2025 European Conference on Computing in Construction

CIB W78 Conference on IT in Construction

Porto, Portugal
July 14-17, 2025

EXPLORING THE POSSIBILITY OF INTEGRATING DIGITAL SIGNATURES INTO IFC-BASED BUILT ASSET INFORMATION MODELS TO ACHIEVE AUTHENTICATION AND DATA INTEGRITY VERIFICATION AT THE OBJECT-LEVEL

Mehdi Fakour[1], Štefan Jaud[2], and Erik A. Poirier[1]
[1]Department of Construction Engineering, École de technologie supérieure, Montréal, QC, Canada
[2]Jaud IT GmbH, Moorenweis, Germany

Abstract

Authentication of construction information in the built asset industry is often achieved through validation and digital signature of 2D drawings. Recently, data-enriched models have been used for this process via memorandums as wrappers listing multiple files. These methods pose challenges for authentication and data integrity, even at the file level. This paper explores integrating digital signatures into Industry Foundation Classes (IFC)-based data exchanges by identifying a structure within the existing IFC data schema as a digital signature container and applying it to assign signatures to each object. Consequently, unauthorized changes become detectable, fostering trust, traceability, and transparency.

Introduction

Building Information Model (BIM) is transforming the built asset industry, moving beyond traditional 2D CAD workflows to incorporate data-enriched 3D models (Kaewunruen et al., 2024). Acting as a common standardized language, BIM models streamline collaboration among all project stakeholders, thereby enhancing decision-making, minimizing errors, and improving overall quality (Adepoju, 2022). Nevertheless, BIM adoption can face several notable challenges as noted by Fakour and Poirier (2024): lack of trust and transparency (Saini et al., 2019), traceability (Celoza et al., 2023), interoperability (Mohammadi et al., 2024), security and integrity of the shared information (Bodea, 2018), professional liability (Arshad et al., 2019), and ownership and intellectual property (IP) rights (Hijazi et al., 2021).

This research aims to address these challenges by investigating the feasibility of integrating digital signatures as a technical mechanism for authentication and data integrity verification in IFC-based exchanges at the object level forming part of a future software toolkit (whose high-level abstract architecture is illustrated in Figure 1). This approach can be integrated by BIM practitioners into existing processes, respecting regional regulations and legal frameworks without prescribing who should sign, when in the workflow signing should occur, or which objects must be signed, offering a path toward enhanced trust, data integrity, and security in collaborative built asset projects. Compared to current solutions (Fakour and Poirier, 2024) that primarily operate at the file level—requiring the entire model file to be signed—object-level signing provides greater granularity and flexibility. It allows individual objects to be independently authenticated, thereby ensuring more granular traceability. The IFC standard, chosen for its open format, fosters system-to-system interoperability. While this research focuses on establishing a theoretical approach to integrate digital signatures in BIMs at the object-level, one evident concern is file size expansion if each object is individually signed. Practical performance and scalability considerations remain outside the immediate scope. Also, the scope of the research does not delve into technical details of digital signatures like cryptographic or hashing algorithms.

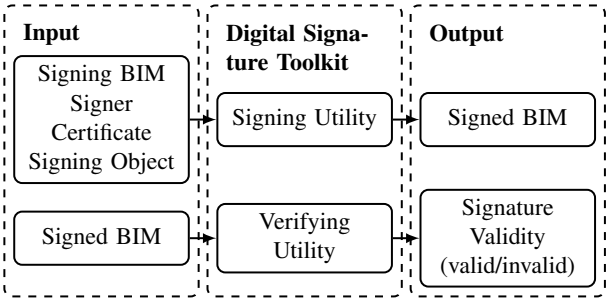

Figure 1: The high-level architecture of future BIM digital signature toolkit.

Background

Authentication in Data Exchange

Authentication refers to the mechanism by which a user, device, or entity confirms its identity within a communication system (Dubey and Thingom, 2017). It ensures that the parties involved in data exchange are who they claim to be, thereby establishing trust (Dubey and Thingom, 2017). There are various techniques for authentication including cryptographic methods like digital signatures (Chandurkar et al., 2023) or biometric methods like fingerprint and facial recognition (Bhatt and Bhushan, 2020).

Data Integrity

Data integrity can be defined as "*the property whereby data remains unaltered from creation to consumption, ensuring it is not modified in any unauthorized man-*

ner during storage or transmission" (IEEE802.1AE-2018, 2018). Ensuring data integrity is a fundamental aspect of managing digital information, especially in collaborative and data-intensive environments dealing with sensitive data. Data integrity verification techniques seek to detect unauthorized modifications, confirm data authenticity, and safeguard data reliability. Although these techniques do not prevent unauthorized alterations, they are essential for identifying and documenting any changes. The common approaches include digital signatures and blockchain technology. Digital signatures are chosen in this research because, compared to alternatives like blockchain, they are simpler to implement and maintain, have broad legal recognition, and can more readily support long-term validation in built asset projects. In contrast, blockchain technology, while decentralized and transparent, involves higher complexity, requires multiple nodes to stay active over an extended period, and entails considerable operational costs (Fakour and Poirier, 2024, 2025).

Digital Signature

Digital signatures emerged alongside advancements in cryptography, fulfilling the growing need for secure digital communications and electronic document handling (Lin, 2023). They feature authentication, data integrity, and non-repudiation—guaranteeing that only authorized signers produce signatures, preventing undetected content modification, and disallowing signers from denying their signatures (Lin, 2023). A crucial element in this ecosystem is the digital certificate, an electronic record issued by a trusted Certificate Authority (CA) that binds a public key to a signer's identity (Zhu and Lin, 2016). The signer holds a corresponding private key for creating digital signatures, while the public key—embedded in the certificate—enables others to confirm the signer's authenticity (Tanwar and Kumar, 2019). The signing process typically involves hashing the content and encrypting the resulting hash with the signer's private key, followed by a verification phase where the recipient uses the signer's public key to decrypt the original hash and compares it against a freshly computed hash (Lin, 2023). Matching hashes confirm that the content remains unaltered and that it originated from an authenticated signer.

IFC

IFC is an open, vendor-neutral standard data model used to represent data about the built environment (buildingSMART International, 2023; ISO16739-1:2024, 2024) and is adopted to ensure interoperability among various BIM tools. The IFC data schema employs a layered architecture to support modularity and extensibility (Venugopal et al., 2012). The IFC schema follows a four-layer architecture: the Resource layer holds foundational definitions like geometry and measures; the Core layer governs core structural entities. The Interoperability layer supports cross-domain interactions; and the Domain layer provides specialized classes for architecture, engineering, and building services (buildingSMART International, 2023; ISO16739-1:2024, 2024).

Information Delivery Specification (IDS)

IDS offers a structured and machine-readable method for defining and validating information requirements for IFC-based models (bSI, 2024). An IDS is embodied as a file with the extension ".ids". This file serves as a container for a series of information Specifications. Each Specification within an IDS file articulates distinct information requirements for a carefully selected subset of an IFC model, which it should adhere to. The .ids file itself is structured based on the IDS XML Schema Definition, ensuring a standardized format for these specifications.

IDS allows for the granular specification of requirements targeting different aspects, or Facets, of an IFC model. These facets are: (1) Entity Facet: This facet allows for setting requirements on specific IFC entities. (2) Attribute Facet: Requirements can be defined for attributes of IFC entities. (3) Classification Facet: This facet enables the specification of which classification systems and specific classification codes should be applied to IFC objects. (4) Property Facet: This is a facet for defining requirements related to Property Sets (Psets) and individual properties associated with IFC entities. (5) Material Facet: Requirements concerning the materials assigned to IFC objects can be defined using this facet. (6) PartOf Facet: This facet allows for specifying requirements for the hierarchical structure and containment relationships within the model.

Model View Definition (MVD)

MVD is a specialized subset of the IFC schema that specifies the exact entities, attributes, relationships, and properties needed for particular information exchanges (Luttun and Krijnen, 2021). When creating an IFC model in native or proprietary software and exporting it to IFC, the exported file aligns with the chosen MVD. This alignment ensures that the data conforms to the MVD's specific requirements, thus promoting consistent and accurate information exchange (Luttun and Krijnen, 2021; Lee et al., 2016a). mvdXML (Chipman et al., 2016) is a data model and format for defining MVDs, ensuring that BIM data exchanges remain structured and consistent for specific use cases (Lee et al., 2020, 2016b). mvdXML's ConceptTemplate is a modular element that describes relevant entities, attributes, relationships, and properties, thereby minimizing redundancy and promoting uniform data requirements. These templates are reusable, allowing for efficient development of new MVDs and improving accuracy in data exchanges (Lee et al., 2020; Afsari and Eastman, 2016). mvdXML provides the structured format for defining an MVD, while ConceptTemplates serve as the modular building blocks within that format.

Research Methodology

The research methodology as shown in Figure 2 began with a series of workshops involving industry practition-

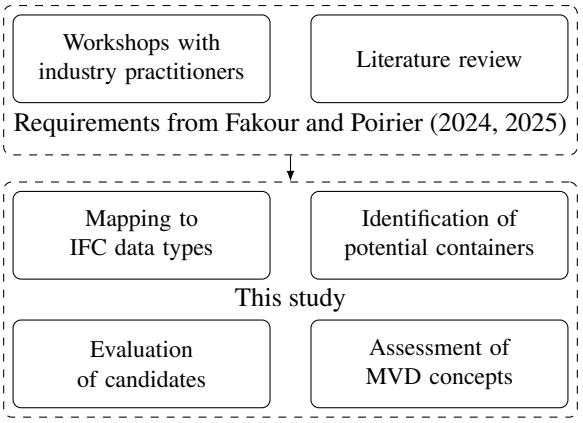

Figure 2: The methodology followed in this study building on top of results from Fakour and Poirier (2024, 2025).

ers, providing insights into the current gap - identified in Fakour and Poirier (2025) - that no solution currently exists for authentication and data integrity verification at the object level in BIMs. These sessions clarified both the requirements for BIM data authentication and the practical constraints. In addition, the study benefited from the expertise of an industry partner specializing in digital identity and cybersecurity, further refining the scope of research and feasibility considerations. A subsequent literature review examined data integrity practices, authentication mechanisms, and IFC schema details, allowing the identification of common metadata requirements essential for robust authentication and data integrity verification. The next phase involved mapping these metadata elements to the resource layer of the IFC schema—specifically chosen because it hosts foundational entities (e.g., IfcPerson, IfcDateTime) used throughout the entire model. However, since resource layer entities cannot be instantiated directly, a suitable container was needed to encapsulate this information, one capable of encompassing the widest range of non-abstract objects in the IFC data schema. Potential containers were evaluated based on multiple criteria, including their capacity to store computed digital signatures, support for multiple signatures on a single object (reflecting shared responsibility among multiple engineers), semantic alignment with authentication needs, and practical implementation considerations. As IFC-based models are exchanged adhering to an MVD, the final step addressed how to embed the chosen container within an MVD-based workflow. This goal was achieved by pinpointing a relevant MVD concept template, ensuring that the container could be integrated smoothly during IFC file export or import processes.

Exchanging Digital Signatures with IFC

Integrating digital signatures into the IFC data schema involves embedding authentication mechanisms within BIM models in a manner compatible with existing schema definitions and digital signature standards. Various studies have explored ways to extend the IFC schema, either by adding new entities or extending existing ones with additional properties (Yu et al., 2023), or by reusing existing entities for new purpose (Won et al., 2022). Recognizing the complexities and challenges associated with modifying the IFC schema as an international standard, this research focuses on reusing existing properties or entities within the current schema. This approach avoids introducing new entities or properties within IFC data schema, thereby maintaining compatibility with existing BIM software and minimizing implementation difficulties (Fakour and Poirier, 2024).

This section explores the process of incorporating digital signatures into the IFC schema by highlighting the required metadata, mapping this metadata to the IFC data schema, evaluating candidate containers within the schema, and discussing the challenges associated with this integration. In particular, the challenges that lead to complexity in extracting the portion of the model or related data specific to an object. These complexities can impact the ability to accurately identify and reference the exact components of the BIM model that need to be signed.

Required Metadata for Digital Signatures

Integrating digital signatures necessitates the inclusion of specific metadata that encapsulates essential information about the signer, the signature, and the context of the signing event. Based on common standards and regulations, there can be various optional fields (Union, 2019) for the metadata included in a digital certificate and digital signature. However, the required metadata generally includes (Fakour and Poirier, 2024):

- Signer Information or Subject (ITU, 2019): Information about the individual or entity owning the digital certificate and signing the data, such as name, organization, and role (Union, 2019);
- Certificate Issuer (ITU, 2019): Details of the entity issuing the digital certificate used;
- Certificate Validity Period (ITU, 2019);
- Signature Timestamp or Signing Time (ETSI, 2010): The date and time when the signature was applied; and
- Digital Signature Value: Actual calculated hash or similar.

Mapping Metadata to the IFC Data Schema

Mapping the required digital signature metadata to the IFC data schema involves identifying suitable existing entities and attributes within the schema that can effectively represent this information. The IFC data schema provides standardized entities and attributes that can be leveraged for this purpose in the resource layer (buildingSMART International, 2023).

Table 1 illustrates a summary of how each piece of required metadata can be effectively mapped to existing elements within the IFC data schema. While individual metadata elements can be represented in various parts of the IFC schema, the challenge lies in finding a container that can encapsulate all these elements cohesively and support con-

Table 1: Mapping of required digital signature metadata to IFC data schema entities and types (Fakour and Poirier, 2024).

Required Metadata	IFC Mapping
Signer Information	IfcPerson, IfcOrganization, or IfcPersonAndOrganization
Certificate Issuer Information	IfcPerson, IfcOrganization, or IfcPersonAndOrganization
Certificate Validity Period	IfcDateTime
Signature Timestamp	IfcDateTime
Signature Value	IfcBinary or IfcText

nection with other elements in the IFC data exchange.

Candidate Containers for Integrating Digital Signatures within the IFC Data Schema

Considering the necessary metadata and the constraint of not extending the IFC schema with new entities or types, the goal is to find a container that supports all required metadata and the objective is to identify a container that supports all required metadata while encompassing the widest possible range of non-abstract objects within the IFC data schema. The IFC schema is structured in a layered and hierarchical architecture, where entities are organized in a way that allows for inheritance and specialization. At the top of this hierarchy is IfcRoot, which serves as the base class for all identifiable entities within the IFC data exchange: "*All entities that are subtypes of IfcRoot can be used independently, whereas resource schema entities, that are not subtypes of IfcRoot, are not supposed to be independent entities*" (buildingSMART International, 2023).

To identify the most suitable container, these potential candidates within the IFC data schema are considered: IfcApproval, IfcOwnerHistory, and IfcObjectReferenceSelect (Fakour and Poirier, 2024). Each candidate is evaluated based on its ability to store all required metadata and potential to store more optional data, relation with the broadest range of entities within IFC Data Schema, support for multiple signatures, semantic alignment with digital signatures purpose, and practicality of implementation.

IfcApproval

IfcApproval represents information about approvals, authorizations, and verifications within a project (buildingSMART International, 2023). It includes attributes such as Identification, which is a unique identifier for the approval (it could represent the digital signature ID); Name, which is the descriptive name of the approval; Description, which provides additional information about the approval; TimeStamp, indicating the date and time when the approval (signature) was granted; and ApprovalStatus, which reflects the status of the approval (e.g., "Signed", "Verified"). IfcApproval can be mapped to digital signature required metadata as follows:

- Signer and Certificate Issuer information is linked via IfcApprovalActorRelationship to IfcPerson, IfcOrganization, or IfcPersonAndOrganization.
- Certificate Validity period and Signature Timestamp can be stored in the TimeStamp attribute.
- The actual digital signature can be placed in the Description attribute. However, to distinguish it from other textual content, a specific tag with a defined beginning and ending can be employed.

In terms of connection to other entities as illustrated in Figure 3 , IfcApproval can be associated with IfcRelAssociatesApproval, which connects to IfcDefinitionSelect and subsequently to IfcObjectDefinition and IfcPropertyDefinition. However, in the current IFC data schema, relationships defined via IfcRelationship cannot be connected to IfcApproval. This is significant because relationships in IFC-based models are treated as objects—meaning each one may require a signature in its own right. IfcApproval is capable of direct storage of the digital signature and all required metadata, support for multiple signatures on the same object via multiple IfcApproval instances which can be linked through IfcApprovalRelationship, semantic alignment with approvals and verifications, and practical implementation using existing schema entities.

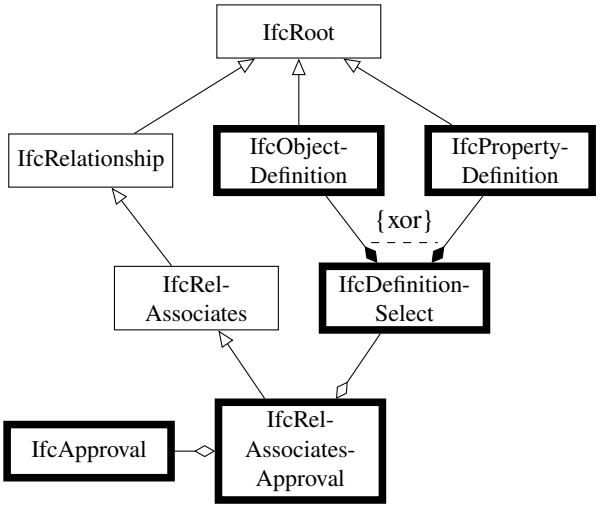

Figure 3: Relationship diagram for IfcApproval to IfcRoot in IFC data schema.

IfcOwnerHistory

IfcOwnerHistory captures ownership and change history of IFC objects (buildingSMART International, 2023). It includes attributes such as OwningUser, representing the user responsible for the object; OwningApplication, representing the application used; ChangeAction, which specifies the type of action performed (e.g., "Modified"); LastModifiedDate, indicating the date of the last modification; and CreationDate, which shows the date the object was

created.

IfcOwnerHistory can be mapped to digital signature required metadata as follows:

- Signer Information is partially represented by OwningUser.
- Certificate Validity Period and Signature Timestamp are represented by LastModifiedDate or CreationDate.

In terms of its connection to other entities in the IFC data schema, the optional attribute OwnerHistory of the entity IfcRoot employs IfcOwnerHistory type as shown on Figure 4. Consequently, it is directly referenced by IfcRoot and thus available to all derived entities. However, IfcOwnerHistory has several limitations: it lacks fields for detailed digital signature metadata (e.g., certificate information, signature value), it only allows one instance per IfcRoot (cardinality constraint), and it is primarily intended for ownership tracking rather than approvals or signatures.

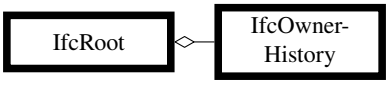

Figure 4: Relationship diagram for IfcOwnerHistory to IfcRoot in IFC data schema.

IfcObjectReferenceSelect

IfcObjectReferenceSelect is a select type that allows referencing various entities, such as IfcAddress, IfcAppliedValue, IfcExternalReference, IfcMaterialDefinition, IfcOrganization, IfcPerson, IfcPersonAndOrganization, IfcTable, and IfcTimeSeries. IfcObjectReferenceSelect can be mapped to digital signature required metadata as follows:

- Signer and Certificate Issuer information can be referenced via IfcPerson, IfcOrganization, or IfcPersonAndOrganization.
- Signature Timestamp or signing time can be stored in IfcTimeSeries.
- The Signature Value could potentially be stored using IfcTable which supports scenarios involving multiple signatures.

In terms of its connection to other entities in the IFC data schema, IfcObjectReferenceSelect is associated through IfcPropertySet and IfcRelDefinesByProperties to IfcObjectDefinition as illustrated in Figure 5. However, IfcObjectReferenceSelect is not connected to IfcRelationship and IfcPropertyDefinition, therefore if it is used as container for digital signature, relationships and property definitions cannot be signed. Moreover, the limitations of IfcObjectReferenceSelect include indirect storage of digital signature data requiring referencing other entities, complexity in managing and retrieving signature data, and less semantic alignment with digital signatures.

Comparative Analysis of Candidate Containers

To determine the most suitable container for integrating digital signatures into the IFC data schema, a comprehensive comparison of the candidates

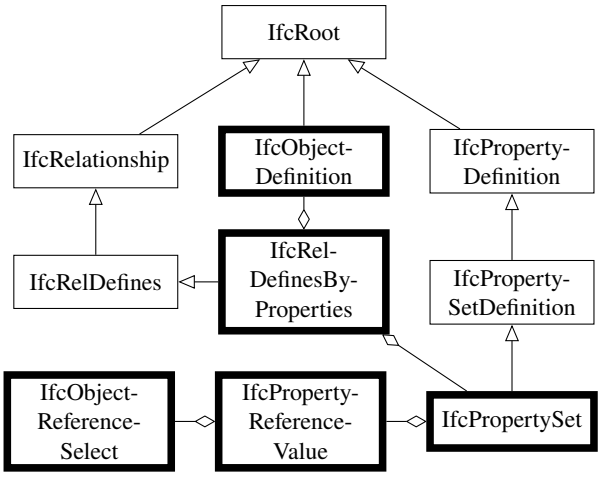

Figure 5: Relationship diagram for IfcObjectReferenceSelect to IfcRoot in IFC data schema.

is essential. The evaluation is conducted against parameters derived from Fakour and Poirier (2024, 2025) research and the core requirements of a robust digital signing solution.This evaluation considers their ability to store all required metadata and other optional metadata, support multiple signatures, relation with the broad range of entities, and semantic alignment with digital signatures. A summary of this comparison is presented in Table 2, highlighting the strengths and limitations of each container for digital signatures.

IfcApproval emerges as the optimal choice due to its capacity to store all required metadata directly within the IFC model, support multiple signatures on the same object, and connect to wider range of entities in IFC Data Schema, ensuring broad applicability across the IFC data exchanges. Its semantic alignment with approvals and verifications makes it an appropriate container for representing digital signatures.

IfcOwnerHistory, although directly connected to IfcRoot and universally present in all independent IFC entities, lacks fields for detailed digital signature metadata and supports only one instance per IFC object. Its primary purpose is tracking ownership and changes rather than approvals or signatures, making it less suitable for embedding digital signatures that require comprehensive metadata and support for multiple signatures.

IfcObjectReferenceSelect offers flexibility by allowing references to various entities and can be attached to a wide range of entities through property sets. However, it cannot be related to IfcRelationship and IfcPropertyDefinition, and it requires indirect storage and adds complexity in managing and retrieving signature data. It lacks direct semantic alignment with digital signatures and does not straightforwardly support multiple signatures on the same object without additional constructs, which can complicate implementation and reduce practicality.

Table 2: Comparison of candidate containers for integrating digital signatures into IFC data schema.

Criterion	IfcApproval	IfcOwnerHistory	IfcObjectReferenceSelect
Ability to Store Digital Signature	Yes (Tagged text in Description)	Limited (lacks fields for detailed signature data)	Indirectly (requires referencing other entities)
Ability to Contain All Required and Other Optional Metadata	Yes (through attributes and associated properties)	Limited (does not support all metadata)	Complex (requires multiple referenced entities)
Support for Multiple Signatures	Yes (via multiple instances associated with the same object)	No (max one instance per object)	Complex (not straightforward without additional constructs)
Semantic Alignment with Digital Signatures	High (aligned with approvals and verifications)	Low (intended for ownership and change tracking)	Moderate (flexible but lacks direct alignment)
Relation With the Broad Range of Entities	Yes (Except IfcRelationship)	Yes (directly referenced by IfcRoot)	Yes (Except IfcRelationship and IfcPropertyDefinition)

Integration of the Chosen Container into Model Based Data Exchange

To associate the chosen container with specific objects, two main possibilities arise: developing an IDS or an MVD. While IDS provides a lightweight means of defining information requirements, its current facets (e.g., PartOf and Property) primarily address simpler relationships and do not readily support more complex constructs like IfcRelAssociatesApproval or reference-based properties such as IfcPropertyReferenceValue. Consequently, IDS cannot handle deeply nested entities or general associations within the IFC data schema without further extensions. Given these limitations as shown in Table 3, this research instead adopts an MVD-based approach.

Table 3: Comparison of IDS and MVD capabilities to associate digital signatures candidate containers to a specific Object.

Option	MVD Mapping	IDS Mapping
IfcApproval	Yes, supported by the "Approval Association" concept template.	Partially, "PartOf" facet does not cover IfcRelAssociatesApproval.
IfcOwnerHistory	Yes, supported by the "Revision Control" concept template.	No, "Entity" and "Attribute" facets do not support detailed specification for IfcOwnerHistory's attributes.
IfcObjectReferenceSelect	No, "Property Sets for Object" does not cover IfcPropertyReferenceValue.	No, "Property" facet does not cover IfcPropertyReferenceValue.

In order to exchange IFC-based models through MVDs, it is crucial to determine how the identified container can be associated with individual objects in these MVD-based workflows. To accomplish this, the relevant concept template must be identified to define the proper mvdXML.

In particular, the Approval Association concept template (buildingSMART, 2020)—which includes IfcApproval—facilitates linking the container to the IfcRoot objects intended for signing. The suggested metadata fields are the most common ones; if additional parameters are required, they can be incorporated into IfcApproval using existing entities already connected to it in the Approval Association concept template.

Conclusions

In this research, a comprehensive analysis of integrating digital signatures into the existing IFC data schema was conducted. By mapping the required digital signature metadata to IFC entities, potential containers within the schema capable of effectively storing this information were identified. Through the evaluation of the candidate containers, it was determined that IfcApproval is the most suitable choice for embedding digital signatures into BIM models.

While IfcApproval stands out as the optimal container, several challenges related to the nature and structure of the IFC data schema were recognized, making the practical utilization of this approach difficult. These challenges stem from the evolving nature of the IFC schema, the methods used for data exchange, the intricate relationships within the schema (van Berlo et al., 2021), potential data redundancies (Du et al., 2020; Sun et al., 2015; Zheng et al., 2024), and the inconsistent implementation of the schema across different software tools. From the perspective of digital signatures, redundancy can create ambiguity regarding which instance of an object was intended to be signed. This ambiguity undermines the reliability of the digital signature and can lead to disputes over responsibility and authenticity. There is a possibility of reducing or even eliminating this ambiguity by defining more precise MVDs—using the Information Delivery Manual (IDM)/MVD methodology—to extract the relevant submodel (Weise et al., 2016; Jaud and Clemen, 2024). However, fully implementing an IDM/MVD methodology can

introduce additional complexity, and many projects only utilize certain aspects of the openBIM ecosystem rather than the entire framework.

Additionally, other challenges such as data security, performance impacts, and user adoption further complicate the integration process. Specifically, the computational time and hardware resources required for signing and verification must be carefully considered, and the increase in file size resulting from added digital signatures could also be significant.

Looking ahead, the proposed solution shall be tested in practical settings, potentially through software extensions or custom plug-ins designed to sign and verify digital signatures within BIM workflows. Another promising direction involves applying the IDM/MVD methodology to define precisely which objects and their constituent parts are being signed. By clarifying the signature process and tailoring it to project-specific needs, object-level digital signatures can strengthen stakeholder trust and elevate data quality throughout a built asset's life cycle.

Acknowledgments

This research is supported by MITACS Grant IT31364 with the collaboration of buildingSMART Canada and Portage CyberTech. We extend our gratitude to all participants for their invaluable support and collaboration.

References

Adepoju, O. (2022). Building Information Modelling. In Re-skilling Human Resources for Construction 4.0: Implications for Industry, Academia and Government, pages 43–64. Springer International Publishing, Cham.

Afsari, K. and Eastman, C. (2016). Consolidated Exchange Models for Implementing Precast Concrete Model View Definition. ISARC Proceedings, 2016 Proceedings of the 33rd ISARC, Auburn, USA:1056–1064.

Arshad, M. F., Thaheem, M. J., Nasir, A. R., and Malik, M. S. A. (2019). Contractual Risks of Building Information Modeling: Toward a Standardized Legal Framework for Design-Bid-Build Projects. Journal of Construction Engineering and Management, 145(4):04019010.

Bhatt, G. and Bhushan, B. (2020). A Comprehensive Survey on various Security Authentication Schemes for Mobile Touch Screen. In 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), pages 248–253.

Bodea, C.-N. (2018). Legal implications of adopting Building Information Modeling (BIM). Juridical Tribune Journal= Tribuna Juridica, 8(1):63–72.

bSI (2024). Information Delivery Specification (IDS) Online Specification.

buildingSMART (2020). Industry Foundation Classes 4.0.2.1 Version 4.0 - Addendum 2 - Technical Corrigendum 1.

buildingSMART International (2023). IFC4.3.2.0 Documentation.

Celoza, A., de Oliveira, D. P., and Leite, F. (2023). Role of BIM Contract Practices in Stakeholder BIM Implementation on AEC Projects. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction, 15(2):04523002.

Chandurkar, S. N., Gotmare, A. R., Ramchaware, Y., Pawar, V., Mirajkar, R., and Sable, N. (2023). Case Study on Cryptography. In 2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), pages 1–8.

Chipman, T., Liebich, T., and Thomas, M. (2016). mvdXML- Specification of a standardized format to define and exchange Model View Definitions with Exchange Requirements and Validation Rules.

Du, X., Gu, Y., Yang, N., and Yang, F. (2020). IFC File Content Compression Based on Reference Relationships. Journal of Computing in Civil Engineering, 34(3):04020012.

Dubey, R. and Thingom, C. (2017). An analysis on direct authentication of data. In 2017 (ICIMIA), pages 415–418.

ETSI (2010). Etsi ts 101 903: "electronic signatures and infrastructures (esi); xml advanced electronic signatures (xades)".

Fakour, M. and Poirier, E. A. (2024). Exploring the digital authentication of built asset information models at the object level. In Proceedings of the 41st International Conference of CIB W78, Marrakech, Morocco.

Fakour, M. and Poirier, E. A. (2025). Exploring the Potential of Digital Signature of Building Information Models to Improve Trust, Transparency, and Traceability in Construction Projects. In Francis, A., Miresco, E., and Melhado, S., editors, Advances in Information Technology in Civil and Building Engineering, pages 178–192, Cham. Springer Nature Switzerland.

Hijazi, A. A., Perera, S., Calheiros, R. N., and Alashwal, A. (2021). Rationale for the Integration of BIM and Blockchain for the Construction Supply Chain Data Delivery: A Systematic Literature Review and Validation through Focus Group. Journal of Construction Engineering and Management, 147(10):03121005.

IEEE802.1AE-2018 (2018). Ieee standard for local and metropolitan area networks-media access control (mac) security. IEEE Std 802.1AE-2018 (Revision of IEEE Std 802.1AE-2006), pages 1–239.

ISO16739-1:2024 (2024). ISO 16739-1:2024.

ITU (2019). X.509: Information technology - open systems interconnection - the directory: Public-key and attribute certificate frameworks.

Jaud, Š. and Clemen, C. (2024). GeoMVD: the Journey to High-Quality Georeferencing Profiles in IFC Datasets. ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences, X-4-W5-2024:203–210.

Kaewunruen, S., Baniotopoulos, C., Guo, Y., Sengsri, P., Teuffel, P., and Bajare, D. (2024). 6D-BIM Applications to Enrich Circular Value Chains and Stakeholder Engagement Within Built Environments. In 4th International Conference "Coordinating Engineering for Sustainability and Resilience" & Midterm Conference of CircularB "Implementation of Circular Economy in the Built Environment", pages 346–356, Cham. Springer Nature Switzerland.

Lee, Y.-C., Eastman, C., Solihin, W., and See, R. (2016a). Modularized rule-based validation of a BIM model pertaining to model views. Automation in Construction, 63:1–11.

Lee, Y.-C., Eastman, C. M., and Solihin, W. (2016b). An ontology-based approach for developing data exchange requirements and model views of building information modeling. Advanced Engineering Informatics, 30(3):354–367.

Lee, Y.-C., Shariatfar, M., Ghannad, P., Zhang, J., and Lee, J.-K. (2020). Generation of Entity-Based Integrated Model View Definition Modules for the Development of New BIM Data Exchange Standards. Journal of Computing in Civil Engineering, 34(3):04020011.

Lin, W. (2023). Digital Signature. In Trends in Data Protection and Encryption Technologies, pages 77–81. Springer Nature Switzerland, Cham.

Luttun, J. and Krijnen, T. (2021). An Approach for Data Extraction, Validation and Correction Using Geometrical Algorithms and Model View Definitions on Building Models. In Proceedings of the 18th International Conference on Computing in Civil and Building Engineering, pages 529–543, Cham. Springer International Publishing.

Mohammadi, S., Aibinu, A. A., and Oraee, M. (2024). Legal and Contractual Risks and Challenges for BIM. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction, 16(1):04523043.

Saini, M., Arif, M., and Kulonda, D. J. (2019). Challenges to transferring and sharing of tacit knowledge within a construction supply chain. Construction Innovation, 19(1):15–33.

Sun, J., Liu, Y.-S., Gao, G., and Han, X.-G. (2015). IFC-Compressor: A content-based compression algorithm for optimizing Industry Foundation Classes files. Automation in Construction, 50:1–15.

Tanwar, S. and Kumar, A. (2019). An efficient and secure identity based multiple signatures scheme based on RSA. Journal of Discrete Mathematical Sciences and Cryptography, 22(6):953–971.

Union, I. T. (2019). X.520: Information technology - open systems interconnection - the directory: Selected attribute types. Technical report, International Telecommunication Union.

van Berlo, L., Krijnen, T., Tauscher, H., Liebich, T., van Kranenburg, A., Paasiala, P., and Paasiala, P. (2021). Future of the Industry Foundation Classes: towards IFC 5. In 38th International Conference of CIB W78, pages 123–137.

Venugopal, M., Eastman, C., Sacks, R., and Teizer, J. (2012). Semantics of model views for information exchanges using the industry foundation class schema. Advanced Engineering Informatics, 26(2):411–428.

Weise, M., Nisbet, N., Liebich, T., and Benghi, C. (2016). IFC model checking based on mvdXML 1.1. In eWork and eBusiness in Architecture, Engineering and Construction: ECPPM 2016, pages 19–26. CRC Press.

Won, J., Kim, T., Yu, J., and Choo, S. (2022). Development of the IFC Schema Extension Methodology for Integrated BIM. In Proceedings of the International Conference on Education and Research in Computer Aided Architectural Design in Europe, volume 2, pages 339–346.

Yu, Y., Kim, S., Jeon, H., and Koo, B. (2023). A Systematic Review of the Trends and Advances in IFC Schema Extensions for BIM Interoperability. Applied Sciences, 13(23):12560.

Zheng, Y., Shi, Y., and Wang, X. (2024). Research on Partial Model Extraction of Railway Infrastructure Based on the Industry Foundation Classes Files. IEEE Access, 12:94690–94701.

Zhu, W.-T. and Lin, J. (2016). Generating Correlated Digital Certificates: Framework and Applications. IEEE Transactions on Information Forensics and Security, 11(6):1117–1127.