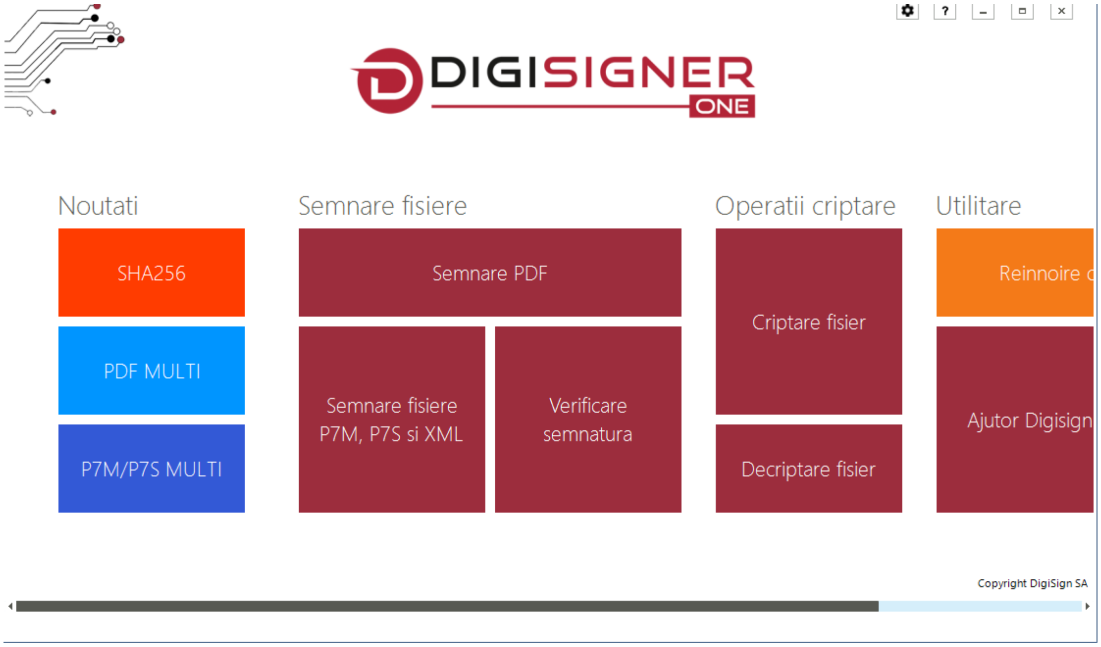
BIM and openBIM-based **Digital Building Permits** are a current topic and more and more municipalities (Dubai, Viena) and countries (Finland, Estonia, Singapore, Hong Kong, South Korea) are adopting this procedure between private entities and public authorities. This trend is also endorsed by openBIM mandates.
The end goal is public authorities can leverage the high bandwidth communication of information empowered by openBIM models, based on open standards (IFC) as a way of issuing permitting and also securely archiving the projects in different phases. IFC files are the STEP Physical File (SPF) representation of the ISO 16739-1 standard, and have the capability to geometrically represent facilities, buildings and elements of buildings as well as the attributes and documentation of these elements and relationship

between them. This makes it a powerful standard for understanding designer intent and for code checking.

Summary

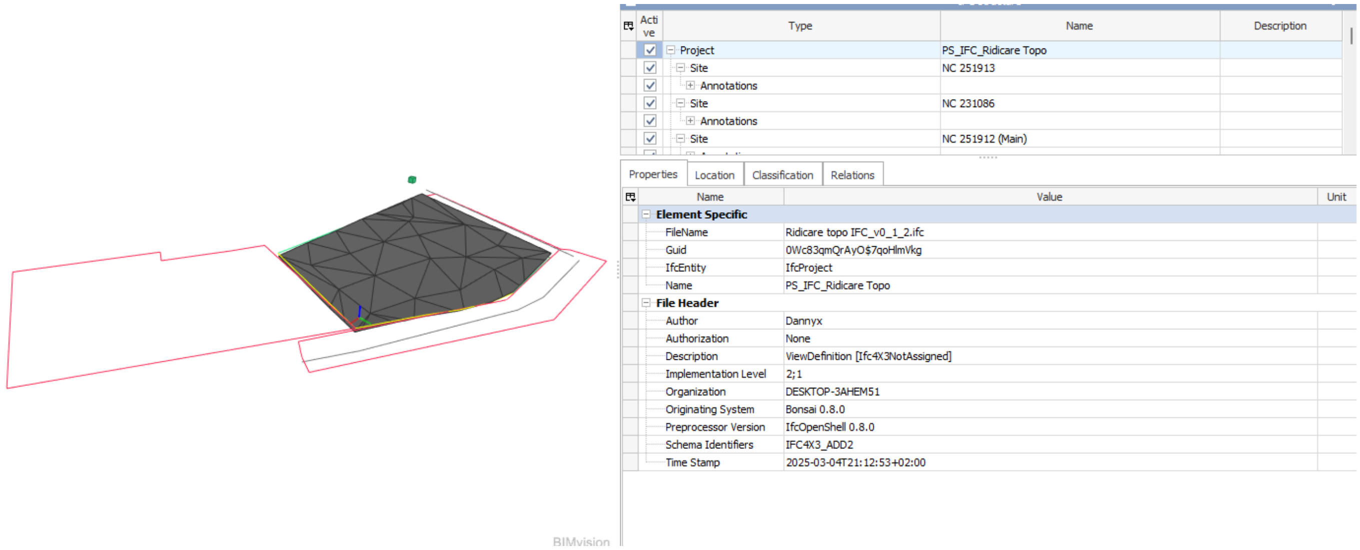
The subject is under discussion in the buildingSMART Implementer Assembly.

IFC and IFCZIP files can be digitally signed using a digital signature with a tool provided by a digital certificate vendor. In this study case, a local, Romanian vendor was used.



Screenshot of digital certificate vendor interface

Methodology

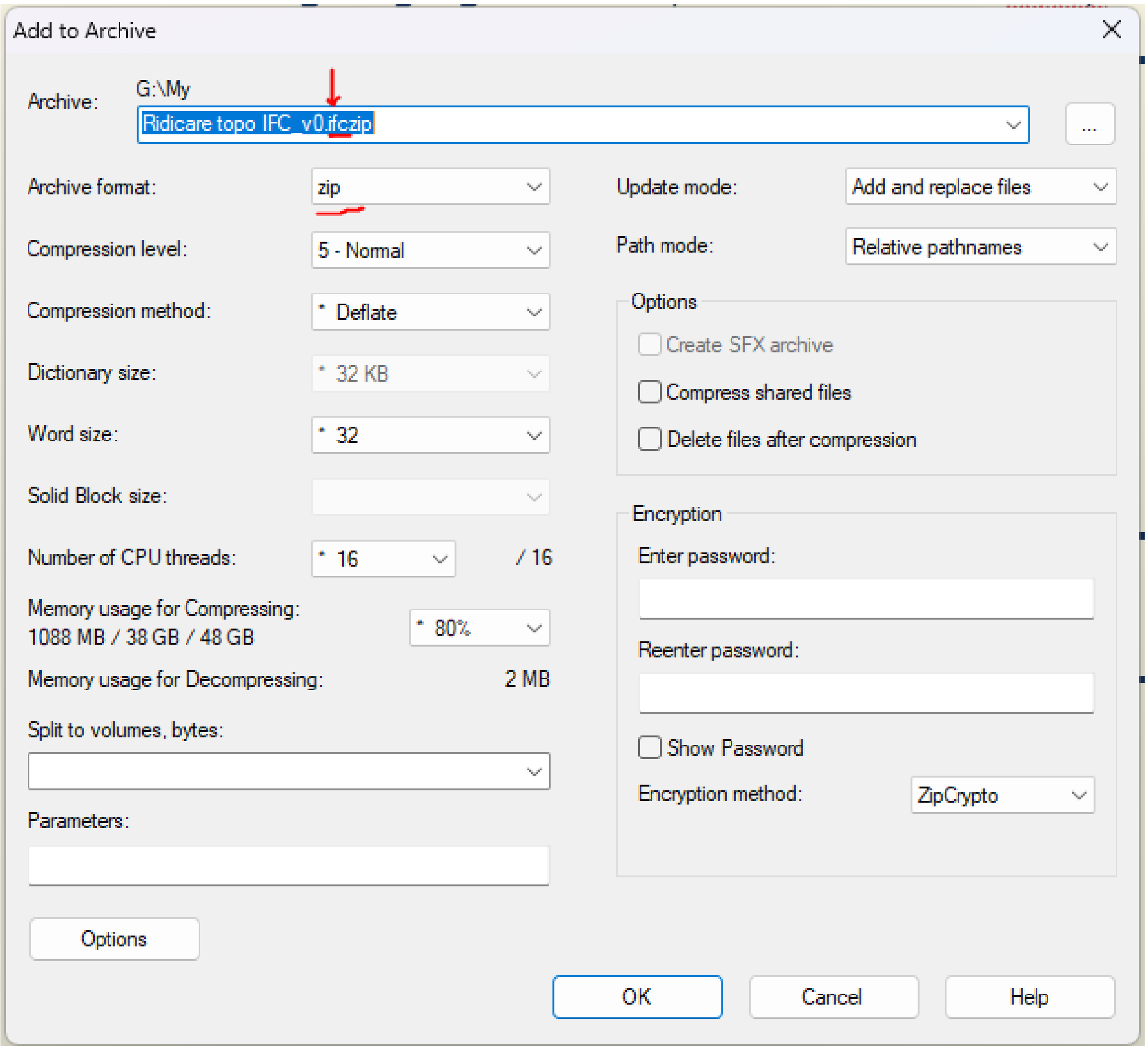


Active	Type	Name	Description
☑	⊟ Project	PS_IFC_Ridicare Topo	
☑	⊟ Site	NC 251913	
☑	⊞ Annotations		
☑	⊟ Site	NC 231086	
☑	⊞ Annotations		
☑	⊟ Site	NC 251912 (Main)	

Name	Value	Unit
⊟ **Element Specific**		
FileName	Ridicare topo IFC_v0_1_2.ifc	
Guid	0Wc83qmQrAyO$7qoHlmVkg	
IfcEntity	IfcProject	
Name	PS_IFC_Ridicare Topo	
⊟ **File Header**		
Author	Dannyx	
Authorization	None	
Description	ViewDefinition [Ifc4X3NotAssigned]	
Implementation Level	2;1	
Organization	DESKTOP-3AHEM51	
Originating System	Bonsai 0.8.0	
Preprocessor Version	IfcOpenShell 0.8.0	
Schema Identifiers	IFC4X3_ADD2	
Time Stamp	2025-03-04T21:12:53+02:00	

An IFC file created for a Site Plan workshop was used as a base for testing. The IFC schema used is 4x3_ADD2 and contains entities such as IfcSite, IfcGeorgraphicElement and IfcAnnotations.

- Only one IFC base file used
- The IFC was archived using **7-Zip** - a free, open-source software as an *.IFCzip. ZipCrypto was the encryption method selected, archive format: zip, and before archiving ”IFC” was manually added in the filename extension of the future archive.



Add to Archive

Archive: G:\My
Ridicare topo IFC_v0.ifczip

Archive format: zip

Compression level: 5 - Normal

Compression method: * Deflate

Dictionary size: * 32 KB

Word size: * 32

Solid Block size:

Number of CPU threads: * 16 / 16

Memory usage for Compressing: 1088 MB / 38 GB / 48 GB * 80%

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

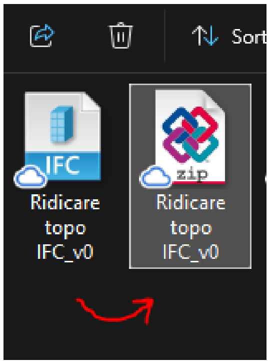
Path mode: Relative pathnames

Options
☐ Create SFX archive
☐ Compress shared files
☐ Delete files after compression

Encryption
Enter password:
Reenter password:
☐ Show Password
Encryption method: ZipCrypto

Screenshot of 7-Zip archiving process

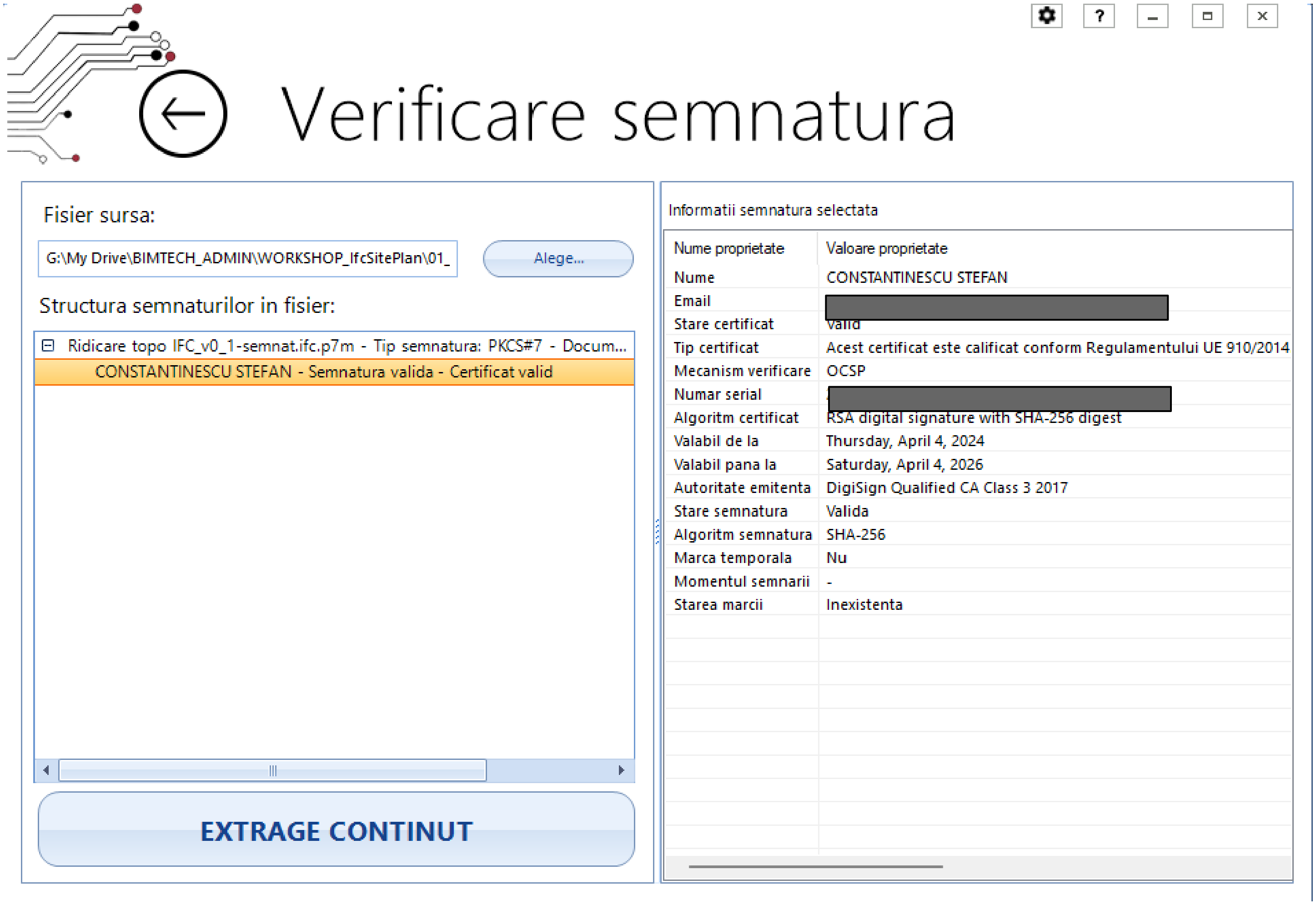
This created the file *Ridicare topo IFC_v0.ifczip* that automatically converted to this thumbnail:



Note: This file can still be opened and visualized by IFC visualisation tools

After this, both files were digitally signed with the DigiSIGNER ONE software with the PKCS #7 Signed Message format (*.p7m).

You can digitally sign either a plain *.IFC file or an *.IFCzip using a digital certificate tool, for this report, the encryption algorithm of the digital certificate software uses SHA-256 encryption algorithm.



Fisier sursa:

G:\My Drive\BIMTECH_ADMIN\WORKSHOP_IfcSitePlan\01_

Structura semnaturilor in fisier:

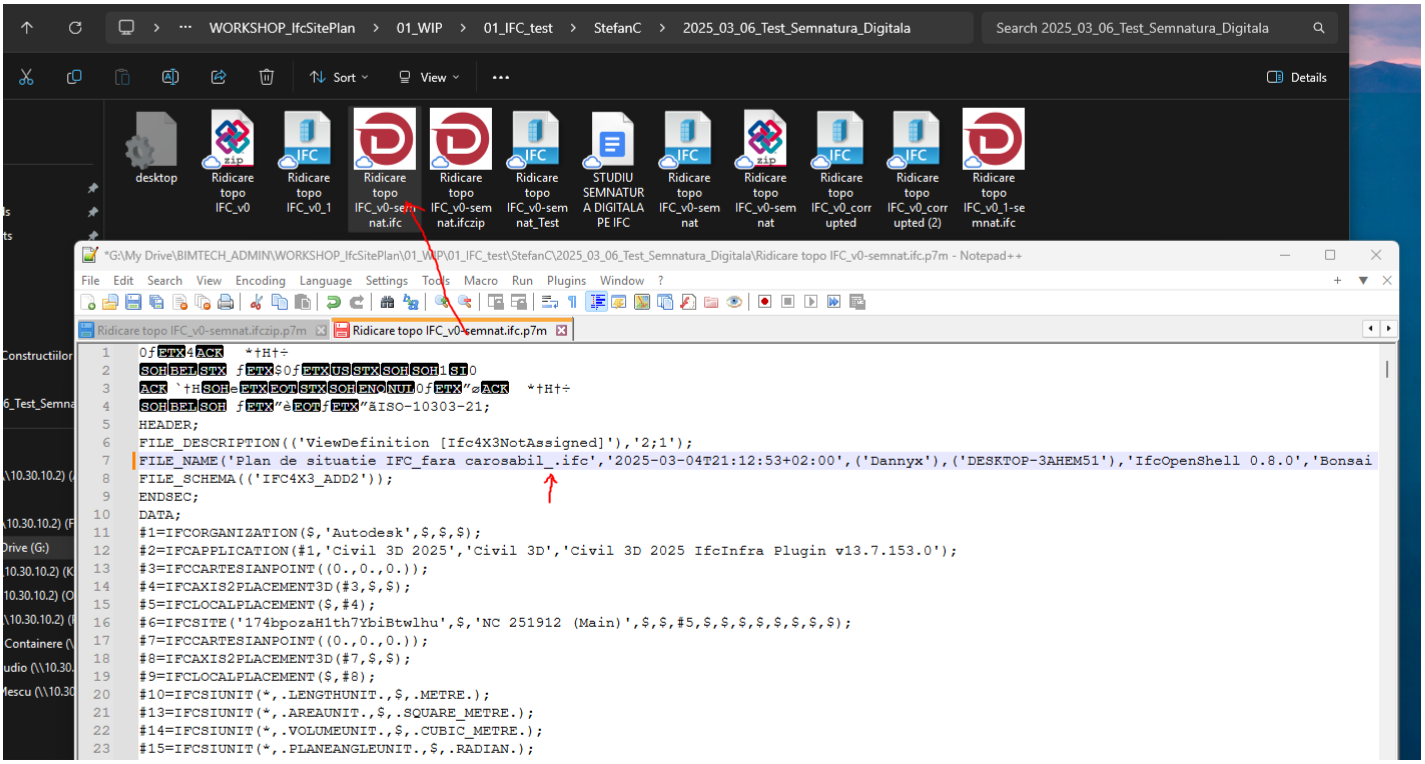
⊟ Ridicare topo IFC_v0_1-semnat.ifc.p7m - Tip semnatura: PKCS#7 - Docum...

CONSTANTINESCU STEFAN - Semnatura valida - Certificat valid

Informatii semnatura selectata

Nume proprietate	Valoare proprietate
Nume	CONSTANTINESCU STEFAN
Email	[redacted]
Stare certificat	[redacted]
Tip certificat	Acest certificat este calificat conform Regulamentului UE 910/2014
Mecanism verificare	OCSP
Numar serial	[redacted]
Algoritm certificat	RSA digital signature with SHA-256 digest
Valabil de la	Thursday, April 4, 2024
Valabil pana la	Saturday, April 4, 2026
Autoritate emitenta	DigiSign Qualified CA Class 3 2017
Stare semnatura	Valida
Algoritm semnatura	SHA-256
Marca temporala	Nu
Momentul semnarii	-
Starea marcii	Inexistenta

After this, a single character was modified in both the *.IFC file and the *.IFCzip, using Notepad++:

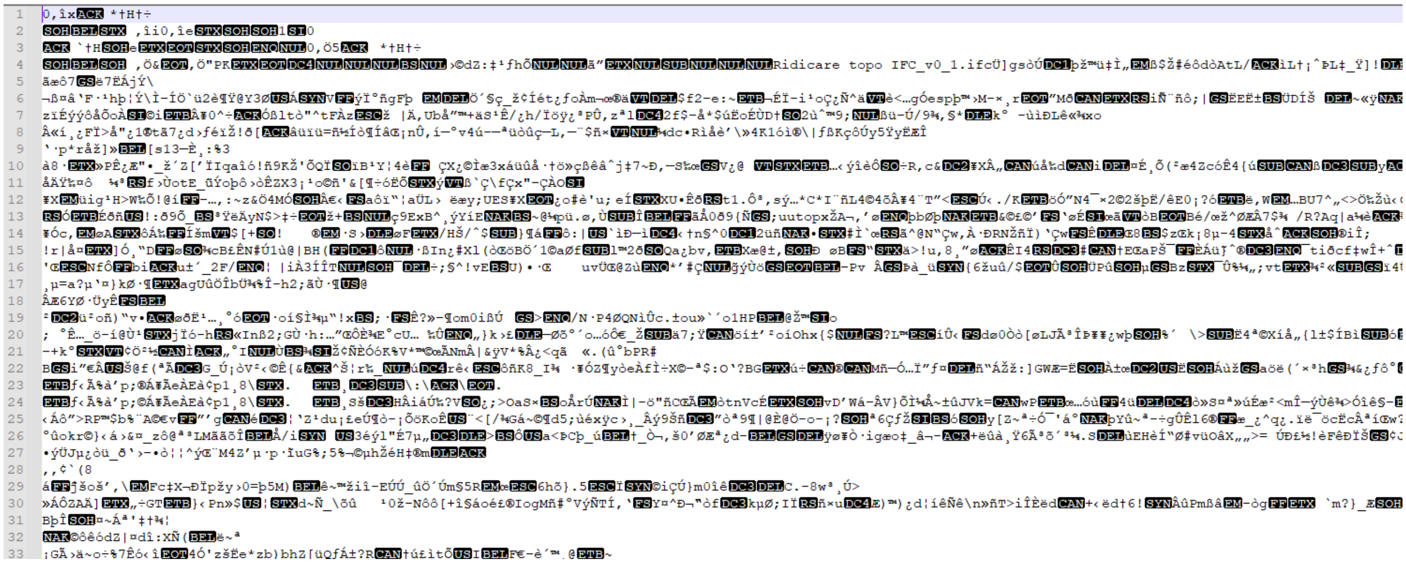


WORKSHOP_IfcSitePlan > 01_WIP > 01_IFC_test > StefanC > 2025_03_06_Test_Semnatura_Digitala
Search 2025_03_06_Test_Semnatura_Digitala
Sort
View
Details
desktop
Ridicare topo IFC_v0
Ridicare topo IFC_v0_1
Ridicare topo IFC_v0-semnat.ifc
Ridicare topo IFC_v0-semnat.ifczip
Ridicare topo IFC_v0-semnat_Test
STUDIU SEMNATURA DIGITALA PE IFC
Ridicare topo IFC_v0-semnat
Ridicare topo IFC_v0-semnat
Ridicare topo IFC_v0_corrupted
Ridicare topo IFC_v0_corrupted (2)
Ridicare topo IFC_v0_1-semnat.ifc
*G:\My Drive\BIMTECH_ADMIN\WORKSHOP_IfcSitePlan\01_WIP\01_IFC_test\StefanC\2025_03_06_Test_Semnatura_Digitala\Ridicare topo IFC_v0-semnat.ifc.p7m - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Ridicare topo IFC_v0-semnat.ifczip.p7m
Ridicare topo IFC_v0-semnat.ifc.p7m

```
0ƒETX4ACK   *†H†÷
SOHBELSTX ƒETX$0ƒETXUSSTXSOHSOH1SI0
ACK `†HSOHeETXEOTSTXSOHENQNUL0ƒETX”⌀ACK   *†H†÷
SOHBELSOH ƒETX”èEOTƒETX”ãISO-10303-21;
HEADER;
FILE_DESCRIPTION(('ViewDefinition [Ifc4X3NotAssigned]'),'2;1');
FILE_NAME('Plan de situatie IFC_fara carosabil_.ifc','2025-03-04T21:12:53+02:00',('Dannyx'),('DESKTOP-3AHEM51'),'IfcOpenShell 0.8.0','Bonsai
FILE_SCHEMA(('IFC4X3_ADD2'));
ENDSEC;
DATA;
#1=IFCORGANIZATION($,'Autodesk',$,$,$);
#2=IFCAPPLICATION(#1,'Civil 3D 2025','Civil 3D','Civil 3D 2025 IfcInfra Plugin v13.7.153.0');
#3=IFCCARTESIANPOINT((0.,0.,0.));
#4=IFCAXIS2PLACEMENT3D(#3,$,$);
#5=IFCLOCALPLACEMENT($,#4);
#6=IFCSITE('174bpozaH1th7YbiBtwlhu',$,'NC 251912 (Main)',$,$,#5,$,$,$,$,$,$,$,$);
#7=IFCCARTESIANPOINT((0.,0.,0.));
#8=IFCAXIS2PLACEMENT3D(#7,$,$);
#9=IFCLOCALPLACEMENT($,#8);
#10=IFCSIUNIT(*,.LENGTHUNIT.,$,.METRE.);
#13=IFCSIUNIT(*,.AREAUNIT.,$,.SQUARE_METRE.);
#14=IFCSIUNIT(*,.VOLUMEUNIT.,$,.CUBIC_METRE.);
#15=IFCSIUNIT(*,.PLANEANGLEUNIT.,$,.RADIAN.);
```

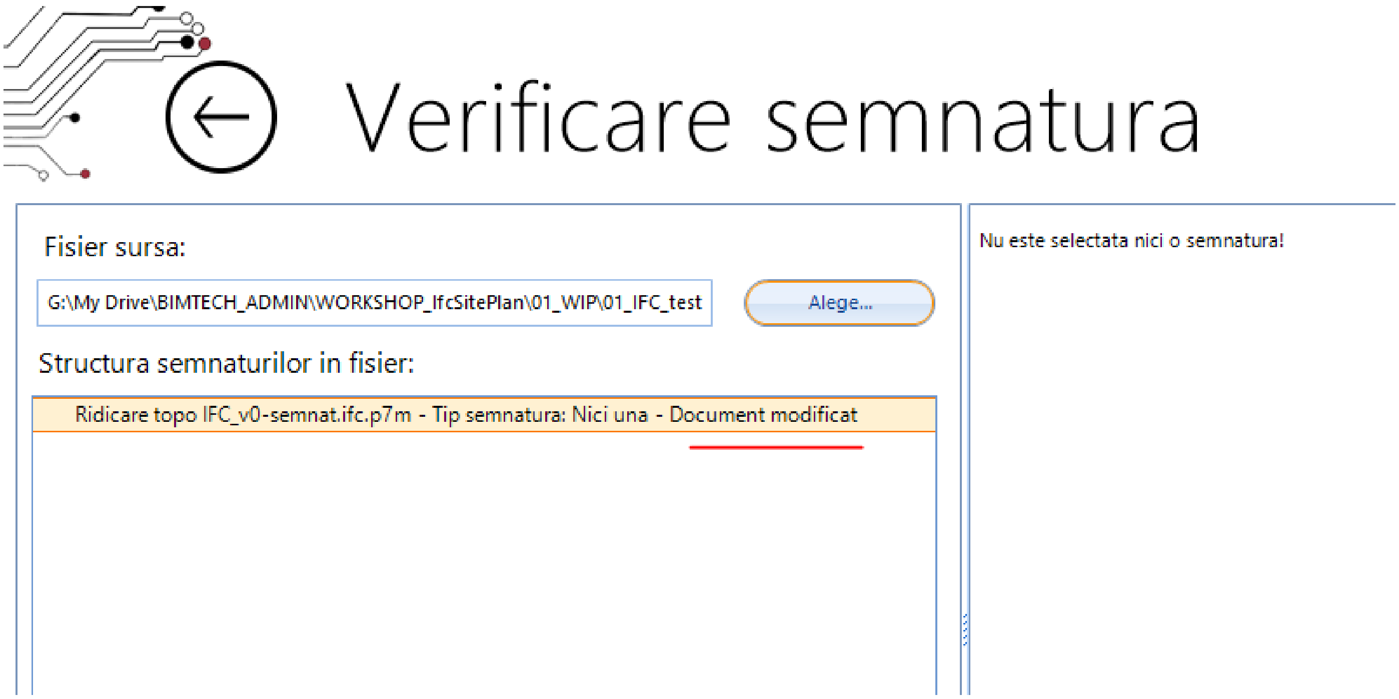
Modified one character in the IFC file, added an “_” (underscore).

In the *.IFCzip, which shows binary data when opened with Notepad++, a single character was also modified somewhere in the beginning of the file (added a “_”).



```
0,îxACK *†H†÷
SOHBELSTX ,ìi0,ìeSTXSOHSOH1SI0
ACK `†HSOHeETXEOTSTXSOHENQNUL0,Ö5ACK  *†H†÷
SOHBELSOH ,Ö&EOT,Ö"PKETXEOTDC4NULNULNULBSNUL›©dZ:‡¹fhÕNULNULã”ETXNULSUBNULNULNULRidicare topo IFC_v0_1.ifcÜ]gsòÚDC1þž™ü‡Ì„EMß$Ž#éôdòAtL/ACKìL†¡ˆÞL‡_Ÿ]!DLE
ãæô7GSë7ËÁjÝ\
```

Findings



Verificare semnatura

Fisier sursa:

G:\My Drive\BIMTECH_ADMIN\WORKSHOP_IfcSitePlan\01_WIP\01_IFC_test

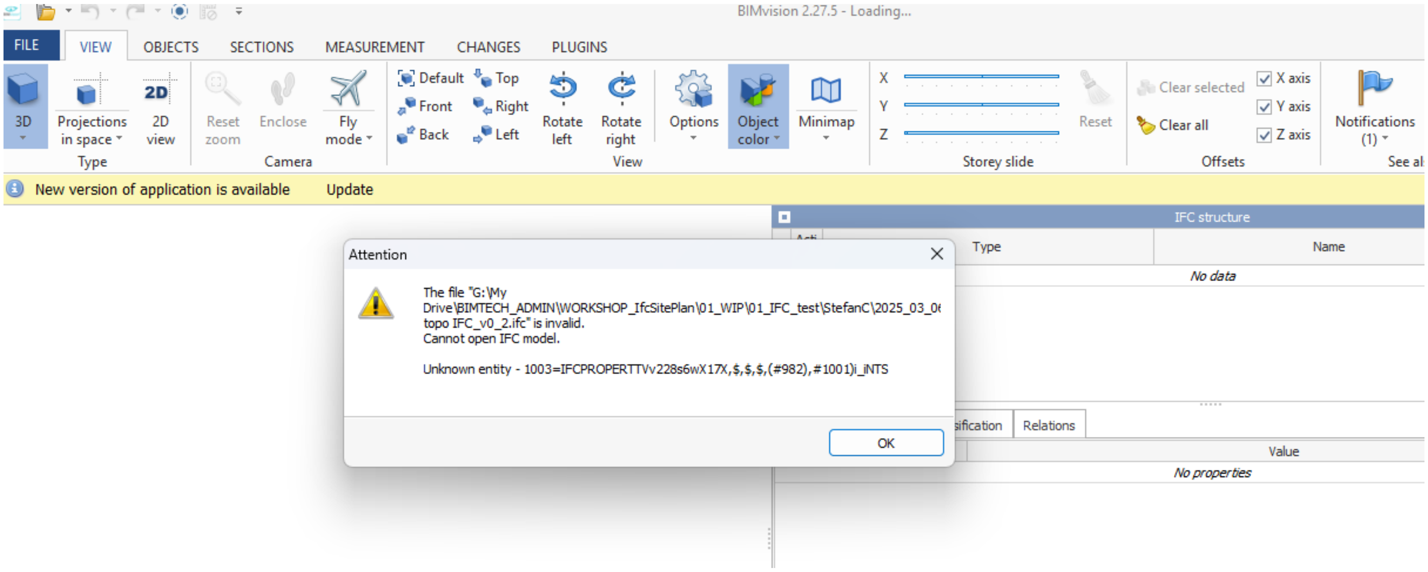
Structura semnaturilor in fisier:

Ridicare topo IFC_v0-semnat.ifc.p7m - Tip semnatura: Nici una - Document modificat

Nu este selectata nici o semnatura!

After the file alterations, when trying to extract contents of the *.p7m file with the digital signature software, a warning ”modified document” as shown in the screenshot above appeared. Nevertheless, the process still produces an IFC file.

After modifying a character in the digitally signed file, you can still extract it, but an error message “cannot open IFC file” will be shown when opening it.



New version of application is available Update

```
The file "G:\My
Drive\BIMTECH_ADMIN\WORKSHOP_IfcSitePlan\01_WIP\01_IFC_test\StefanC\2025_03_0(
topo IFC_v0_2.ifc" is invalid.
Cannot open IFC model.

Unknown entity - 1003=IFCPROPERTTVv228s6wX17X,$,$,$,(#982),#1001)i_iNTS
```

Error from BIM Vision: Cannot open IFC model.

Insights and analysis

Upon digital signing, the files are encapsulated into a PKCS #7 Signed Message format (*.p7m), which is the attached variant of the signature (only one file created).

IFC viewers like Blender with Bonsai extension and BIMvision cannot directly open the digitally signed (*.p7m) files, as they have been altered with the ”hash” generated by digitally signing them.

To access the original .IFC file, the proprietary software provided by the digital certificate issuing vendor needs to be used for the extraction.

On the other hand, extracting the contents of the *.p7m file based on the *.IFCzip can be done using free open-source archiving software (such as 7-Zip), which appears to recognize that the contents of the *.p7m file is a compressed IFC (.IFCzip) and provides the ability to extract it, thus bypassing the need for the public authority to have any proprietary digital certificate software installed.

When the digital certificate token was disconnected from the workstation, the extraction could be followed through, thus the*.p7m file can be extracted using only the 7-Zip application.

The Digitally signed files remain editable using standard text editors (tested with Notepad++). However, even a single character change corrupts the digital signature (obviously) and either generates an error message, or it renders the file unusable.

After modification and extracting the *.IFCzip from the altered (*.p7m) files, IFC viewers are no longer able to open the IFC if it had any alterations.

Digital Certificate Software detects file alterations in both .IFC and .IFCzip files and reports the digital signature as invalid if any changes have occurred.

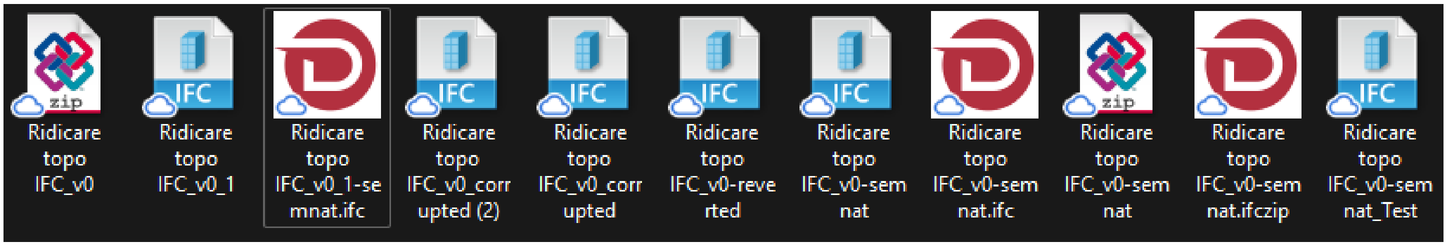
Other insights

*.IFCzip files differ from *.IFC files by being archived (through the Zip compression algorithm), making the express language of IFC schema unreadable when viewed in a text editor, and also significantly shrinking the file size. (sometimes to only 20% of the original file size)

Limitations

- Only one digital certificate software was used
- Only one *.IFC file tested
- Only one digital signature used

Conclusions


Ridicare topo IFC_v0
Ridicare topo IFC_v0_1
Ridicare topo IFC_v0_1-semnat.ifc
Ridicare topo IFC_v0_corrupted (2)
Ridicare topo IFC_v0_corrupted
Ridicare topo IFC_v0-reverted
Ridicare topo IFC_v0-semnat
Ridicare topo IFC_v0-semnat.ifc
Ridicare topo IFC_v0-semnat
Ridicare topo IFC_v0-semnat.ifczip
Ridicare topo IFC_v0-semnat_Test

This is a first effort of testing digital signatures by buildingSMART Romania **Tools and Standards Domain** with a single IFC file and only one party digitally signing. Even so, the tests show that the digital signing technology provided by the digital certificate software is enough to detect even if a single character of the file has been altered (in the end, this is the scope of digital signatures), which highlights strong evidence that this method can be used to secure the integrity and authenticity of *.IFC and *.IFCzip files delivered by the client to the public authority.

Another important point is that using .IFCzip files as deliverables instead of .IFC, the authority can extract the signed file with a free, open source archiver.

This makes a strong case for the use of .IFCzip, as it not only significantly shrinks the file sizes, having a smaller impact on the cloud/hardware infrastructure, but also enables the public authorities to extract the signed files without any digital certificate or digital signature software installed.

Can use digital signature on *.IFC and *.IFCzip

Any alteration of the files creates an impossibility to use the extracted files afterwards. This method can be used as a secure way to assure the authenticity of delivered *.IFC and *.IFCzip files using digital signatures.

Recommendations for future testing

- Test with other types of digital signatures options such as “Cosemnatura” and “Contrasemnatura” (co-signing and counter-signing when multiple parties are engaged in the process)

- Study the different use cases and life-cycle phases that emerge from Digital Building Permits Platforms, including contractual agreements of private/private and PPP cases.

- Test out the methology to introduce the ”hash” generated by the signature inside the IFC schema, thus making the IFC still usable even after signing;

- Further testing on what happens if you revert the changes to the files. First results show that the .IFCzip file recovers when extracted with 7-Zip, but when opened with the digital signature software, the software detects the certificate has been modified even if reverted to initial state.