Change toolkit for digital building permit

Deliverable number	D4.5
Deliverable name	IFC digital signature module
Work package number	WP4 Software development
Deliverable leader	DiRoots
Dissemination Level	Public

Status	Final
Version Number	V1.0
Due date	M31
Submission date	30-04-2025

Project no. 101058559

Start date of project: 1 October 2022

Duration: 36 months

File name: CHEK_101058559_D4.5-IFC digital signature module_V1.0-Final

Funded by the European Union

This project has received funding from the European Union under the Horizon Europe Research & Innovation Programme 2021-2027 (grant agreement no. 101058559).

Authors and contributors

Author	Organisation	E-mail
Luiggi Alfaro	DIR	luiggi.alfaro@diroots.com

Quality control

Author	Organisation	Role	Date
Piotr Zaborowski	OGC	WP leader	23/04/2025
Francesca Noardo	OGC	Reviewer	30/04/2025
Jantien Stoter	TUD	Coordinator	29/04/2025

Document history

Release	Description	Date	Author
V0.1	First Draft	02/04/2025	Luiggi Alfaro
V0.2	First revie	22/04/2025	Luiggi Alfaro
V0.3	Second review	24/04/2025	Luiggi Alfaro
V1.0	Final version	30/04/2025	Luiggi Alfaro

Contents

1. Executive Summary

The IFC Digital Signature Module is an important component in securing digital workflows for building permit submissions. It ensures the authenticity and integrity of Building Information Modeling (BIM) data by allowing stakeholders to cryptographically verify that an IFC file has been authored and approved by a verified user. This capability is crucial in municipal permitting processes where the integrity of digital submissions must be legally and technically guaranteed. By mitigating risks such as document tampering, impersonation, or unauthorized alterations, the module contributes to a safer, more trustworthy digital ecosystem for construction projects.

To meet these needs, the DSign application was developed. DSign empowers users to securely review and sign IFC files within a browser-based viewer. Before signing, users can visually validate model geometry and metadata to confirm the file's correctness. The workflow, from user registration in the DiStellar platform to file loading, signing, and export, ensures a smooth and secure experience, with the steps aligned with eIDAS standards for Qualified Electronic Signatures (QES).

Importantly, the signing process is conducted entirely in the local browser environment, ensuring that no IFC data is uploaded to external servers. This approach protects sensitive architectural data while giving users full control over when and how files are shared.

DSign is poised to become a foundational tool in the ongoing digital transformation of construction permitting. It streamlines validation workflows while guaranteeing legal compliance. By embedding trust at the source of data creation, DSign lays the groundwork for a more transparent, efficient, and secure permitting process that meets the evolving demands of modern digital governance.

2. Introduction

2.1 Signature Process and Regulation

The IFC Digital Signature Module, implemented as the DSign web application within the DiStellar platform, was developed in alignment with the [1]This compliance is crucial for ensuring that signatures are legally binding, cryptographically secure, and traceable to a verified individual. This compliance is crucial for ensuring that signatures are legally binding, cryptographically secure, and traceable to a verified individual.individual.This compliance is crucial for ensuring that signatures are legally binding, cryptographically secure, and traceable to a verified individual.

To fulfil these requirements, the module incorporates:

- Timestamped digital signatures
- Qualified certificates issued by Trusted Service Providers (TSPs). TSPs are entities officially recognized to issue certificates and digital identity services.
- A confirmation step that requires user consent before signing, ensuring non-repudiation and meeting regulatory standards.

When a user initiates a signature, a confirmation dialog is triggered in the DSign web application, and the user must validate the operation via the Evrotrust mobile application, which manages identity verification and signature authorization.

2.2 Encryption and Signature Process (General Overview)

The digital signature workflow used in the DSign web application follows asymmetric cryptographic principles and leverages Qualified Electronic Signatures (QES). QES are the highest standard of digital signatures under the eIDAS Regulation, offering legal equivalence to handwritten signatures across the EU. QES also ensure that the signer's identity is securely verified using strong, multi-factor user authentication mechanisms.

Here's a simplified overview:

- A cryptographic hash of the IFC file is created.
- The user's private key (secured via the TSP, Evrotrust in DSign's case) signs the hash.
- A digital envelope is generated containing the signed hash, timestamp, and trusted certificate.
- This envelope is embedded within the IFC file in a non-disruptive manner.
- Using the public key embedded in the certificate, any party can later verify that:

[1] eIDAS information: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

- The file has not been altered post-signature.
- The signature originated from an officially verified identity.

These mechanisms ensure:

- Data integrity of the IFC model.
- Authentication of the signer's identity.
- Legal compliance for submission to authorities involved in issuing digital building permits.

2.3 Supported IFC versions

DSign uses the DiStellar IFC viewer as its IFC viewer, which runs in the background of the DiSign tool to sign IFC documents. DSign-DiStellar enforces compatibility with a defined set of schema versions to ensure reliable rendering and signature validation, the supported versions are listed in the table below:

Table 1 Supported IFC Versions

Version	IFC Name
4.3.2.0	IFC 4.3 ADD2
4.0.2.1	IFC4 ADD2 TC1
4.0.2.0	IFC4 ADD2
4.0.1.0	IFC4 ADD1
4.0.0.0	IFC4
2.3.0.1	IFC2x3 TC1
2.3.0.0	IFC2x3

3. IFC Digital Signature

3.1 IFC File Support for Signatures

The IFC (Industry Foundation Classes) format, being based on the STEP (ISO 10303) structure, does not natively support digital signatures. To embed signature data without compromising compatibility, DSign introduces a signature envelope within the file using a comment-based section. This method allows all viewers and BIM tools to safely read and ignore the added data, ensuring the signature metadata does not disrupt parsing or visualization.

The envelope includes the metadata about the signature, timestamp, user identity, and certificate chain, appended as standardized IFC comments.

Figure 1: Step IFC file section showing enveloped metadata for the signature

3.2 Cost Implications of eIDAS-Compliant Signatures

Because the process depends on certificates issued by official Trusted Service Providers (TSPs), there are costs associated with generating and validating these signatures. Each signature operation includes:

- Identity verification (Evrotrust as the TSP)
- Time-stamp issuance
- Certificate validation and logging

To make the system accessible, DiStellar-DSign provides 2 free signatures per user. Beyond that, users must purchase additional credits to continue signing files.

3.3 Workflow: Signature & Validation Process

A) Signature Process

1. **Register in DiStellar**: The user must create a DiStellar account that will be used for the DSign tool.
2. **Load IFC File**: The user uploads any valid IFC file into the platform.
3. **Review Data**: The embedded viewer allows users to inspect geometry and metadata to ensure the file is correct.
4. **Download Evrotrust**: The user installs the Evrotrust mobile app and completes identity verification.
5. **Trigger Signature**: On DSign, when the user initiates the signature, a confirmation dialog appears.
6. **Mobile Confirmation**: The user receives a prompt on their phone via Evrotrust to authorize the signature.

7. **File Signing**: Upon confirmation, the IFC file is signed and the envelope with signature metadata is embedded.
8. **Download Signed File**: The final output is a digitally signed IFC file, compliant with eIDAS, ready for permit submission.

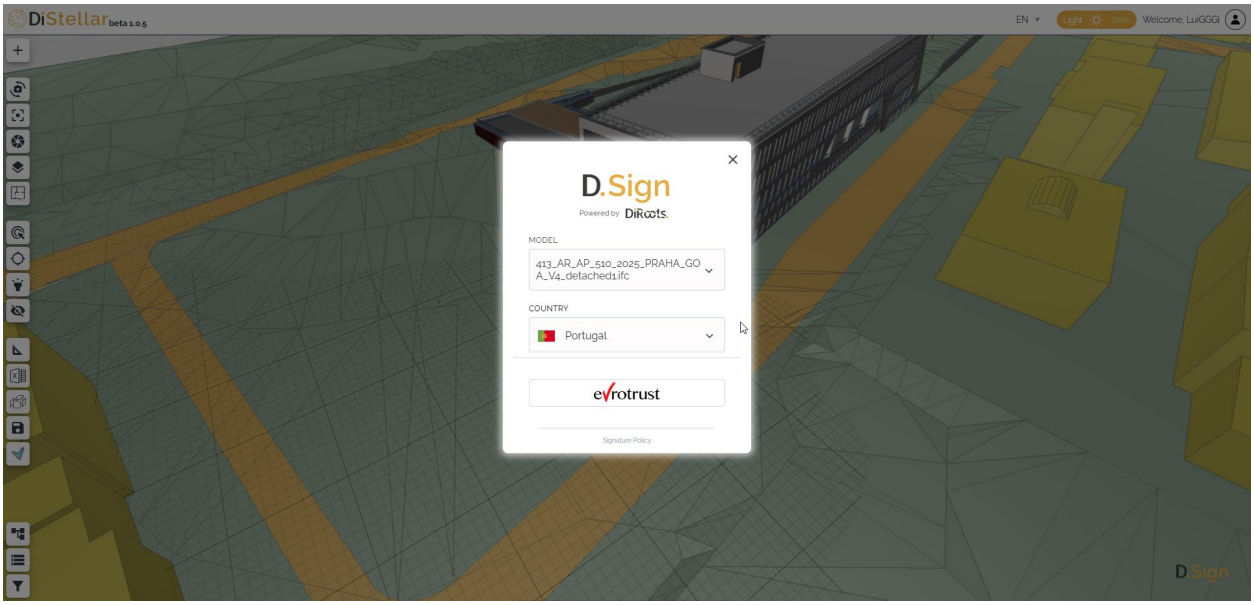

Figure 2. DSign application shown on top of DiStellar IFC viewer

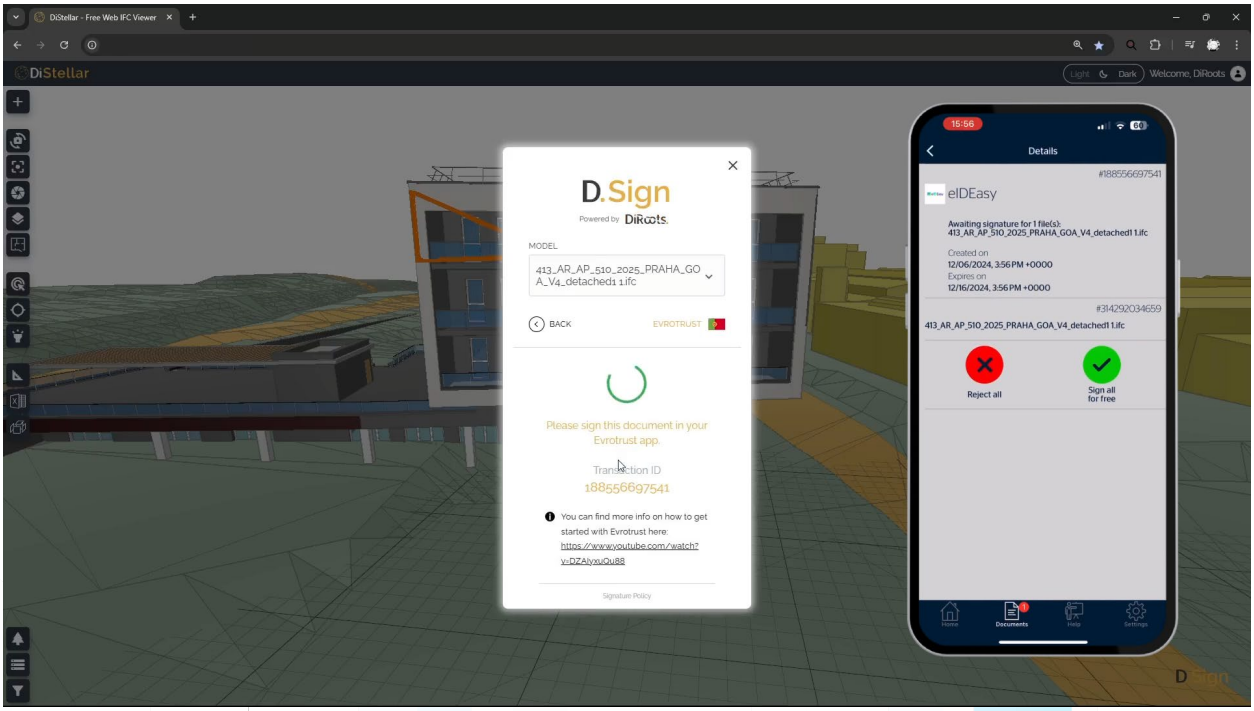

Figure 3. DSign workflow step before confirming signature

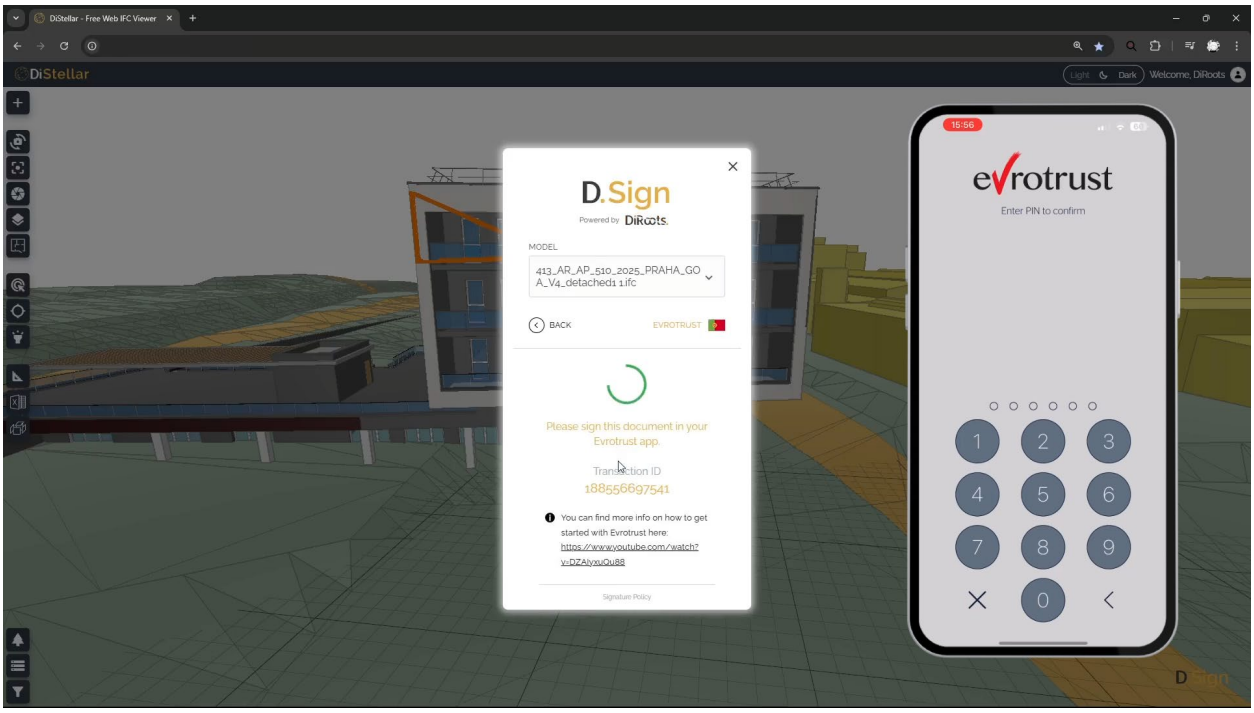

Figure 4. DSign workflow step before confirming signature

Figure 5. DSign workflow step after confirming signature

B) Validation Process

1. **Upload Signed IFC**: The user loads the signed file into DiStellar web app.
2. **Validation Check**: The app checks the embedded envelope, validates the signature, certificate, and timestamp.
3. **Visual Indicator**: A green check is displayed for valid files; otherwise, the system warns of invalid or unverified signatures as shown in the 2 cases below.

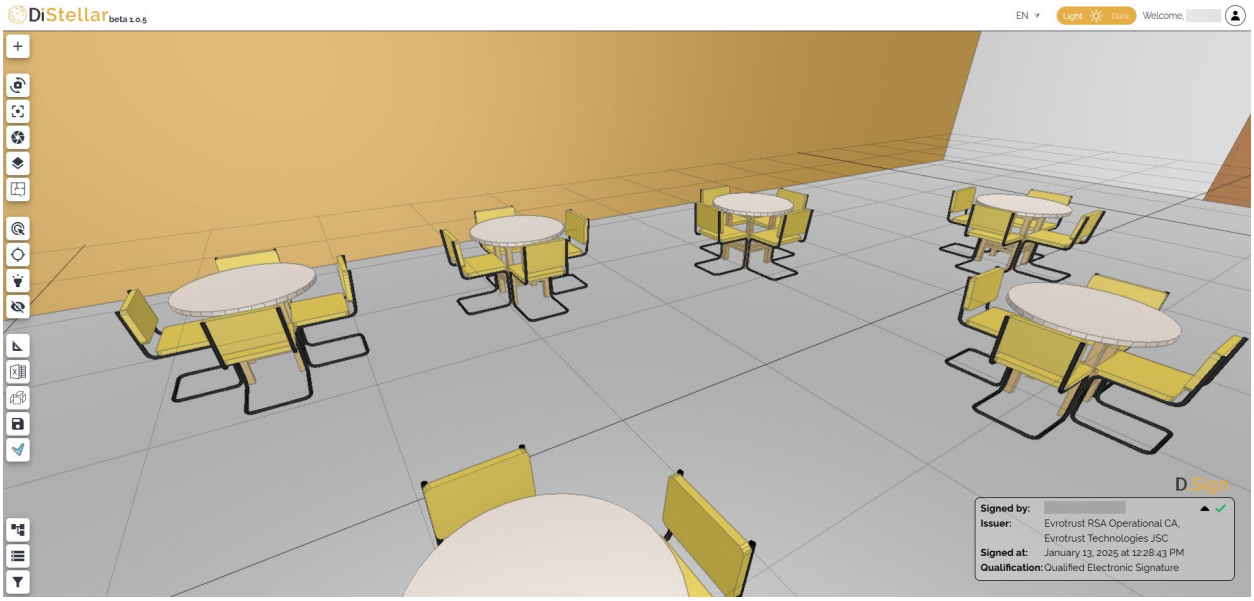

Figure 6. Signed IFC file showing a valid signature

Figure 7. Signed IFC file showing an invalid signature

3.4 Security and Data Privacy

To ensure maximum protection of user data and model confidentiality, DSign operates fully within the user's local browser environment. This means that IFC files are never uploaded to any external server or cloud storage during the signing or validation process. Instead, all actions, including file inspection, signature embedding, and signature verification, are performed directly in the browser, leveraging client-side processing.

By avoiding file transmission to external locations, DSign significantly reduces exposure to potential data breaches or unauthorized access. Any action involving file sharing or submission must be explicitly carried out by the user, such as when sending the signed file to a third party.

4. Conclusion

The DSign application represents a fundamental step in aligning the digital building permitting process with the stringent security and legal requirements set forth by the eIDAS regulation using IFC files. By enabling users to digitally sign and validate IFC files within a secure and user-friendly web environment, DSign ensures that building models submitted for permits are authentic, tamper-proof, and legally binding. Furthermore, it is, actually, the key to legally unblock the whole process of digitalisation of building permit, since legal responsibility for the submitted data needs to be ensured, and such a tool becomes essential.

The integration of qualified digital signatures, timestamping, and certificate validation guarantees that only verified individuals can authorize these critical documents. Furthermore, the design of the signature envelope, seamlessly embedded into the IFC file without disrupting its structure, maintains full compatibility across existing BIM tools and viewers.

With its modular architecture, DSign is also a scalable web-based component that can be integrated into trusted BIM platforms, subject to compliance validation. This positions DSign as regulation-compliant solution that addresses current and emerging needs in digital governance, transparency, and accountability in the AEC industry.

By securing IFC files at their source and embedding trust into every submission, DSign helps lay the foundation for a more secure, efficient, and legally reliable digital permitting ecosystem.

5. References

5.1 List of Figures

5.2 List of Tables

5.3 List of used abbreviations

IFC	-	Industry Foundation Classes
BIM	-	Building Information Modeling
eIDAS	-	Electronic Identification, Authentication and Trust Services (EU Regulation)
QES	-	Qualified Electronic Signature
TSP	-	Trusted Service Provider
ISO	-	International Organization for Standardization
AEC	-	Architecture, Engineering, and Construction
WP	-	Work Package