Towards BIM-based Authentication at the Object-Level

A Framework for Embedding Digital Signatures into 3D Geometric Models through Industry Foundation Classes

buildingSMART Canada

ÉTS Le génie pour l'industrie

notarius

Project team:

Mehdi Fakour, M.Sc

Erik A. Poirier, PhD

Patrick Drolet, MBA

Claudia Cozzitorto, M.Arch

Bill Moore, P.Eng.

With the collaboration of Stefan Jaud, Jaud IT GmbH

Parts of this report were published in the following publications:

Fakour (2025) Framework for embedding digital signatures into IFC-based BIMs for object-level authentication and data integrity verification, Masters Thesis, École de Technologie Supérieure.

Fakour, M. & Poirier, E. A. (2024). Exploring the digital authentication of built asset information models at the object level. *Proceedings of the 41st International Conference of CIB W78, Marrakech, Morocco, 2-3 October, ISSN: 2706-6568.* (ISSN: 2706-6568), http://itc.scix.net/paper/w78-2024-40

Fakour, M. & Poirier, E. A. (2025). Exploring the Potential of Digital Signature of Building Information Models to Improve Trust, Transparency, and Traceability in Construction Projects. *Advances in Information Technology in Civil and Building Engineering*, pp. 178–192. doi: 10.1007/978-3-031-84208-5_15.

Fakour, M., Jaud, S. & Poirier, E. A. (2025). Framework for Embedding Digital Signatures in IFC-Based Bims for Authentication and Data Integrity Verification at the Objectlevel [SSRN Scholarly Paper]. Rochester, NY: Social Science Research Network. Retrieved on 202507-15 from: https://papers.ssrn.com/abstract=5248778.

EXECUTIVE SUMMARY

Building Information Modeling (BIM) has transformed how projects are planned, executed, and managed within the built asset industry. BIM's emergence as an effective digital ecosystem has helped promote collaboration while increasing productivity and efficiency by providing project stakeholders with comprehensive information management capabilities (Azhar, 2011; Hijazi, Perera, Calheiros & Alashwal, 2021). The adoption of BIM reshapes project coordination and management processes, profoundly enhancing decision-making throughout the life cycle of built assets (Hijazi et al., 2021). While the use of BIM is prompting industry practitioners to reconfigure their practices around emerging digital workflows, verifying and authenticating project information (e.g. signing and sealing drawings and specifications) still follows traditional workflows, where professionals will flatten project information into drawing sheets and specifications, and then sign and seal these artifacts to fulfill their professional obligations. This conversion from information rich 3D geometric information models into 2D representational media contributes to significant information loss throughout a project's lifecycle. To unlock the true potential of BIM-enabled digital workflows, verification and authentication of project information should be maintained within the project's information ecosystem and therefore support digital-workflows with minimal transformations. Recent advancements have attempted to address these limitations, namely the Model as A Legal Document (MALD) initiative within the U.S Departments of Transportation (U.S. DOTs) which relies on memorandums to support model-based digital delivery, face significant limits around traceability at the object-level, especially in multi-disciplinary domains.

At its core, BIM's effectiveness as an information-rich 3D modeling approach relies heavily on interoperability between information systems, enabling seamless data exchange among various software platforms. Industry Foundation Classes (IFC), developed by buildingSMART International (bSI), have emerged as a critical open, vendor-neutral standard supporting interoperability, aiming to overcome persistent issues of software incompatibility and inefficient data conversions (bSI, 2024b). Nevertheless, despite these advancements, notable barriers persist, particularly concerning data integrity and authentication at the detailed, object-specific level. Traditional authentication methods, often limited to file-level verification through formats like PDF, fall short in providing reliable verification for individual BIM objects.

These limitations underscore a need for advanced methods capable of precise, object level authentication and data integrity verification within BIM workflows. Digital signatures present a viable technological solution, offering robust cryptographic mechanisms that guarantee data authenticity, accountability, and non-repudiation which are crucial elements for addressing legal, compliance, and practical challenges (Mulder, Mermoud, Lenders & Tellenbach, 2023b).

This report aims to address existing gaps related to object level authentication within IFC-based BIM data exchanges through the effective utilization of digital signatures. The research systematically evaluates two principal approaches: firstly, integrating digital signatures directly into the existing IFC schema; and secondly, embedding digital signature blocks into IFC files independently of the IFC schema (Fakour & Poirier, 2024).

The integratin of digital signatures directly within the IFC data schema is first investigated, examining specific IFC schema containers capable of supporting digital signature metadata without any alterations. However, this investigation uncovered considerable challenges, including schema complexity, IFC data schema version incompatibility, redundant instances, and implementation intricacies, suggesting that direct schema integration might hinder practical adoption (Fakour & Poirier, 2024).

Consequently, an alternative solution is put forward: embedding digital signature blocks directly into IFC files. Utilizing ISO 10303-21's optional signature section, this approach circumvents schema-related issues while maintaining full compatibility with existing software platforms (ISO10303-21, 2016). The resulting framework supports minimal disruption to established industry workflows, enabling stakeholders to reliably verify object-level authenticity and data integrity without substantial operational adjustments.

Ultimately, the primary aim of this report is to equip decision-makers, BIM managers, and cybersecurity professionals with a clear, practical solution for enhancing object-level trust and data integrity in BIM workflows, aligning with existing regulations, standards, and reinforcing the reliability and security of collaborative BIM processes across the built asset industry.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

BIM	Building Information Modeling
BIMs	Building Information Models
bSI	buildingSMART International
CDEs	Common Data Environments
FBA	Formula-Based Authentication
GUIDs	Globally Unique Identifiers
IDS	Information Delivery Specifications
IFC	Industry Foundation Classes
MFA	Multi-Factor Authentication
MVD	Model View Definitions
OTPs	One-Time Passwords
PBA	Password-Based Authentication
PINs	Personal Identification Numbers
SSO	Single Sign-On

1. INTRODUCTION

1.1. THE NECESSITY OF AUTHENTICATION AND DATA INTEGRITY VERIFICATION IN BIMS

Current limitations in traditional two-dimensional project documentation approaches are increasingly recognized within the construction industry (Olatunji, 2011). Building Information Modeling (BIM) has emerged as a viable solution, significantly enhancing collaboration among multidisciplinary participants throughout the project lifecycle (Volker & Chao-Duivis, 2010). Although BIM has revolutionized project delivery and management through its collaborative capabilities, several critical challenges remain, notably concerning data integrity and authentication at the object-specific level.

Current BIM practices primarily employ file-level authentication methods, which do not provide sufficient granularity for verifying individual BIM objects effectively. The challenges in BIM implementation are multifaceted, ranging from techno-centric process changes (Holzer, 2011, 2007) to legal and contractual complexities (Olatunji, 2011; Abd Jamil & Fathi, 2020; Mohammadi, Aibinu & Oraee, 2024). Addressing these concerns has led researchers to propose solutions aligned with varying project delivery methods and contracting systems, including integrated digital delivery (Maier, 2020; Hwang, Ngo & Her, 2020). However, these solutions skirt the technical issues, overlooking the granular object-level verification, essential for enhancing trust and accountability through digital workflows.

Authenticating and ensuring the integrity of BIM data at the object level addresses several key industry issues:

1. **Trust and Transparency:** Establishing object-level authentication fosters trust among stakeholders by ensuring the accuracy and reliability of information, vital for effective collaboration (Hijazi *et al.*, 2021; Saini, Arif & Kulonda, 2019).
2. **Traceability:** Enhanced traceability is enabled by authenticating BIM objects, allowing stakeholders to effectively track changes throughout the project life cycle, which is crucial for accountability and legal auditing purposes (Bodea, 2018; Deng, Gan, Das, Cheng & Anumba, 2019).
3. **Communication and Collaboration:** Trustworthy and intact BIMs facilitate improved communication among project participants, minimizing miscommunication and reducing errors, thus bolstering collaborative efficiency (Arensman & Ozbek, 2012).

4. **Interoperability:** Maintaining data integrity is vital for resolving interoperability issues, particularly in system-to-system interactions, ensuring consistent data exchange across different software platforms (Turk, 2020; Sattler *et al.*, 2021).
5. **Integrity of Shared Information:** Authentication mechanisms prevent unauthorized changes, preserving the accuracy and reliability of shared BIM data essential for informed decision-making (Alwash, Love & Olatunji, 2017).
6. **Professional Liability:** Object-level authentication supports professional liability by clearly assigning responsibility for each BIM object, thus mitigating legal disputes and enhancing overall accountability (Celoza, de Oliveira & Leite, 2023; Arensman & Ozbek, 2012).
7. **Evidentiary Value:** Ensuring BIM data integrity is crucial for its acceptance as reliable evidence in legal and contractual scenarios, thereby enhancing compliance and dispute resolution capabilities (Olatunji, 2011; Alwash *et al.*, 2017).
8. **Comprehensive Data Integrity:** Unlike traditional 2D drawings, comprehensive authentication of BIM data ensures the integrity of detailed, multidimensional models essential for regulatory compliance (Celoza *et al.*, 2023).
9. **Ownership and Intellectual Property Rights:** Object-level authentication clearly establishes and protects intellectual property and ownership rights, promoting transparency and compliance with legal agreements (Mohammadi *et al.*, 2024; Hijazi *et al.*, 2021).

Ensuring robust authentication and data integrity verification at the object level within BIM workflows is critical to addressing several industry challenges hindering the transition to fully digital workflows. Enabling digital authentication of BIMs will ultimately reinforce trust, facilitate regulatory compliance, reduce legal risks, and enhance collaborative effectiveness across construction projects.

1.2. CURRENT AUTHENTICATION PRACTICES FOR BIMS AND THEIR LIMITATIONS

In the construction sector and related fields such as aerospace and manufacturing, current authentication methodologies primarily secure digital models by encapsulating them within digitally signed container files. Standards such as ARINC827-1 and ARINC835-1 for aerospace (ARINC827-1, 2020; ARINC835-1, 2014), ISO 21597-1:2020 for construction (ISO21597-1, 2020), and PDF/A-3 (ISO10303-21, 2016) guide the use of containers embedding original files alongside metadata. These practices, while effective in confirming the integrity and origin of entire containers, lack detailed verification capabilities for individual files within the container,

creating vulnerability for undetected alterations to specific file contents and hindering object oriented digital workflows.

Common Data Environments (CDEs), framed through standards such as ISO 19650-1 (ISO19650-1, 2018), serve as centralized platforms facilitating project data management through controlled access, version management, and audit functionalities. Outside access control, authentication of information containers within CDEs remains at the file level, without mechanisms verifying objects individually. Consequently, unauthorized changes within BIMs can remain undetected, posing significant risks when reusing information over the extensive life cycles typical in built asset projects, while complicating long-term archival and retrieval processes.

Blockchain-based solutions, such as BIMCHAIN, have emerged as promising approaches to enhance traceability and data integrity by providing secure, multi-signature, time-stamped exchanges (Bimchain, 2018; Pradeep, Amor & Yiu, 2020). While effective in detecting file modifications, blockchain systems typically operate at the file level and face significant implementation complexities, difficulties in handling the intricacies of object-level tracking, and limitations related to long-term data retrieval and regulatory acceptance (Li & Kassem, 2021).

Efforts to achieve object-level authentication have been explored through embedding digital certificates directly within 3D models, as suggested in studies by (Hedberg, Thomas, Helu, Krima & Barnard Feeney, 2020; Hedberg, Hartman, Rosche & Fischer, 2017a). This approach employs X.509 digital certificates embedded in models to authenticate individual objects, ensuring clear traceability and accountability. However, implementing such embedded digital certificates necessitates substantial modifications to existing data schemas, presenting practical implementation challenges and increased complexity.

In summary, existing authentication solutions, despite their individual merits, collectively highlight critical gaps, particularly in providing detailed, object-specific authentication and ensuring compatibility with long-term archival needs and industry practices. A comparative overview of these authentication practices is presented in Table 1 (Fakour *et al.*, 2025).

Table 1 Summary of current authentication solutions

Solution	Mechanism	Authentication Level	Traceability	Implementation Complexity	Durability
Standard Containers (e.g., PDF/A-3, ICDD)	Package with embedded files and metadata	Package/File Level	Limited	Low	Long-Term
Aerospace Standards (ARINC 827, ARINC 835)	Secure container with digital signatures	Package/File Level	Limited	Low	Long-Term
CDEs	Centralized data repositories with access control	File Level	Moderate	Low	Varies
BIMCHAIN (Blockchain Based)	Blockchain for multi-signature, timestamped exchange	File Level	Moderate	High	Dependent on Network
Semantic Differential Transaction (Blockchain)	Blockchain tracking of object changes	Object Level	High	High	Dependent on Network
Embedded Digital Certificates	X.509 certificates within models	Object Level	High	Moderate to High	Long-Term

1.3. PROBLEM DEFINITION

BIM has transformed the built asset industry by improving collaboration, efficiency, and information flow throughout the project life cycle. Its integration with open standards like the Industry Foundation Classes (IFC – ISO 16739-1:2024) supports interoperability across diverse software platforms, enabling structured data exchange and reducing miscommunication.

However, the digital nature of BIM introduces challenges related to data authenticity and integrity particularly in data exchange workflow. Current authentication methods are effective

at the package level or file level but lack the precision needed to verify individual objects within a model.

This lack of object-level authentication creates risks in BIM data exchange workflows. Unauthorized modifications to specific elements may go undetected, leading to disputes, liability issues, and diminished accountability and trust.

To address this gap, a practical solution is needed to support object-level authentication and traceability within IFC-based BIMs. This research proposes a framework for embedding digital signatures at the object level to ensure data provenance, legal compliance, and professional accountability.

1.4. REQUIREMENTS OF AN IDEAL SOLUTION

The requirements for a robust and ideal solution to authenticate and verify the integrity of BIMs at the object level have been distilled from a comprehensive analysis of literature, current data exchange practices in construction, aviation, and manufacturing industries, established standards in digital information exchange, and interviews with domain experts. A notable reference is the digital delivery framework developed by the Utah Department of Transportation (UDOT) (Maier, 2020) as summarized in Figure 1, which aligns closely with the ALCOA++ principles - Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, Available- suggested by U.S. Food and Drug Administration (FDA) for ensuring data integrity (Sabale *et al.*, 2024). The requirements are detailed below.

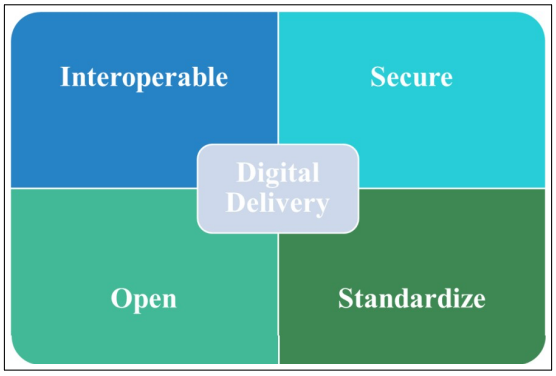

Figure 1. Attributes of digital delivery framework adapted from (Maier, 2020)

Integration with Existing Workflows The solution must integrate seamlessly with current BIM tools and workflows, requiring minimal adjustments to existing processes. This ensures ease of adoption and promotes operational continuity.

Object-Level Authentication and Data Integrity It must allow for object-level digital signatures to support traceability, authorship verification, and detection of unauthorized changes. This addresses the limitations of file-level authentication and enhances accountability.

Support for Hierarchical Signatures and Metadata The toolkit should enable hierarchical signing, allowing professionals to co-sign or endorse existing signatures, and to append metadata that describes the signature context and model transformations (Hedberg *et al.*, 2020).

Discipline and Region Independence The approach should be agnostic to engineering disciplines and regional regulations, making it adaptable across diverse project settings and jurisdictions.

Alignment with ALCOA++ Principles Maier's framework, emphasizing interoperability, security, openness, and standardization, maps to the ALCOA++ attributes—ensuring data is Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available (Maier, 2020).

Functional Requirements The system must support a hierarchy of users. Designers should be able to sign objects (individually or in batches); project managers should monitor authentication status and audit trails; and regulators must be able to validate signed models for compliance.

Non-Functional Requirements Performance efficiency, scalability, usability, maintainability, and cross-platform compatibility are critical. The system must handle large models, support digital certificate management, and remain responsive during signing and verification.

2. THEORETICAL FOUNDATIONS

2.1. AUTHENTICATION: DEFINITIONS AND METHODS

Authentication refers to the process of validating the identity of an entity, such as a user, device, or process, before granting access to a system or resource (Mulder, Mermoud, Lenders & Tellenbach, 2023a; Patiyoot, 2024). According to the ISO/IEC 27000 standard, authentication provides "assurance that a claimed characteristic of an entity is correct" (ISO/IEC27000, 2018). Various authentication factors are used to support different methods of verifying identity. These are commonly classified into four categories (Stallings & Brown, 2015; Mulder *et al.*, 2023a; Velasquez, Caro & Rodriguez, 2018):

1. **Something the individual knows**: Such as passwords, PINs, or secret answers (Grassi, Garcia & Fenton, 2017; Arutyunov, 2012).
2. **Something the individual possesses**: Includes tokens, smart cards, mobile devices, or one-time passwords (OTP) generators (Velasquez *et al.*, 2018).
3. **Something the individual is**: Based on biometric identifiers like fingerprints, facial features, or iris scans (Jain, Ross & Prabhakar, 2004; van Oorschot, 2020).
4. **Somewhere the individual is**: Determined via GPS, IP address, or login context (Mulder *et al.*, 2023a).

A range of authentication techniques has evolved, typically drawing upon one or more of the above factors:

- **Password-Based Authentication(PBA)**: Relies on user knowledge (Shah, Fazl-e-Hadi & Minhas, 2009). Vulnerabilities include susceptibility to guessing and phishing (Grivei, 2015; Ariffin, Abdulhalem & Husin, 2021).
- **Multi-Factor Authentication (MFA)**: Uses multiple factors such as a password and a mobile OTP (Grassi *et al.*, 2017; Velasquez *et al.*, 2018). Provides increased protection against single-factor breaches.
- **Biometric Authentication**: Based on physiological traits such as facial or fingerprint recognition (Stallings & Brown, 2015; Ju, Seo, Han, Ryou & Kwak, 2013).
- **Token-Based Authentication**: Utilizes hardware or software tokens (Stallings & Brown, 2015). Examples include USB keys, OTP apps, and smart cards (Guennoun, Abbad, Talom, Rahman & El-Khatib, 2009).

- **Certificate-Based Authentication**: Uses digital certificates issued by trusted CAs to validate identity (Arutyunov, 2012; Stallings & Brown, 2015). Common in HTTPS/SSL connections.
- **Single Sign-On (SSO)**: Allows users to authenticate once to access multiple services (Yun, Chao, Haoling, Tao & Hefang, 2022). Enhances convenience but introduces a single point of failure.
- **Adaptive Authentication**: Adjusts requirements based on risk factors such as location and device (Mulder *et al.*, 2023a).
- **Continuous Authentication**: Continuously verifies user identity using behavioral or physiological data (Guennoun *et al.*, 2009; van Oorschot, 2020).
- **Formula-Based Authentication (FBA)**: Users compute a login formula result using personal logic (Shah *et al.*, 2009). This method is resilient to shoulder-surfing attacks.

These techniques collectively strengthen digital systems by offering scalable and flexible mechanisms to confirm identity, balancing usability, security, and resilience against evolving threats.

2.2. DATA INTEGRITY AND VERIFICATION TECHNIQUES

Data integrity is the assurance that data remains accurate, consistent, and reliable throughout its life-cycle -from creation to transmission and storage (IEEE 802.1AE-2018, 2018; Cawthra, Ekstrom, Lusty, Sexton & Sweetnam, 2020). It ensures that information is not tampered with, altered without authorization, or corrupted. In contexts such as Building Information Modeling (BIM), maintaining data integrity is especially critical due to the collaborative nature and long life cycle of built asset projects (Hijazi *et al.*, 2021; Gu, Singh & Wang, 2010).

The characteristics of data integrity can be broadly categorized as:

- **Accuracy:** Data must be correct and free from errors (FDA, 2018; Batini & Scannapieca, 2006).
- **Completeness:** All required elements should be included (FDA, 2018; Batini & Scannapieca, 2006).
- **Consistency:** Data must remain uniform across different systems (Batini & Scannapieca, 2006).
- **Traceability:** Data should have a recorded history, allowing auditing (FDA, 2018).

To uphold these characteristics, the ALCOA++ framework has emerged as a widely recognized set of principles for managing trustworthy digital records (Girard & Watkin, 2021; FDA, 2018).

These principles include:

- **Attributable:** Each data entry is linked to its originator (FDA, 2018).
- **Legible:** Data must be clearly readable (FDA, 2018).
- **Contemporaneous:** Records must be captured in real time (FDA, 2018).
- **Original:** The data should be in its initial or verified form (FDA, 2018).
- **Accurate:** All entries should be truthful and error-free (FDA, 2018).
- **Complete, Consistent, Enduring, and Available:** These additions ("++") ensure that records are thorough, standardized, durable, and retrievable (Girard & Watkin, 2021).

To verify data integrity, several technical solutions exist:

- **Digital Signatures.** These cryptographic techniques validate both the origin and content of a message (Rai *et al.*, 2023; Kishore, Raina, Nayar & Thakur, 2021). By hashing the content and encrypting it with the sender's private key, digital signatures ensure that any modification to the content will be detected during verification with the public key (Seetha, 2017).
- **Blockchain.** A decentralized ledger that ensures tamper-evidence by linking blocks of data using cryptographic hashes. Any modification to a previous block changes its hash, invalidating subsequent links (Kabiri & Sharifzadeh, 2022). While robust, blockchain introduces complexity, requires consensus mechanisms, and poses interoperability and regulatory challenges (Dong, Yaqiong, Huaiguang & Duan, 2022; Guru, Perumal & Varadarajan, 2021).

Digital signatures are more favorable for BIM-based data integrity verification due to their ease of integration, compliance readiness, and support for long-term validation (Rai *et al.*, 2023; Fakour & Poirier, 2024).

2.3. SYNERGY BETWEEN AUTHENTICATION AND DATA INTEGRITY

Authentication and data integrity are deeply interconnected elements of information security, each reinforcing the other to ensure trust in digital systems. Authentication verifies the identity of users, devices, or systems accessing resources, while data integrity ensures that the information remains accurate, consistent, and unaltered during storage or transmission (ISO/IEC2501, 2008; Grassi *et al.*, 2017).

Biometric authentication, for instance, inherently supports the principle of attributability in data integrity by linking actions to verifiable individuals (FDA, 2018). Cryptographic techniques such as digital signatures exemplify this synergy-they authenticate the signer and simultaneously verify that the content remains unchanged (Chen, Moody, Regenscheid & Robinson, 2023;

Stallings & Brown, 2015). Similarly, blockchain integrates authentication through consensus algorithms and ensures integrity using Merkle trees, creating immutable, auditable records that align with ALCOA++ principles such as originality and endurance (Yu, Zhang, Yu & He, 2023a; Perera, Nanayakkara, Rodrigo, Senaratne & Weinand, 2020).

Adaptive and multi-factor authentication methods further enhance this interplay by adding contextual and layered security, thus minimizing risks of unauthorized data manipulation (Velasquez *et al.*, 2018; Mulder *et al.*, 2023a). Conversely, data integrity mechanisms like smart contracts rely on authenticated identities to enforce secure, rule-based transactions (Huang, Bian, Li, Zhao & Shi, 2019).

This mutual reinforcement of identity assurance and data integrity fosters a cohesive and secure digital environment-essential for compliance in highly regulated sectors such as construction, healthcare, and finance (Girard & Watkin, 2021).

3. OVERVIEW OF IFC AS A TARGET SCHEMA AND RELATED CONCEPTS

IFC represents a central standard within the buildingSMART ecosystem. It provides a range of open digital specifications aimed at enabling collaboration across the built environment. Among these, IFC serves as a foundational schema for describing building and infrastructure data in a vendor-neutral, platform-independent format (bSI, 2024a). It is officially recognized as an international standard and plays a critical role in facilitating interoperability across diverse BIM software and systems (ISO16739-1:2024, 2024).

Originally developed in 1995, IFC predates many modern data exchange frameworks like XML or JSON and was instead built upon the EXPRESS schema language and the STEP Physical File (SPF) format (van Berlo *et al.*, 2021). This structure supports rigorous, machine readable definitions of construction-related objects, their attributes, and relationships. Since its inception, IFC has evolved through several versions. IFC 2x3 remains the most widely implemented in industry practice, while the more recent official version, IFC 4x3 add 2 expands the scope to include infrastructure domains such as railways, roads, and waterways, with both dynamic and static schema enhancements (Zheng, Shi & Wang, 2024; Gao, Lu & Fung, 2024).

3.1. IFC DATA SCHEMA ARCHITECTURE

The IFC data schema defines a standardized framework for BIM data exchange and interoperability across diverse software platforms (ISO16739-1:2024, 2024; Kim, Lee, Han, Kim & Choi, 2020). It is specified using the EXPRESS data modeling language and typically serialized in the STEP physical file format (bSI, 2023).

Conceptually, the IFC schema is structured into four hierarchical layers: Resource, Core, Interoperability, and Domain (bSI, 2023; Yu, Kim, Jeon & Koo, 2023b). This layered architecture promotes extensibility, modularization, and cross-domain interoperability while facilitating both semantic richness and practical implementation (Dong, Lam, Huang & Dobbs, 2007; Shi, Liu, Gao, Gu & Li, 2018).

- **Resource Layer:** This foundational layer contains base definitions, such as units, measures, geometry, and time. These elements cannot exist independently within a model, as they lack globally unique identifiers (GUIDs) (bSI, 2023).

- **Core Layer:** Composed of the Kernel schema and core extensions, this layer defines abstract entities and foundational relationships applicable across disciplines. Entities here and above receive GUIDs and can be instantiated independently (Won, Kim, Yu & Choo, 2022).
- **Interoperability Layer:** This layer provides schemas that define cross-disciplinary entities used for exchanging product, process, and resource information between different domains (Yu *et al.*, 2023b).
- **Domain Layer:** The uppermost layer contains discipline-specific schemas tailored to architecture, structural engineering, HVAC, and other specialized fields. These schemas are optimized for intra-domain exchange of semantically rich data (Yu *et al.*, 2023b).

The hierarchical organization enables definitions in higher layers to reuse or reference elements from lower layers, supporting modular growth of the schema and simplifying software implementation (Park, Chen & Cho, 2020; bSI, 2023). The object-oriented modeling approach embedded in the schema defines entities as objects with attributes and interrelationships, enabling detailed and structured representation of building components (Park *et al.*, 2020; Shi *et al.*, 2018).

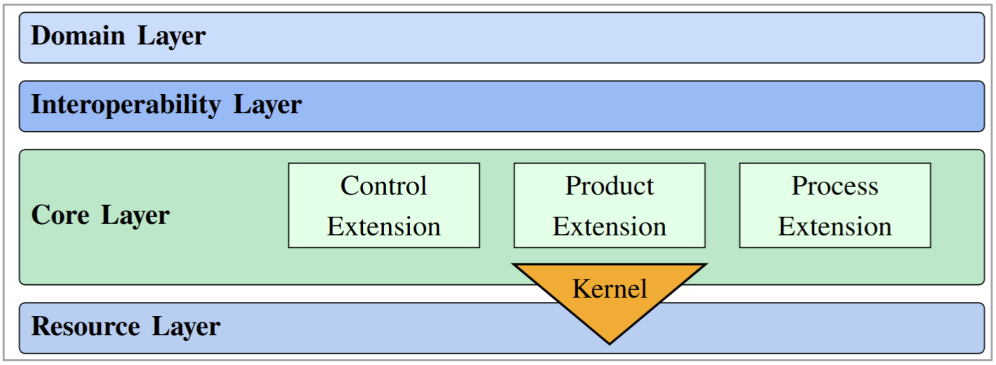

Figure 2. IFC data schema layered architecture Adapted from (bSI, 2023)

3.2. IFC FILE SERIALIZATIONS

IFC data can be stored and exchanged through multiple serialization formats, each addressing specific needs within the BIM community. The primary official formats include IFC-SPF, IFC-XML, and IFC-ZIP (bSI, 2024a). These formats differ in terms of readability, file size, interoperability, and suitability for various applications.

The most used format is **IFC-SPF** (STEP Physical File), based on ISO 10303-21 (Sun, Liu, Gao & Han, 2015; Zheng *et al.*, 2024). Files with the '.ifc' extension are structured as plain text, consisting of a header section containing metadata and a data section encoding entity instances using a line-by-line format (Du, Gu, Yang & Yang, 2020). Each line represents an entity with a

unique ID, entity name, attributes, and references. Although human-readable, large models may result in considerable file sizes with redundant data, affecting parsing efficiency and hindering exchange workflows (Sun *et al.*, 2015).

IFC-XML, standardized by ISO 10303-28, expresses IFC data using XML syntax. Files with the '.ifcXML' extension offer enhanced readability and compatibility with web and cloud-based systems (Afsari, Eastman & Castro-Lacouture, 2017; Baranova, 2021). The format enables easier data parsing through XML tools but produces substantially larger files than IFC-SPF, limiting scalability (Frei, 2019).

IFC-ZIP compresses IFC-SPF or IFC-XML files using ZIP compression. The resulting '.ifcZIP' format reduces file size, making it ideal for data transmission and archiving (Sun *et al.*, 2015; Xu, Kim & Chen, 2022). It adds an extra decompression step but preserves compatibility with underlying formats.

A comparative overview is provided in Table 2. While this research focuses on the IFC-SPF format due to its broad adoption and interoperability, support for other formats remains important for adaptability.

Table 2. Comparative summary of the IFC serializations

Aspect	IFC-SPF	IFC-XML	IFC-ZIP
Usability	Widely supported; plain text; moderate readability	Self-describing XML; enhanced readability	Requires decompression; adds a step
File Size	Moderate to large for complex models	Often an order of magnitude larger than IFC-SPF	Significantly reduced compared to uncompressed formats
Interoperability	High; broad software support	Good within XML-compatible systems; less common	Depends on underlying IFC format
Applications	STEP-based workflows	XML-based workflows	Efficient storage and transfer; archiving
Processing	Requires parsing of text files; efficient	Requires XML parsing; more processing overhead	Requires decompression; adds processing time
Standardization	ISO 10303-21	ISO 10303-28	Uses standard ZIP compression; based on standardized formats

3.3. MODEL VIEW DEFINITIONS (MVDS)

MVDs represent specialized subsets of the IFC schema designed to meet specific information exchange requirements within the built asset industry (bSI, 2024b; Chipman, Liebich & Thomas, 2016; ISO16739-1:2024, 2024). Given the comprehensive and flexible nature of the IFC schema, which encompasses diverse elements such as geometry, properties, and relationships, MVDs serve to constrain this schema by selecting only the entities, attributes, and relationships relevant to a defined exchange scenario (Yu *et al.*, 2023b; Chipman *et al.*, 2016). This enhances both the efficiency and interoperability of data exchanged between stakeholders.

The adoption of MVDs ensures that IFC files exported from proprietary BIM tools adhere to a predefined structure that meets the needs of workflows or use cases (Luttun & Krijnen, 2021; Lee, Eastman, Solihin & See, 2016). For instance, an export using the Coordination View or Reference View MVD guarantees that only the necessary elements are included for coordination purposes. This specificity reduces data redundancy and ambiguity while improving consistency across BIM platforms.

Initially, MVDs were created independently by various parties, resulting in fragmented and non-interoperable implementations. To address these challenges, buildingSMART International introduced the mvdXML standard, a structured XML-based format that formalizes the specification, validation rules, and exchange requirements of MVDs (Chipman *et al.*, 2016; Jaud & Clemen, 2024; Jiang, Jiang, Han, Wu & Wang, 2019). At the core of mvdXML are Concept Templates—modular components that describe consistent configurations of IFC entities and their associated data. These templates are reusable and help reduce duplication, enabling standardized and scalable MVD development across different domains (Lee, Shariatfar, Ghannad, Zhang & Lee, 2020; Afsari & Eastman, 2016).

By implementing MVDs through mvdXML and Concept Templates, software vendors and project teams can ensure structured, reliable, and domain-specific exchanges of BIM data, improving accuracy, efficiency, and compliance in openBIM workflows.

3.4. INFORMATION DELIVERY SPECIFICATIONS (IDS)

Information Delivery Specifications (IDS) provide a standardized, machine-readable approach for defining and validating specific information requirements for IFC-based models (bSI, 2024c). An IDS file, identified by the ".ids" extension, serves as a structured container for a series of individual specifications. Each specification describes precise requirements that a subset of an

IFC model must satisfy. The file structure follows the IDS XML Schema Definition, ensuring consistency and interoperability.

IDS enables the articulation of requirements at a granular level through the concept of *facets*, where each facet corresponds to a particular aspect of an IFC model. These facets include:

- **Entity facet:** Used to define requirements on the inclusion or use of specific IFC entity types within the model.
- **Attribute facet:** Specifies conditions on the attributes of IFC entities, such as mandatory fields or value ranges.
- **Classification facet:** Enables requirements regarding classification systems and codes that must be associated with IFC objects.
- **Property facet:** Allows the definition of expected property sets (Psets) and individual property values to be attached to entities.
- **Material facet:** Captures requirements about the material definitions linked to objects in the model.
- **PartOf facet:** Supports specifying hierarchical relationships, including containment and aggregation structures, that the model must follow.

By leveraging IDS, stakeholders can define and verify structured information requirements in a consistent way, ensuring that IFC models deliver the right data at the right level of detail for their intended use. This approach contributes to reducing ambiguity and improving compliance in openBIM workflows.

4. SOLUTIONS PATHWAYS

Multiple solution pathways were considered to address the problem of digital authentication of BIMs at the object level. As illustrated in Figure 8, these are categorized into two main groups: (1) **IFC Data Schema-Based Solutions**, which aim to integrate digital signatures within the IFC schema itself, and (2) **Schema-Independent Solutions**, which involve embedding digital signatures at the IFC-based model's file, independent of the schema.

Within the IFC schema-based category, two approaches were explored. The first involves proposing a new entity in the IFC schema to accommodate digital signatures. However, this approach was ultimately set aside due to the complexity and time-consuming nature of modifying standardized schemas. The second approach is to reuse existing entities in the IFC data schema by identifying an entity that can (1) contain all the required metadata related to digital signatures, (2) be associated with all other entities in the IFC data schema, and (3) provide a mechanism for associating the digital signature container with other entities. This direction was examined further, and its details are presented in the following sections. However, due to limitations and challenges encountered in this path, an alternative approach was pursued.

The schema-independent path focuses on designing a digital signature block appended to the IFC file, in alignment with ISO 10303 standards. Following the initial implementation, several practical challenges emerged, leading to the need for restructuring the signature block. The structure and implementation consideration of both the initial and restructured signature blocks are discussed in subsequent sections.

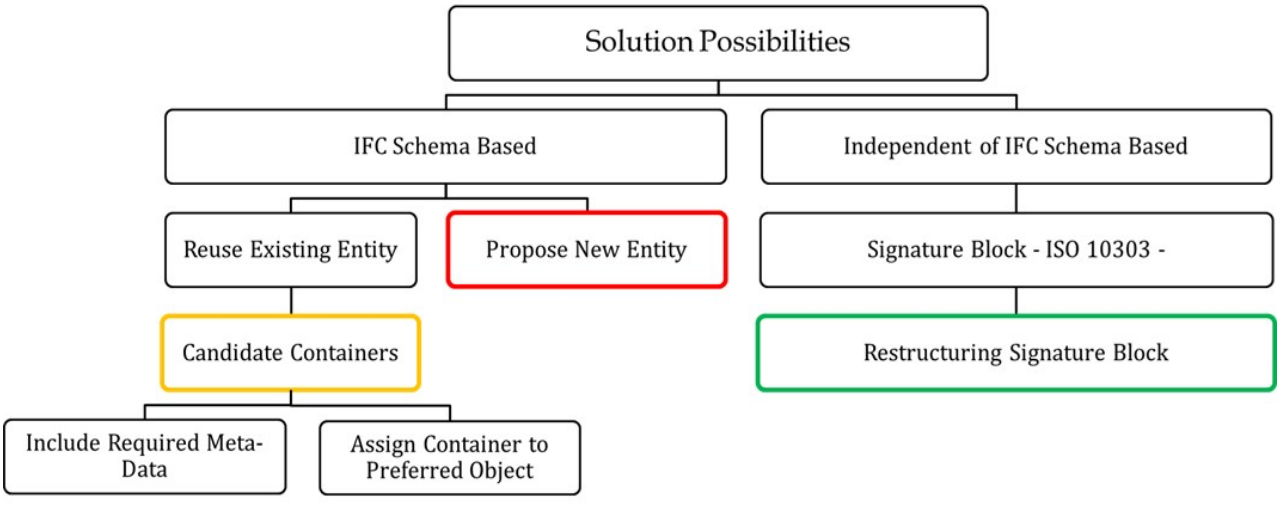

Figure 3. Solution pathways

5. INTEGRATING DIGITAL SIGNATURES WITHIN THE EXISTING IFC DATA SCHEMA

This section examines how digital signatures can be integrated into the IFC schema by identifying the necessary metadata, aligning it with existing schema structures, assessing suitable container entities, exploring how these containers can be associated with target entities, and outlining key integration challenges.

5.1. MAPPING DIGITAL SIGNATURE METADATA TO IFC SCHEMA

To integrate digital signatures into IFC-based BIM models, it is essential to align required metadata with suitable entities in the IFC schema. This metadata typically includes signer identity, certificate issuer, signature validity, timestamp, and the signature value itself (ITU-X509, 2019; ITU-X520, 2019; ETSI, 2010). These elements are standard in most digital signature frameworks and are critical for enabling reliable authentication and long-term validation.

The mapping process involves selecting existing IFC entities and data types that can represent these required meta-data for digital signatures. For signer details and certificate issuer data, the entities IfcPerson, IfcOrganization, or IfcPersonAndOrganization from the IfcActorResource schema can be employed (bSI, 2023). Data-Time related attributes like signature timestamp and certificate validity can be stored using IfcDateTime. The actual digital signature—whether a binary or encoded string—can be held in IfcBinary or IfcText, potentially within a IfcPropertySet for grouping relevant properties (Fakour & Poirier, 2024).

Table 3 provides a concise overview of this mapping. While individual metadata components align with specific schema elements, the key challenge remains identifying a suitable container within IFC data schema that can encapsulate all metadata and be reliably associated with the entities being signed.

Table 3. Mapping of Required Digital Signature Metadata to IFC Schema

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

5.2. CANDIDATE CONTAINERS FOR INTEGRATING DIGITAL SIGNATURES IN IFC SCHEMA

To embed digital signatures without extending the IFC schema, it is essential to identify an existing container that can encapsulate all required metadata while maintaining broad compatibility across IFC entities. Since the IFC schema is structured hierarchically—with IfcRoot serving as the base class for all identifiable entities—candidate containers must support inheritance, wide applicability, and alignment with IFC's core architecture (bSI, 2023).

Three main candidates are evaluated based on their metadata coverage, semantic fit, ability to support multiple signatures, and relation to other schema elements: IfcApproval, IfcOwnerHistory, and IfcObjectReferenceSelect (Fakour & Poirier, 2024).

5.2.1. IfcApproval

This entity captures authorization and verification processes. Attributes like Identification, Name, Description, TimeStamp, and ApprovalStatus can be used to store key metadata. Signer and issuer information can be linked via IfcApprovalActorRelationship, while the digital signature can be embedded as tagged text within Description. It connects to entities through IfcRelAssociatesApproval and supports multiple signatures using IfcApprovalRelationship, though it does not connect to IfcRelationship entities (Figure 4).

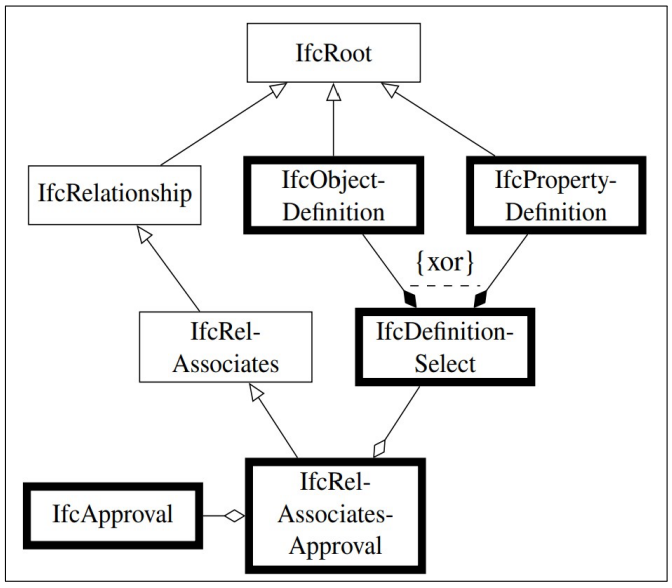

Figure 4. Association path of IfcApproval within the IFC schema

5.2.2. IfcOwnerHistory

Primarily used for tracking authorship and changes, IfcOwnerHistory includes fields such as OwningUser, ChangeAction, CreationDate, and LastModifiedDate. It is directly referenced by all IfcRoot subtypes (Figure 5), offering universal availability. However, it lacks capacity for storing detailed certificate metadata, calculated digital signature, and supports only one instance per object which is the only last one, limiting its utility for digital signing.

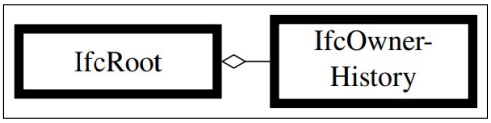

Figure 5. Reference of IfcOwnerHistory from IfcRoot

5.2.3. IfcObjectReferenceSelect

This select type can point to various reference entities, including IfcPerson, IfcOrganization, IfcTimeSeries, and IfcTable, which may collectively store the digital signature and its metadata. It connects to objects via IfcPropertySet and IfcRelDefinesByProperties (Figure 6), but cannot link to IfcRelationship or IfcPropertyDefinition, limiting its coverage. It also requires a multi-entity referencing approach, adding complexity to implementation.

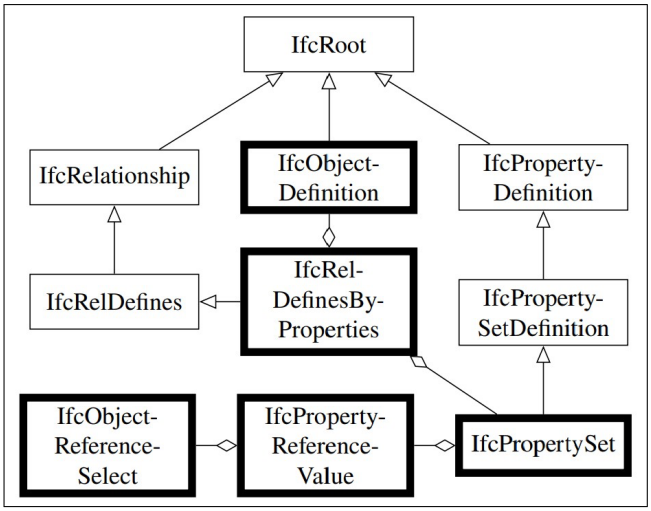

Figure 6. Reference path for IfcObjectReferenceSelect in IFC schema

5.3. COMPARATIVE EVALUATION BETWEEN POTENTIAL CANDIDATES

The comparative analysis in Table 4 assesses each candidate's suitability for storing digital signatures. Based on these criteria, IfcApproval presents the most balanced and practical option for embedding digital signatures into IFC-based BIMs, given its native attributes, semantic relevance, and support for multiple approvals. However, since IfcApproval cannot be associated, it cannot serve as a digital signature container for authenticating that portion of the IFC data schema.

Table 4. Comparison of candidate containers for integrating digital signatures into IFC schema with IfcRelationship and its derived entities

Criterion	IfcApproval	IfcOwnerHistory	IfcObjectReferenceSelect
Digital Signature Storage	Yes	Limited	Indirect
Metadata Support	Full	Partial	Fragmented
Multiple Signatures	Supported	No	Complex
Semantic Alignment	High	Low	Moderate
Relation to IFC Entities	Broad (excl. IfcRelationship)	Universal	Broad (excl. IfcRelationship, IfcPropertyDefinition)

5.4. INTEGRATION INTO MODEL-BASED DATA EXCHANGE

To associate the selected container (IfcApproval) with specific IFC objects during data exchange, two primary strategies exist: defining an IDS or utilizing an MVD. Although IDS offers a lightweight, machine-readable framework for specifying information requirements, its current capabilities are limited to simpler associations. Specifically, IDS facets such as PartOf and Property do not accommodate complex constructs like IfcRelAssociatesApproval or reference-based attributes such as IfcPropertyReferenceValue. As a result, IDS cannot effectively manage deeply nested structures or associations.

Given these constraints, using MVDs provides greater flexibility and precision in associate digital signature containers to IFC objects. Table 5 compares the mapping capabilities of IDS and MVD approaches for different container options.

For MVD-based data exchange, defining an appropriate mvdXM mapping requires referencing a relevant Concept Template. In the case of IfcApproval, the Approval Association Concept Template enables its attachment to IfcRoot-based entities for signature purposes. This template accommodates core metadata, and any additional attributes can be incorporated through schema elements already linked to IfcApproval within the template's structure.

Table 5. Comparison of IDS and MVD capabilities to associate digital signature containers with IFC objects

Container Option	MVD Mapping	IDS Mapping
IfcApproval	Supported via the Approval Association Concept Template	Partially supported; PartOf facet does not cover IfcRelAssociatesApproval
IfcOwnerHistory	Supported via the Revision Control Concept Template	Not supported; Entity and Attribute facets are insufficient
IfcObjectReferenceSelect	Not supported; MVD lacks mapping for IfcPropertyReferenceValue	Not supported; Property facet does not accommodate IfcPropertyReferenceValue

5.5. OTHER CHALLENGES OF USING THE IFC DATA SCHEMA FOR DIGITAL SIGNATURES

Integrating digital signatures into IFC-based BIM models introduces several challenges due to the inherent complexity and structure of the IFC schema. These challenges are discussed below.

Compatibility Across Schema Versions : The evolution of the IFC schema poses risks regarding backward and forward compatibility. Entities introduced in recent versions (e.g., IfcTable in IFC 4.0) may not be available in older schemas, while others may become obsolete in future versions (bSI, 2023). For example, using newer constructs such as IfcObjectReferenceSelect might limit interoperability with legacy systems or future-proofing efforts.

Limitations of Model View Definitions (MVDs) : MVDs are predefined subsets of the IFC schema used to satisfy specific exchange requirements (Afsari, Eastman & Shelden, 2016; Chipman *et al.*, 2016). While useful for standardizing data exchange, two major issues arise when using MVDs for object-level signing: (1) referenced entities may be omitted in exported IFC files, raising legal and accountability concerns; and (2) capturing every potential entity combination in an MVD is infeasible due to the complexity of the schema (Yu *et al.*, 2023b).

Complexity of Relationships : IFC relies heavily on complex relationship structures, including inverse and objectified relationships, to maintain data consistency and flexibility. However, these constructs create challenges in data navigation and object-level processing (van Berlo *et al.*, 2021). While graph-based methods offer one solution (Ismail, Nahar & Scherer, 2017; Tauscher & Crawford, 2018), circular references in IFC relationships complicate their application.

Redundancy in IFC Files : Files generated by various BIM tools often include redundant entities due to inconsistencies in import/export workflows. This redundancy contributes to inflated file sizes and ambiguity in assigning responsibility during signature verification (Du *et al.*, 2020; Sun *et al.*, 2015; Zheng *et al.*, 2024).

Optional Data and Inconsistent Implementation : Many IFC entities include optional attributes, and their population depends on the authoring software and chosen MVD. This variability may lead to missing critical metadata required for digital signing. Automated extraction and population of signature-related fields from signatory certificates can help mitigate this issue.

6. EMBEDDING DIGITAL SIGNATURES IN IFC-BASED MODEL FILES

Given the current limitations of the IFC format and more importantly its instantiation in current software platforms, an alternative solution is provided. A structured framework for embedding digital signatures into IFC-based BIMs, aiming to support object-level authentication, is introduced. The proposed solution is designed to work either as an integrated module within existing BIM authoring tools or as an independent utility.

As shown in Figure 7 like any usual digital signature toolkit, the framework is divided into two core processes: signing and verifying. The signing process accepts an IFC-based model, signer certificates, and a list of model objects under the signer's responsibility. It produces a digitally signed IFC-based model as output. The verification process takes the signed model as input and returns a list of objects with their identifiers, associated digital signatures, and signature verification status.

The software toolkit supporting this framework comprises three main modules: (1) the **Signing Utility**, responsible for executing the digital signing operations; (2) the **Verifying Utility**, which handles the signature validation procedures; and (3) the **Common Utilities**, which include functions for certificate handling, file I/O, cryptographic hashing, and digital signature generation.

6.1. OPTIONS FOR EMBEDDING DIGITAL SIGNATURES IN IFC-BASED BIMS

To support object-level authentication in IFC-based BIMs, each digital signature must be encapsulated in a block containing metadata and references to the objects for which the signer assumes responsibility. There are multiple strategies for embedding these signature blocks, differing in file placement and the number of signatures per block.

Signature blocks may be embedded directly within the IFC-based file or maintained in a separate file. Embedding them in the same file facilitates unified file management and long-term archiving by keeping all data centralized. In contrast, external signature files allow for independent updates and accommodate scenarios where the original model must remain unchanged.

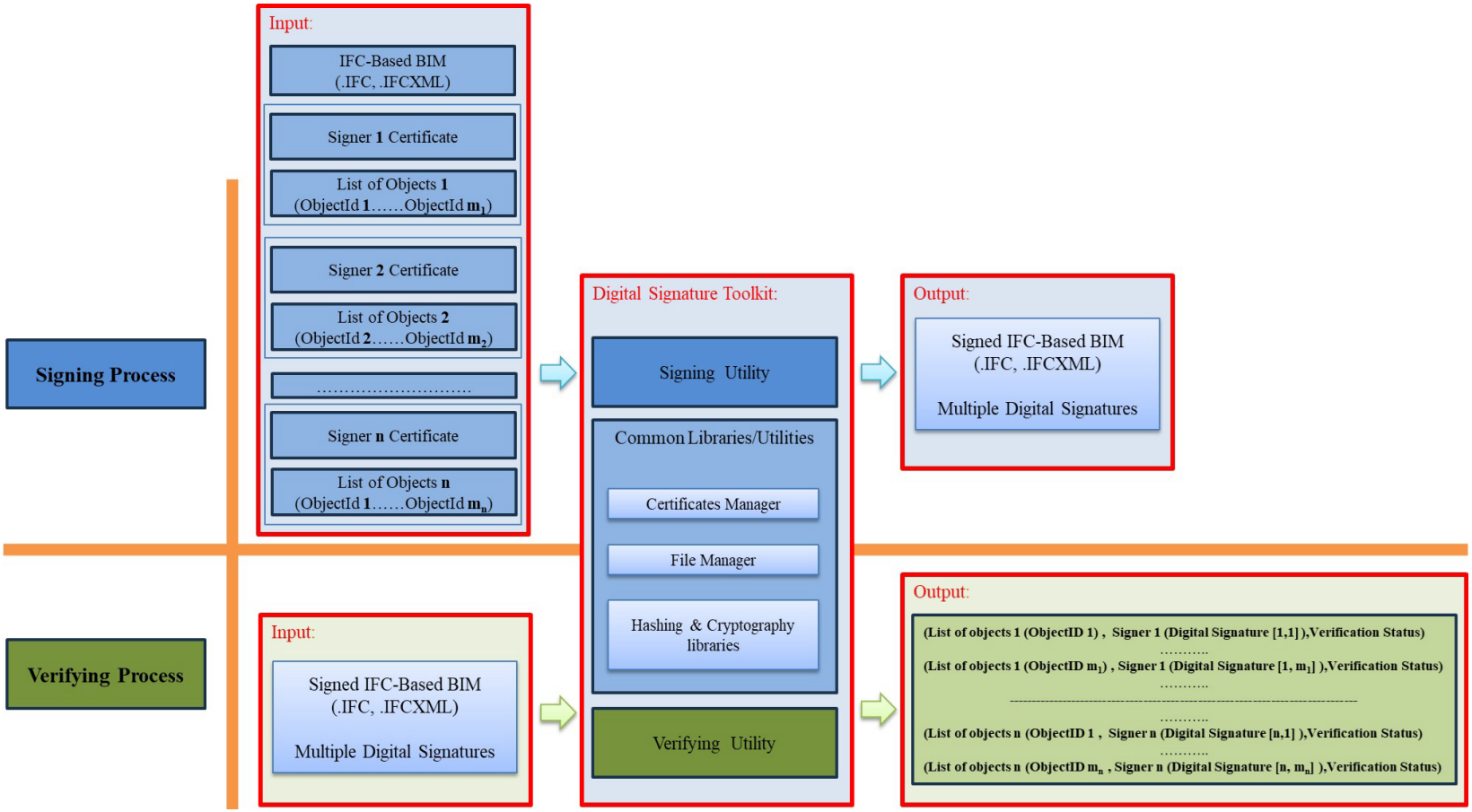

Figure 7. Overall structure of the software toolkit for adding Digital Signatures in IFC-based BIMs

Additionally, the number of signatures per block introduces further variation. Using one signature per block ensures clarity in authorship and object attribution, although it may result in data redundancy when multiple signers reference the same object. Grouping multiple signatures within a single block improves efficiency but makes it harder to isolate the contributions of individual signatories.

These dimensions result in four possible configurations, as shown in Figure 8: (1) one signature per block in the same file, (2) one per block in a separate file, (3) multiple signatures per block in the same file, and (4) multiple signatures per block in a separate file.

To balance clarity, accountability, and traceability, this research adopts the first approach : embedding one signature per block directly in the same IFC-based file.

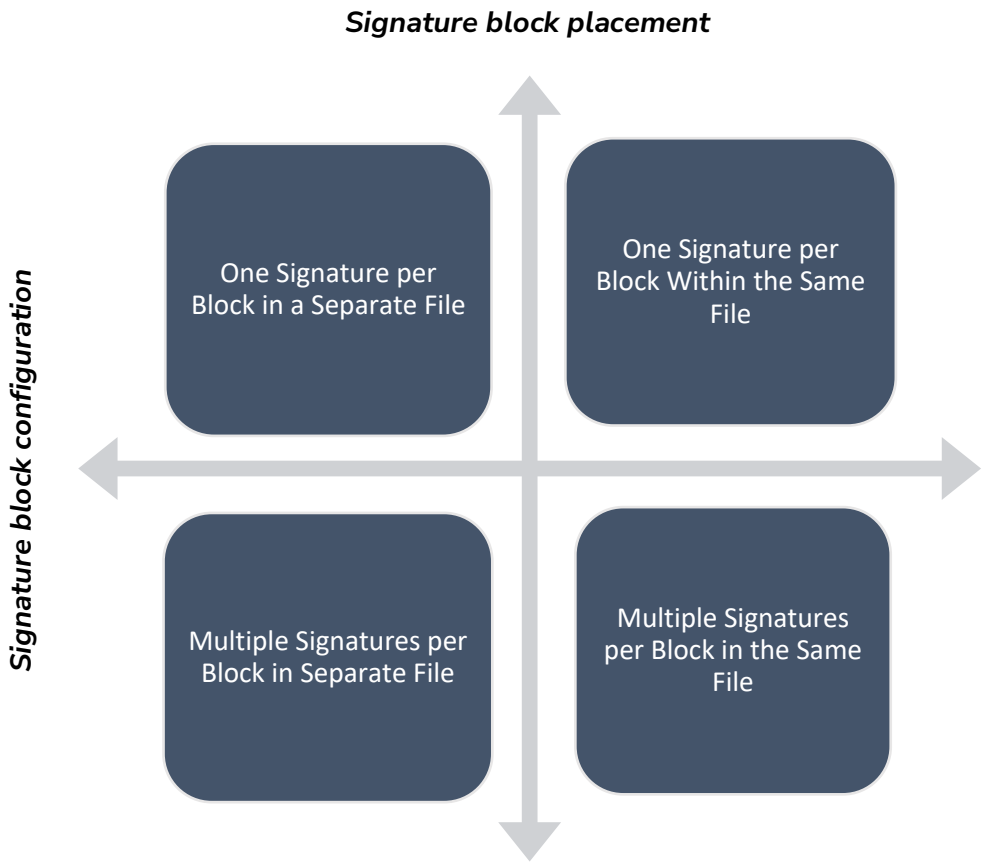

Figure 8. Potential solutions considering signature placement options and signature block configurations

6.2. EMBEDDING A DIGITAL SIGNATURE UTILIZING THE ISO 10303-21 OPTIONAL SIGNATURE SECTION

6.2.1. Signatures in IFC-Based BIMs

In the context of secure data exchange within manufacturing, STEP files—defined by ISO 10303-21—have been extended to support digital signatures by incorporating a designated optional *signature section* (Hedberg, Krima & Camelio, 2017b; Hedberg,Jr., Krima & Camelio, 2019; Hedberg *et al.*, 2020). This addition improves data trust and traceability and has inspired similar adaptations for IFC-based BIMs. While earlier efforts focused on file-level authentication (Fahdah, 2023), this research adopts the same ISO-defined signature section to enable object-level authentication in BIMs.

According to ISO 10303-21 (ISO10303-21, 2016), a STEP file may consist of five sections: one mandatory—the *header*—and four optional: *anchor*, *reference*, *data*, and *signature*. The header, marked by HEADER; and ENDSEC; contains meta-information. The anchor and reference sections define external references, while the data section holds the actual model content. Finally, the signature section—marked by SIGNATURE; and ENDSEC;—permits the embedding of one or more digital signature blocks.

IFC-based files typically implement only the mandatory header and data sections. As shown in Figure 9, this research proposes inserting digital signature blocks into the optional signature section, appended after the data section. Since current BIM authoring and viewing tools typically treat the end of the data section as the end of the file, they remain functional and unaffected by the added signature content.

Tests with popular IFC tools—such as ACCA's usBIM platform (ACCA, 2024)—confirmed that signature blocks placed beyond the data section did not interfere with typical use cases. However, the bSI IFC validation tool (version 0.7.4) (bSI, 2025a) currently flags these additional sections as invalid, since it adheres strictly to IFC's default structure. One workaround, as proposed by buildingSMART (bSI, 2025b), is to encapsulate the signature blocks in comment syntax (e.g., /* ... */) to bypass validation errors.

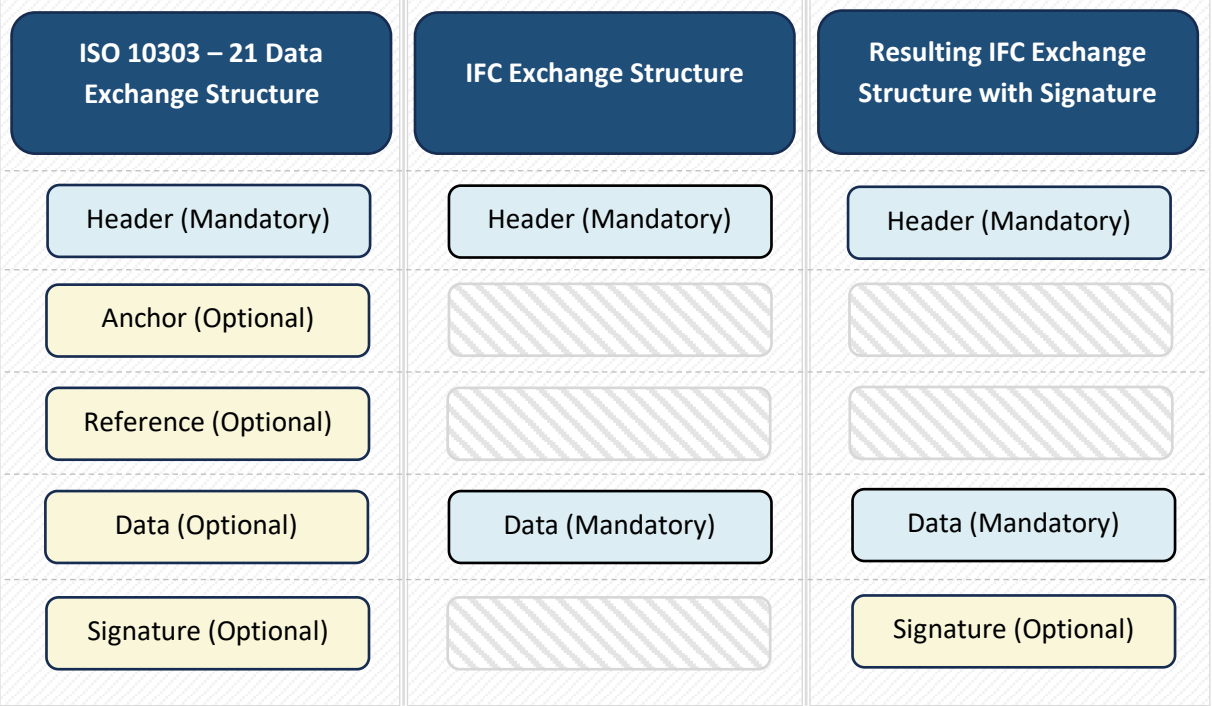

Figure 9. Comparison of ISO 10303-21 data exchange structure and IFC Exchange structure and resulting IFC exchange structure with signature

6.3. STRUCTURE OF THE SIGNATURE BLOCK

To support object-level authentication in IFC-based BIMs without altering the existing schema, a structured digital signature block is designed as an external attachment. This structure allows for seamless integration while maintaining compatibility with current BIM authoring and viewing tools. The proposed layout is shown in Figure 10. Each signature block comprises three main parts: the Header, Body, and Digital Signature.

Header. This section includes metadata about the signer, such as name, role, organization, geographical location, certificate validity, and signing timestamp, following widely accepted standards like X.509 (ITU-X509, 2019), XAdES (ETSI, 2010), and X.520 (ITU-X520, 2019). An optional field stores the hash of the previous signature block—or of the entire IFC data section in the first block—to support block chaining and detect any tampering or missing signatures.

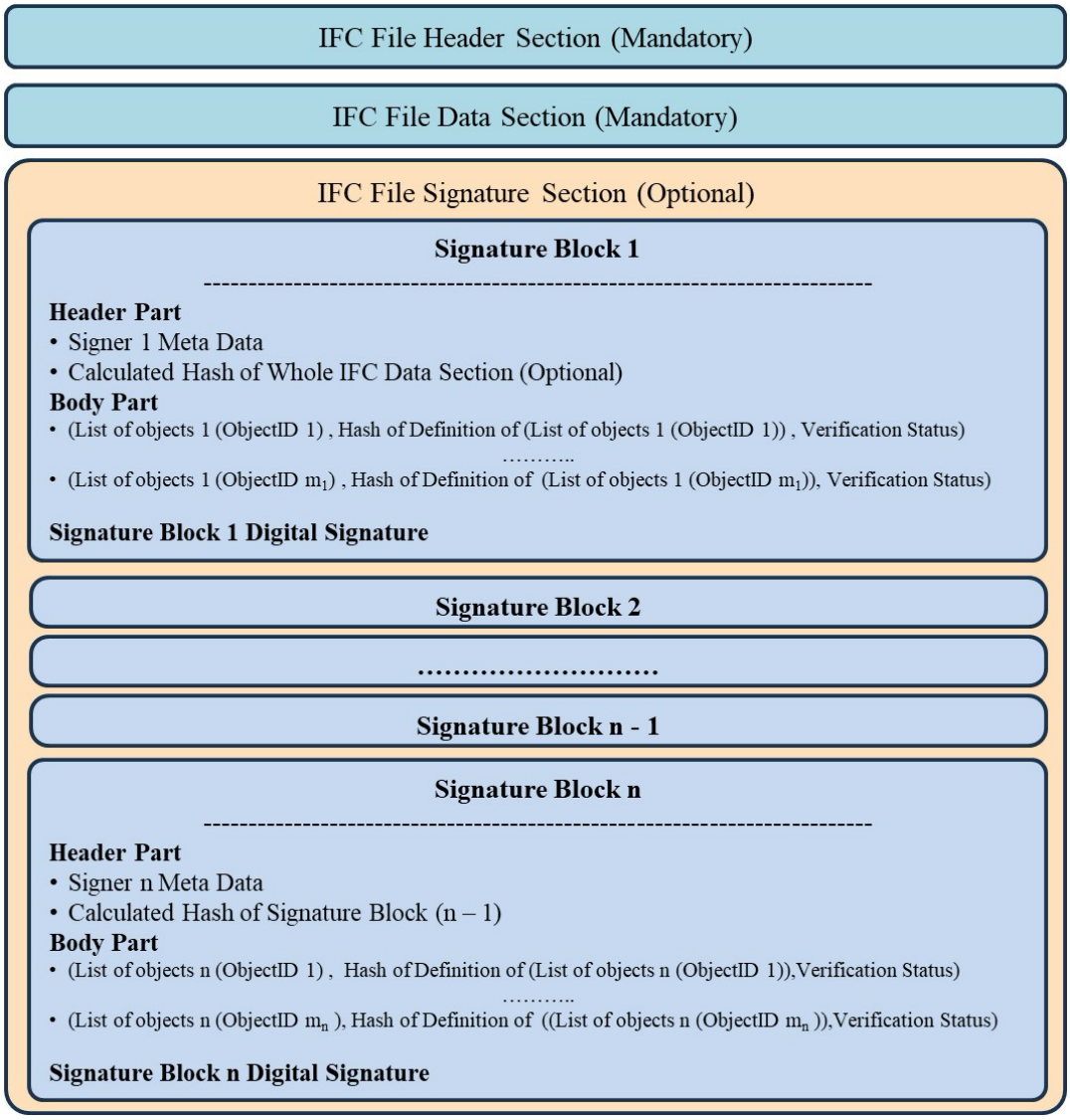

Figure 10. Structure of the signature block for embedding digital signatures into IFC-based BIMs at the object level

Body. This portion holds a list of triplets, each representing a signed object through its ObjectID, the computed hash of its definition, and a verification status. The hash ensures object-level data integrity, while the status field indicates whether the object remains unaltered ("valid"), has been modified ("invalid"), or is yet to be verified ("unverified").

Digital Signature. The entire block is digitally signed by the signer, ensuring that any post signing modifications are detectable. This not only secures the integrity of the block but also binds the signer's identity and professional responsibility to specific elements of the model, promoting trust and accountability.

6.3.1. Creating the Signature Block

The process of generating a signature block for embedding into IFC-based BIMs involves several sequential steps to ensure reliable object-level authentication and integrity. Each block is uniquely identified using a UUID and assigned a sequence number to establish its position in the signature chain. This helps verify block order and supports sequential validation when multiple signatures are present.

The signer's metadata—such as name, organization, role, certificate validity, and signing time—is collected either from user input or extracted from a digital certificate. To maintain consistency, it is recommended to align these details with recognized standards including X.509, XAdES, and X.520 (ITU-X509, 2019; ITU-X520, 2019; ETSI, 2010).

Next, the Digital Signature Toolkit receives a list of ObjectIDs corresponding to the BIM elements for which the signer is responsible. Definitions for each object are then extracted from the IFC file, enabling the generation of a hash for each. Among various available algorithms, SHA-256 was selected due to its strong security and practical performance balance (Alamgir, Nejati & Bright, 2024). However, this choice remains adaptable to future requirements.

These elements are assembled into a triplet structure containing the ObjectID, its hash, and an initial verification status set to "unverified." Additionally, the header stores the hash of the previous block (or the entire data section for the first block) to maintain continuity across signature blocks.

The entire block is then signed using the signer's private key, forming the digital signature portion. Finally, the signature block is embedded in the IFC file using the optional SIGNATURE; section defined by ISO 10303-21 (ISO10303-21, 2016), placed after the ENDSEC; of the data section to avoid disrupting standard IFC software tools.

6.3.2. Implementation Key Points and Considerations

Implementing digital signatures in IFC-based BIMs requires addressing several critical aspects to ensure the reliability, efficiency, and compatibility of the solution. This subsection outlines the major decisions and techniques employed during implementation.

Hash Calculation Scope.

To maintain stability and prevent false indications of tampering, hash computations are limited to the data section of the IFC file. The header section is excluded, as it may change with every import, export, or save operation—due to updates in metadata or timestamps—without affecting

the actual BIM content. Including the header in hash calculations would lead to frequent verification failures caused by these non-substantive changes.

Canonicalization for Consistency.

To ensure consistent hash values across different platforms, canonicalization techniques are applied to the data section prior to hashing:

- **Whitespace and Line Break Normalization:** Superfluous characters such as tabs, spaces, and carriage returns are standardized or removed to prevent discrepancies.
- **Object Order Assumptions:** Although object order in STEP-based IFC files is not semantically significant, this implementation assumes line order remains unchanged. Sorting based on ObjectIDs, while ideal for consistency, was avoided due to performance concerns. Importantly, line order only affects verification if the hash of the entire data section is included in the first signature block.
- **Comment Handling:** Comments within the data section are ignored by default. However, they are considered in the hash if the optional full-section hash is included in the signature block.

Performance Optimization.

Hashing each object can be computationally demanding for large models. Future optimizations, such as parallel processing, may be needed to maintain efficiency.

Impact on File Size.

Adding signature blocks—especially in multi-stakeholder scenarios—can lead to a noticeable increase in IFC file size. This is particularly relevant when many signatures are appended across extensive object lists.

6.3.3. Implementation Summary and Performance Evaluation

This subsection outlines the implementation process and performance evaluation of the digital signature embedding solution. The prototype was developed using C# in Microsoft Visual Studio 2022. To test scalability and efficiency, a 70 MB IFC file containing 1,131,327 ObjectIDs was used, simulating a realistic BIM environment.

In the test, three distinct object lists—each assigned to a different engineer—were defined such that they covered the entire dataset without overlaps. Initially, the signing operation required approximately 12 seconds on a laptop equipped with an Intel Core i7-8550U processor and 16 GB of RAM. Through algorithmic refinement and data structure optimization, execution time was

reduced to under 3 seconds, significantly improving performance. It was observed that hash computation was memory-intensive, underscoring the importance of effective memory management for large-scale models.

Following the embedding of the signature blocks, the IFC file size nearly doubled, posing concerns for data transmission and software responsiveness. Compression techniques such as GZip (Microsoft, 2022) and CBOR (Bormann & Hoffman, 2013) were tested to mitigate the size increase. However, due to the inherently high entropy of cryptographic hash outputs—designed for security and randomness—compression proved ineffective (Magfirawaty, Suryadi & Ramli, 2017; Erbay & Ergïn, 2018; Loza & Matuszewski, 2014; Gupta & Agarwal, 2008).

The limited impact of compression and the large file overhead highlighted the impracticality of the initial solution. As a result, efforts were redirected toward restructuring the signature block format to address these limitations, as discussed in the following section.

6.4. RESTRUCTURING SIGNATURE BLOCKS TO OPTIMIZE FILE SIZE

To address the significant file size increase encountered in the initial implementation, the structure of the signature blocks was redesigned to improve efficiency. The primary issue was the large volume of individual object-level hashes, which greatly inflated the file size. To reduce this overhead, the revised approach introduces the concept of object collections.

Rather than generating a separate hash for each object, the definitions of objects within each collection are concatenated into a single string, and one hash is computed per collection. These collection-level hashes are then compressed to further reduce storage requirements. This structure allows for continued support of object-level authentication while significantly limiting the data volume added by digital signatures. The redesigned signature block format is illustrated in Figure 11.

Implementation Steps and Test Results

The modified implementation follows these steps: assign a UUID and sequence number, compile signer metadata, input object collections, extract and concatenate object definitions, calculate and compress hashes, construct the body section, include the previous block's hash, generate the digital signature, and embed the block.

Testing was conducted on the same 70 MB IFC model used previously. Each of the three signature blocks—assigned to three engineers—contained three object collections. The file size increase was reduced to under 20 MB after hash calculation and further reduced to less than 3 MB with compression. This is a notable improvement over the original approach, where the file size nearly doubled. Performance remained consistent, with signing times staying below 3 seconds.

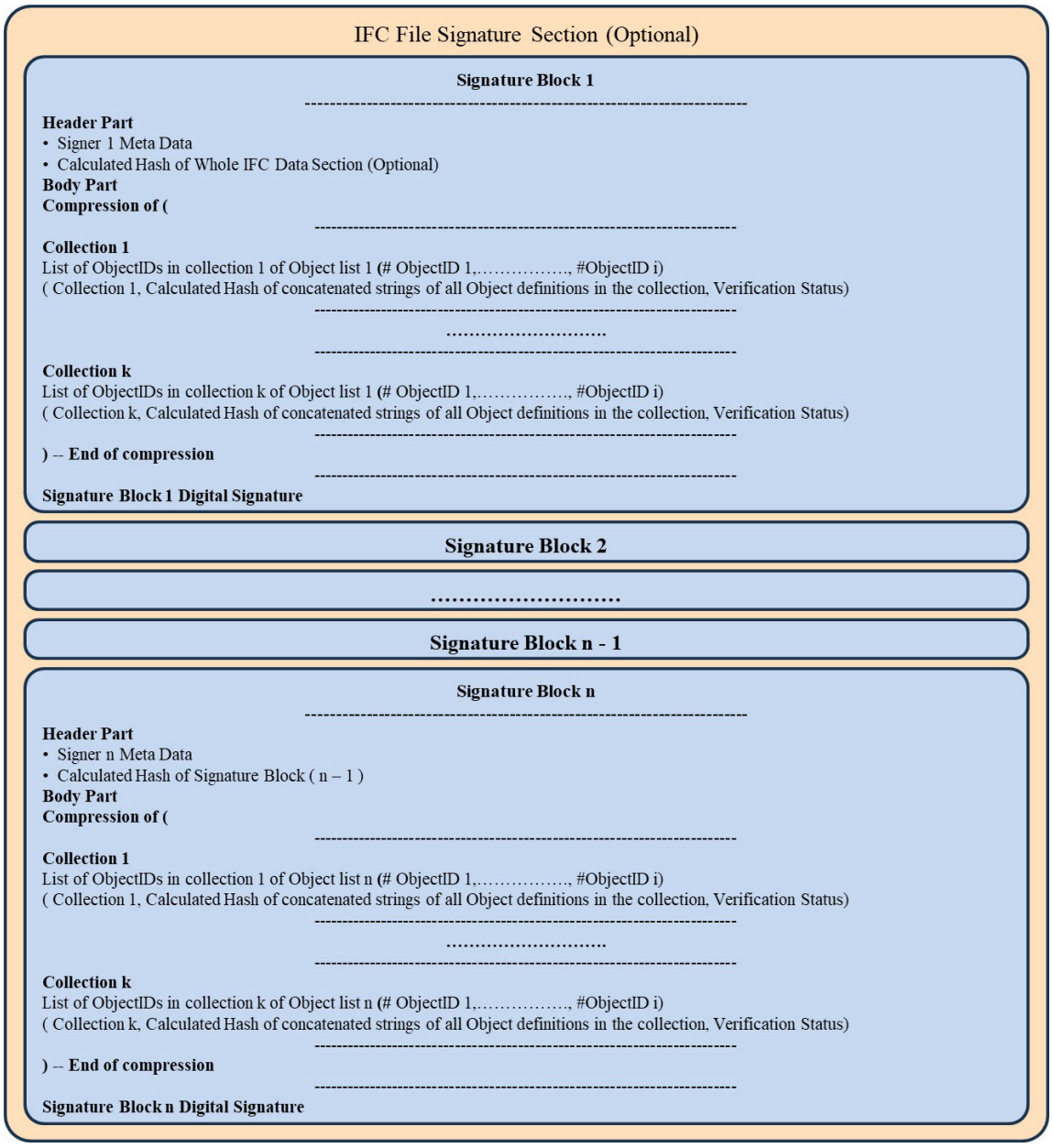

Figure 11. Optimized structure of the signature block using collections for embedding digital signatures into IFC-based BIMs

6.5. DISCUSSION AND COMPARISON OF PROPOSED SIGNATURE BLOCK STRUCTURES

This section compares the two implemented digital signature block structures, each offering unique strengths and limitations. Table 6 summarizes the key differences between object-level and collection-level approaches.

The initial structure focused on object-level authentication, computing a separate hash for each object within the IFC model. While this method offered high granularity and precise tampering detection, it introduced substantial overhead. The large number of hashes significantly increased the file size, negatively impacting the usability of BIM tools and the efficiency of file transmission.

To address this limitation, a restructured design was implemented using collection-level authentication. In this approach, object definitions within a collection are concatenated, and a single hash is computed per collection. This substantially reduced the number of hashes and allowed effective compression, minimizing the impact on file size.

Despite its benefits, the restructured approach trades off authentication granularity. While it can detect changes within a collection, it does not isolate tampered individual objects. However, if a collection contains only one object, the collection-level and object-level structures are functionally equivalent.

In summary, the restructured signature block presents a more scalable and efficient solution for large IFC models, balancing integrity assurance with file size management.

Table 6. Comparison of initial and restructured signature block structures

Aspect	Initial Signature Block (Object-Level)	Restructured Signature Block (Collection-Level)
Tampering Detection	Detects individual object changes	Detects changes at the collection level only
File Size Impact	Large increase due to many hashes	Reduced file size through grouping and compression
Equivalence Case	Always object-specific	Matches object-level structure if collection has one object

7. CONCLUSION AND FUTURE WORK

This research addressed a critical gap in the built asset industry by proposing a practical and scalable solution for embedding digital signatures at the object level within IFC-based BIMs. As the industry increasingly embraces digital collaboration, the need for robust mechanisms to ensure data authenticity and integrity becomes paramount. Current file-level authentication methods fall short in enabling traceable accountability in complex, multi-stakeholder environments. This research presents a structured framework that introduces object- and collection-level digital signature capabilities without modifying the IFC data schema, thus maintaining interoperability and compatibility with openBIM workflows.

The study identified the limitations of IFC data schema-dependent approaches and transitioned toward a schema-independent solution. The developed framework includes a signature block structure embedded in the optional ISO 10303-21 signature section of IFC files, allowing digital signatures to be attached without interfering with existing authoring tools. Initial implementation using object-level hashing demonstrated technical feasibility but resulted in significant file size increase. In response, a restructured signature block—using collection-level hashing and compression—was introduced, reducing file size impact while preserving authentication capabilities. This restructured approach was tested on large IFC datasets, showing improved performance and practicality.

Future Work

While the developed framework shows promise, further work and development is required to advance its applicability and adoption:

- **Real-world Validation:** The framework should be deployed in actual BIM projects to assess its performance under diverse workflows, project types, and software environments.
- **Integration with BIM Tools:** Practical implementation would benefit from integration into commercial BIM platforms through plugins or extensions, enabling seamless signing and verification within existing authoring tools.
- **Standards and Regulatory Advocacy:** Engaging with buildingSMART International to propose formal support for optional digital signature sections in IFC exchange structures could enhance the standardization and acceptance of the solution.
- **Broader Applicability:** Since the solution is based on ISO 10303, it could be extended to other domains that use STEP-based data exchange formats and require similar levels of data integrity assurance.

In summary, this research introduces a novel and technically feasible approach for embedding digital signatures into BIM data at the object level. By balancing interoperability, performance, and authentication requirements, the proposed solution enhances digital trust and sets the foundation for future innovations in secure BIM data exchange.

Considerations in the development of IFC5

One of the objectives in the development of IFC 5 is to establish sufficient flexibility for defining and incorporating new domains through an Entity Component System (ECS) architecture. This approach emphasizes composition over inheritance, following the composite reuse principle to increase the reusability of definitions and facilitate the addition of new specifications. While this design philosophy enhances modularity and extensibility, it introduces complexity in information retrieval, particularly when following relationships and references within the model. In considering digital authentication within the IFC5 framework, a critical gap to be addressed is the insufficient consideration of how information and relations are extracted from the model, along with the need for simplifying these relationships to improve overall system usability and performance.

Two primary options emerge for addressing digital signature requirements within the IFC 5 framework. The first approach involves adding a new container specifically designed for digital signatures, which would contain all required metadata, store calculated digital signatures, and associate with all non-abstract entities in the IFC data schema. Alternatively, the second approach focuses on reusing existing entities, particularly the IfcOwnerHistory entity, to resolve current limitations such as storing only the last owner and accommodating single ownership scenarios. This reuse strategy would enable multiple owners for shared accountability scenarios, provide the capability to store comprehensive ownership history, and solve the critical issue of storing calculated digital signatures within the existing framework structure.

REFERENCES

Abd Jamil, A. H. & Fathi, M. S. (2020). Enhancing BIM-Based Information Interoperability: Dispute Resolution from Legal and Contractual Perspectives. *Journal of Construction Engineering and Management*, 146(7), 05020007. doi: 10.1061/(ASCE)CO.19437862.0001868.

ACCA. (2024). BIM Software | ACCA. Retrieved on 2024-09-20 from: https://www.accasoftware.com/en/bim-software.

Afsari, K., Eastman, C. & Castro-Lacouture, D. (2017). JavaScript Object Notation (JSON) data serialization for IFC schema in web-based BIM data exchange. *Automation in Construction*, 77, 24–51. doi: 10.1016/j.autcon.2017.01.011.

Afsari, K. & 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. doi: 10.22260/ISARC2016/0127.

Afsari, K., Eastman, C. & Shelden, D. (2016). Data Transmission Opportunities for Collaborative Cloud-Based Building Information Modeling. doi: 10.5151/despro-sigradi2016-448.

Alamgir, N., Nejati, S. & Bright, C. (2024). SHA-256 Collision Attack with Programmatic SAT. *CEUR Workshop Proceedings*, 3717, 91–110.

Alwash, A., Love, P. E. D. & Olatunji, O. (2017). Impact and Remedy of Legal Uncertainties in Building Information Modeling. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, 9(3), 04517005. doi: 10.1061/(ASCE)LA.19434170.0000219.

Arensman, D. B. & Ozbek, M. E. (2012). Building Information Modeling and Potential Legal Issues. *International Journal of Construction Education and Research*, 8(2), 146–156. doi: 10.1080/15578771.2011.617808.

Ariffin, N. A. M., Abdulhalem, A. A. & Husin, N. A. (2021). Text and Image: A new hybrid authentication Scheme. *Journal of Physics: Conference Series*, 1793(1), 012047. doi: 10.1088/1742-6596/1793/1/012047. Publisher: IOP Publishing.

ARINC827-1. (2020). ARINC827-1· 827-1 Electronic Distribution of Software by Crate (EDS Crate). Retrieved on 2024-01-25 from: https://aviation-ia.sae-itc.com/standards/arinc8271-827-1-electronic-distribution-software-crate-eds-crate.

ARINC835-1. (2014). ARINC835-1· ARINC Report 835-1: Guidance for Security of Loadable Software Parts Using Digital Signatures. Retrieved on 2024-01-25 from: https://aviationia.sae-itc.com/standards/arinc835-1-arinc-report-835-1-guidance-security-loadablesoftware-parts-using-digital-signatures.

Arutyunov, V. V. (2012). Identification and authentication as the basis for information protection in computer systems. *Scientific and Technical Information Processing*, 39(3), 133–138. doi: 10.3103/S0147688212030021.

Azhar, S. (2011). Building Information Modeling (BIM): Trends, Benefits, Risks, and Challenges for the AEC Industry. *Leadership and Management in Engineering*, 11(3), 241–252. doi: 10.1061/(ASCE)LM.1943-5630.0000127. Publisher: American Society of Civil Engineers.

Baranova, O. (2021). Open data formats in building information modeling. *24th International Scientific Conference on Construction the Formation of Living Environment*, 263, 04062. doi: 10.1051/e3sconf/202126304062.

Batini, C. & Scannapieca, M. (2006). *Data Quality*. Springer Berlin Heidelberg. doi: 10.1007/3540-33173-5.

Bimchain. (2018). Bimchain. Retrieved on 2023-02-17 from: https://bimchain.io/.

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

Bormann, C. & Hoffman, P. E. (2013). *Concise Binary Object Representation (CBOR)* (Report n°RFC 7049). Retrieved on 2024-10-03 from: https://datatracker.ietf.org/doc/r fc7049.

bSI. (2023). IFC4.3.2.0 Documentation. Retrieved on 2024-05-07 from: https://standards.buildingsmart.org/IFC/RELEASE/IFC4_3/.

bSI. (2023). IFC4.3.2.0 Documentation. Retrieved on 2024-05-07 from: https://standards.buildingsmart.org/IFC/RELEASE/IFC4_3/.

bSI. (2024a). Industry Foundation Classes (IFC). Retrieved on 2024-05-06 from: https://technical.buildingsmart.org/standards/ifc/.

bSI. (2024b). Model View Definitions (MVD). Retrieved on 2024-05-06 from: https://technical.buildingsmart.org/standards/ifc/mvd/.

bSI. (2024a). IFC Formats. Retrieved on 2024-11-26 from: https://technical.buildingsmart.org/standards/ifc/ifc-formats/.

bSI. (2024b). Industry Foundation Classes (IFC). Retrieved on 2024-05-06 from: https://technical.buildingsmart.org/standards/ifc/.

bSI. (2024c). Information Delivery Specification (IDS) Online Specification. Retrieved on 202504-01 from: https://github.com/buildingSMART/IDS/blob/development/Documentation/UserManual/README.md.

bSI. (2025a). buildingSMART IFC Validation Service. Retrieved on 2025-04-23 from: https://validate.buildingsmart.org/.

bSI. (2025b). Digital signatures (IVS-499 and IVS-500) buildingSMART/validate. Retrieved on 2025-06-02 from: https://github.com/buildingSMART/validate/pull/190.

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J. & Sweetnam, J. (2020). NIST SPECIAL PUBLICATION 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events.Retrieved on 2025-02-03 from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-25.pdf.

Celoza, A., de Oliveira, D. P. & 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. doi: 10.1061/JLADAH.LADR-916. Publisher: American Society of Civil Engineers.

Chen, L., Moody, D., Regenscheid, A. & Robinson, A. (2023). *NIST FIPS 186-5: Digital Signature Standard (DSS)* (Report n°NIST FIPS 186-5). Gaithersburg, MD: National Institute of Standards and Technology (U.S.).

Chipman, T., Liebich, T. & Thomas, M. (2016). mvdXML- Specification of a Standardized Format to Define and Exchange Model View Definitions with Exchange Requirements and Validation Rules. buildingSMART.

Deng, Y., Gan, V. J. L., Das, M., Cheng, J. C. P. & Anumba, C. (2019). Integrating 4D BIM and GIS for Construction Supply Chain Management. *Journal of Construction Engineering and Management*, 145(4), 04019016. doi: 10.1061/(ASCE)CO.1943-7862.0001633. Publisher: American Society of Civil Engineers.

Dong, B., Lam, K., Huang, Y. & Dobbs, G. (2007). A comparative study of the IFC and gbXML informational infrastructures for data exchange in computational design support environments. *IBPSA 2007 - International Building Performance Simulation Association 2007*, pp. 1530–1537.

Dong, H., Yaqiong, H., Huaiguang, W. & Duan, Q. (2022). Research on Key technologies and development of blockchain. *Proceedings of SPIE - The International Society for Optical Engineering*, 12456, 59–66. doi: 10.1117/12.2659352.

Du, X., Gu, Y., Yang, N. & Yang, F. (2020). IFC File Content Compression Based on Reference Relationships. *Journal of Computing in Civil Engineering*, 34(3), 04020012. doi: 10.1061/(ASCE)CP.1943-5487.0000894.

Erbay, C. & Ergïn, S. (2018). Random Number Generator Based on Hydrogen Gas Sensor for Security Applications. *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 709–712. doi: 10.1109/MWSCAS.2018.8624016.

ETSI. (2010). ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)" [Technical Specification]. ETSI (European Telecommunications Standards Institute).

Fahdah, I. (2023). IfcFilesSigning. Retrieved on 2024-02-02 from: https://github.com/Ibrahim Fahdah/IfcFilesSigning.

Fakour, M. & Poirier, E. A. (2024). Exploring the digital authentication of built asset information models at the object level. *Proceedings of the 41st International Conference of CIB W78, Marrakech, Morocco, 2-3 October, ISSN: 2706-6568.* (ISSN: 2706-6568), http://itc.scix.net/paper/w78-2024-40

Fakour, M. & Poirier, E. A. (2025). Exploring the Potential of Digital Signature of Building Information Models to Improve Trust, Transparency, and Traceability in Construction Projects. *Advances in Information Technology in Civil and Building Engineering*, pp. 178–192. doi: 10.1007/978-3-031-84208-5_15.

Fakour, M., Jaud, S. & Poirier, E. A. (2025). Framework for Embedding Digital Signatures in IFC-Based Bims for Authentication and Data Integrity Verification at the Object level [SSRN Scholarly Paper]. Rochester, NY: Social Science Research Network. Retrieved on 202507-15 from: https://papers.ssrn.com/abstract=5248778.

FDA. (2018). Data Integrity and Compliance with Drug CGMP Questions and Answers Guidance for Industry. Pharmaceutical Quality/Manufacturing Standards (CGMP).

Frei, F. (2019). OKSTRA und IFC – ein Vergleich. *Strasse und Autobahn*, 70(5), pp 410–4. Retrieved from: https://trid.trb.org/View/1648414.

Gao, W., Lu, W. & Fung, A. (2024). OpenBIM in the Global Architecture Engineering and Construction Industry: A Literature Review of Academic Research. *International Journal of Construction Management*. doi: 10.1080/15623599.2024.2392302.

Girard, S. & Watkin, A. (2021). Meeting Data Integrity ALCOA+ Principles Using Digital Data Management Solutions. Retrieved from: https://www.eurotherm.com/life-sciencescpg/data-integrity-life-sciences/alcoa/.

Grassi, P. A., Garcia, M. E. & Fenton, J. L. (2017). *Digital identity guidelines: revision 3* (Report n°NIST SP 800-63-3). Gaithersburg, MD. Retrieved on 2023-11-16 from: https: //nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

Grivei, A.-C. (2015). Touch based biometric authentication for Android devices. *2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. WSD–15–WSD–18. doi: 10.1109/ECAI.2015.7301209.

Gu, N., Singh, V. & Wang, X. (2010). Applying augmented reality for data interaction and collaboration in BIM. *Proceedings of the 15th International Conference on Computer Aided Architectural Design in Asia, CAADRIA 2010*, pp. 511–520.

Guennoun, M., Abbad, N., Talom, J., Rahman, S. M. M. & El-Khatib, K. (2009). Continuous authentication by electrocardiogram data. *2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH)*, pp. 40–42. doi: 10.1109/TICSTH.2009.5444466.

Gupta, A. & Agarwal, S. (2008). Compression using encryption. *Lecture Notes in Electrical Engineering*, 6, 645–653. doi: 10.1007/978-0-387-74935-8_44.

Guru, D., Perumal, S. & Varadarajan, V. (2021). Approaches towards blockchain innovation: A survey and future directions. *Electronics (Switzerland)*, 10(10). doi: 10.3390/electronics10101219.

Hedberg, Thomas, J., Helu, M., Krima, S. & Barnard Feeney, A. (2020). *Recommendations on ensuring traceability and trustworthiness of manufacturing-related data* (Report n°NIST AMS

300-10). Gaithersburg, MD. Retrieved on 2024-07-10 from: https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.300-10.pdf.

Hedberg, T. D., Hartman, N. W., Rosche, P. & Fischer, K. (2017a). Identified research directions for using manufacturing knowledge earlier in the product life cycle. *International Journal of Production Research*, 55(3), 819–827. doi: 10.1080/00207543.2016.1213453. Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/00207543.2016.1213453.

Hedberg, T. D., Krima, S. & Camelio, J. A. (2017b). Embedding X.509 Digital Certificates in Three-Dimensional Models for Authentication, Authorization, and Traceability of Product Data. *Journal of Computing and Information Science in Engineering*, 17(1), 011008. doi: 10.1115/1.4034131.

Hedberg,Jr., T. D., Krima, S. & Camelio, J. A. (2019). Method for Enabling a Root of Trust in Support of Product Data Certification and Traceability. *Journal of Computing and Information Science in Engineering*, 19(041003). doi: 10.1115/1.4042839.

Hijazi, A. A., Perera, S., Calheiros, R. N. & 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. doi: 10.1061/(ASCE)CO.19437862.0002142. Publisher: American Society of Civil Engineers.

Holzer, D. (2007). Are you talking to me? Why BIM alone is not the answer.

Holzer, D. (2011). BIM's Seven Deadly Sins. *International Journal of Architectural Computing*, 9(4), 463–480. doi: 10.1260/1478-0771.9.4.463. Publisher: SAGE Publications.

Huang, Y., Bian, Y., Li, R., Zhao, J. L. & Shi, P. (2019). Smart Contract Security: A Software Lifecycle Perspective. *IEEE Access*, 7, 150184–150202. doi: 10.1109/ACCESS.2019.2946988.

Hwang, B.-G., Ngo, J. & Her, P. W. Y. (2020). Integrated Digital Delivery: Implementation status and project performance in the Singapore construction industry. *Journal of Cleaner Production*, 262, 121396. doi: 10.1016/j.jclepro.2020.121396.

IEEE 802.1AE-2018. (2018). IEEE Standard for Local and Metropolitan Area Networks-Media Access Control (MAC) Security.

Ismail, A., Nahar, A. & Scherer, R. (2017). Application of Graph Databases and Graph Theory Concepts for Advanced Analysing of BIM Models Based on IFC Standard.

ISO10303-21. (2016). ISO 10303-21:2016. Retrieved on 2024-07-31 from: https://www.iso.or g/standard/63141.html.

ISO16739-1:2024. (2024). ISO 16739-1:2024. Retrieved on 2024-05-07 from: https://www.iso. org/standard/84123.html.

ISO19650-1. (2018). ISO 19650-1:2018. Retrieved on 2024-11-07 from: https://www.iso.org/standard/68078.html.

ISO21597-1. (2020). ISO 21597-1:2020. Retrieved on 2024-01-24 from: https://www.iso.org/standard/74389.html.

ISO/IEC2501. (2008). ISO/IEC 25012:2008.

ISO/IEC27000. (2018). ISO/IEC 27000:2018. Retrieved on 2025-03-04 from: https://www.iso. org/standard/73906.html.

ITU-X509. (2019). X.509: Information Technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate Frameworks. Retrieved on 2024-0513 from: https://www.itu.int/rec/T-REC-X.509-201910-I/en.

ITU-X520. (2019). *X.520: Information Technology - Open Systems Interconnection - The Directory: Selected Attribute Types*. Retrieved on 2024-05-14 from: https://www.itu.int/ rec/T-REC-X.520-201910-I/en.

Jain, A., Ross, A. & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4–20. doi: 10.1109/TCSVT.2003.818349. Conference Name: IEEE Transactions on Circuits and Systems for Video Technology.

Jaud, Š. & 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. doi: 10.5194/isprs-annals-X-4-W5-2024203-2024.

Jiang, S., Jiang, L., Han, Y., Wu, Z. & Wang, N. (2019). OpenBIM: An Enabling Solution for Information Interoperability. *Applied Sciences*, 9(24), 5358. doi: 10.3390/app9245358.

Ju, S.-h., Seo, H.-s., Han, S.-h., Ryou, J.-c. & Kwak, J. (2013). A Study on User Authentication Methodology Using Numeric Password and Fingerprint Biometric Information. *BioMed Research International*, 2013(1), 427542. doi: 10.1155/2013/427542. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1155/2013/427542.

Kabiri, Y. & Sharifzadeh, M. (2022). Blockchain and Smart Contracts. In *Industry 4.0 Vision for the Supply of Energy and Materials: Enabling Technologies and Emerging Applications* (pp. 59–72). wiley. doi: 10.1002/9781119695868.ch2.

Kim, I., Lee, Y., Han, C.-H., Kim, G. & Choi, J. (2020). Validation of Support for Creation of License Drawings Using Application for openBIM-Based Automatic Generation of 2D Drawings. *Applied Sciences*, 10(18), 6470. doi: 10.3390/app10186470.

Kishore, N., Raina, P., Nayar, N. & Thakur, M. (2021). Fast Implementation of Digital Signatures Using Parallel Techniques. *2021 International Conference on Computing, Communication and Green Engineering, CCGE 2021*, pp. 1–7. doi: 10.1109/CCGE50943.2021.9776382.

Lee, Y.-C., Eastman, C., Solihin, W. & See, R. (2016). Modularized rule-based validation of a BIM model pertaining to model views. *Automation in Construction*, 63, 1–11. doi: 10.1016/j.autcon.2015.11.006.

Lee, Y.-C., Shariatfar, M., Ghannad, P., Zhang, J. & 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. doi: 10.1061/(ASCE)CP.1943-5487.0000888.

Li, J. & Kassem, M. (2021). Applications of Distributed Ledger Technology (DLT) and Blockchain-enabled Smart Contracts in Construction. *Automation in Construction*, 132, 103955. doi: 10.1016/j.autcon.2021.103955.

Loza, S. & Matuszewski, L. (2014). A true random number generator using ring oscillators and

SHA-256 as post-processing. *2014 International Conference on Signals and Electronic Systems (ICSES)*, pp. 1–4. doi: 10.1109/ICSES.2014.6948739.

Luttun, J. & Krijnen, T. (2021). An Approach for Data Extraction, Validation and Correction Using Geometrical Algorithms and Model View Definitions on Building Models. *Proceedings of the 18th International Conference on Computing in Civil and Building Engineering*, pp. 529–543. doi: 10.1007/978-3-030-51295-8_38.

Magfirawaty, Suryadi, M. T. & Ramli, K. (2017). Development and performance analysis for high-quality discrete time chaos random number generator using LFSR-based hash function. *Far East Journal of Electronics and Communications*, 17(6), 1529–1541. doi: DOI: 10.17654/EC017061529.

Maier, F. (2020). Model Development Standards in the Construction Industry and Beyond.

Microsoft. (2022). GZipStream Class (System.IO.Compression). Retrieved on 2024-1003 from: learn.microsoft.com/en-us/dotnet/api/system.io.compression.gzipstream.

Mohammadi, S., Aibinu, A. A. & 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. doi: 10.1061/JLADAH.LADR-1040. Publisher: American Society of Civil Engineers.

Mulder, V., Mermoud, A., Lenders, V. & Tellenbach, B. (Eds.). (2023a). *Trends in Data Protection and Encryption Technologies*. Cham: Springer Nature Switzerland. doi: 10.1007/978-3031-33386-6.

Mulder, V., Mermoud, A., Lenders, V. & Tellenbach, B. (Eds.). (2023b). *Trends in Data Protection and Encryption Technologies*. Cham: Springer Nature Switzerland. doi: 10.1007/978-3031-33386-6.

Olatunji, O. A. (2011). A Preliminary Review on The Legal Implications of BIM And Model Ownership. Electronic Journal of Information Technology in Construction, 16, 687–696.

Park, J., Chen, J. & Cho, Y. (2020). Point Cloud Information Modeling (PCIM): An Innovative

Framework for As-Is Information Modeling of Construction Sites. Construction Research Congress 2020: Computer Applications - Selected Papers from the Construction Research Congress 2020, pp. 1319–1326.

Patiyoot, D. (2024). Patiyoot 2: Key Distribution, and Session Key for Authentication Protocol in Wireless Network. 2024 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), pp. 85–87. doi: 10.1109/ECTIDAMTNCON60518.2024.10480016.

Perera, S., Nanayakkara, S., Rodrigo, M. N. N., Senaratne, S. & Weinand, R. (2020). Blockchain

Technology: Is It Hype or Real in the Construction Industry? *Journal of Industrial Information Integration*, 17, 100125. doi: 10.1016/j.jii.2020.100125.

Poirier, E. A., Forgues, D. & Staub-French, S. (2017). Understanding the impact of BIM on collaboration: a Canadian case study. *Building Research & Information*, 45(6), 681–695. doi: 10.1080/09613218.2017.1324724.

Pradeep, A. S. E., Amor, R. & Yiu, T. W. (2020). Blockchain Improving Trust in BIM Data Exchange: A Case Study on BIMCHAIN. *Construction Research Congress 2020: Computer Applications*, 1174–1183. doi: 10.1061/9780784482865.124. Publisher: American Society of Civil Engineers.

Rai, A., Singh, M., Sudheendramouli, H., Panwar, V., Balaji, N. & Kukreti, R. (2023). Digital Signature for Content Authentication. Proceedings of the 2nd IEEE International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2023, pp. 1–6. doi: 10.1109/ACCAI58221.2023.10200472.

Sabale, M., Pande, V., Tagalpallewar, A., Swami, A., Pawar, A. & Baheti, A. (2024). Maintaining Data safety and accuracy through Data Integrity (DI): A Comprehensive Review. *Research Journal of Pharmacy and Technology*, 17(5), 2431–2440. doi: 10.52711/0974360X.2024.00381.

Saini, M., Arif, M. & Kulonda, D. J. (2019). Challenges to transferring and sharing of tacit knowledge within a construction supply chain. *Construction Innovation*, 19(1), 15–33. doi: 10.1108/CI-03-2018-0015. Publisher: Emerald Publishing Limited.

Sattler, L., Lamouri, S., Pellerin, R., Paviot, T., Deneux, D. & Maigne, T. (2021). A Survey About BIM Interoperability and Collaboration Between Design and Construction. *Service Oriented, Holonic and Multi-Agent Manufacturing Systems for Industry of the Future*, (Studies in Computational Intelligence), 151–179. doi: 10.1007/978-3-030-80906-5_11.

Seetha, R. (2017). An Enhanced Digital Signature Scheme. *International Journal of Applied Engineering Research*, 12(22), 11878–11884.

Shah, S. U., Fazl-e-Hadi & Minhas, A. A. (2009). New Factor of Authentication: Something You Process. *2009 International Conference on Future Computer and Communication*, pp. 102–106. doi: 10.1109/ICFCC.2009.79.

Shi, X., Liu, Y.-S., Gao, G., Gu, M. & Li, H. (2018). IFCdiff: A content-based automatic comparison approach for IFC files. *Automation in Construction*, 86, 53–68. doi: 10.1016/j.autcon.2017.10.013.

Song, S., Zhang, C. & Marks, E. (2021). Effectiveness and Practicability Analysis of BIM Adoption in the AEC Industry. Computing in Civil Engineering 2021 - Selected Papers from the ASCE International Conference on Computing in Civil Engineering 2021, pp. 530–537. doi: 10.1061/9780784483893.066.

Stallings, W. & Brown, L. (2015). *Computer security: principles and practice* (ed. Third edition). Boston: Pearson.

Sun, J., Liu, Y.-S., Gao, G. & Han, X.-G. (2015). IFCCompressor: A Content-Based Compression Algorithm for Optimizing Industry Foundation Classes Files. *Automation in Construction*, 50, 1–15. doi: 10.1016/j.autcon.2014.10.015.

Tauscher, H. & Crawford, J. (2018). Graph Representations and Methods for Querying, Examination, and Analysis of IFC Data. In Karlshøj, J. & Scherer, R. (Eds.), *eWork and eBusiness in Architecture, Engineering and Construction* (ed. 1, pp. 421–428). CRC Press. doi: 10.1201/9780429506215-53.

Turk, Z. (2020). Interoperability in construction - Mission impossible? *Developments in the Built Environment*, 4, 100018. doi: 10.1016/j.dibe.2020.100018.

van Berlo, L., Krijnen, T., Tauscher, H., Liebich, T., van Kranenburg, A., Paasiala, P. & Paasiala, P. (2021). Future of the Industry Foundation Classes: Towards IFC 5.

van Oorschot, P. C. (2020). User Authentication—Passwords, Biometrics and Alternatives. In van Oorschot, P. C. (Ed.), *Computer Security and the Internet: Tools and Jewels* (pp. 55–90). Cham: Springer International Publishing. doi: 10.1007/978-3-030-33649-3_3.

Velasquez, I., Caro, A. & Rodriguez, A. (2018). Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, 94, 30–37. doi: 10.1016/j.infsof.2017.09.012.

Volker, L. & Chao-Duivis, M. (2010). Potential conflicts with procurement law during architect selection. *W113-Special Track 18th CIB World Building Congress*, pp. P 346.

Won, J., Kim, T., Yu, J. & Choo, S. (2022). Development of the IFC Schema Extension Methodology for Integrated BIM. *Proc. Int. Conf. Educ. Res. Comput. Aided. Archit. Des. Eur.*, 2, 339–346.

Xu, H., Kim, J. & Chen, J. (2022). An iterative reference mapping approach for BIM IFCXML classified content compression. *Advanced Engineering Informatics*, 54. doi: 10.1016/j.aei.2022.101788.

Yu, Y., Zhang, Y., Yu, J. & He, X. (2023a). An Overview of the Application and Development of Data Integrity Verification Techniques. *Second International Conference on Applied Statistics,*

Computational Mathematics, and Software Engineering (ASCMSE 2023), 12784, 410–415. doi: 10.1117/12.2691857.

Yu, Y., Kim, S., Jeon, H. & Koo, B. (2023b). A Systematic Review of the Trends and Advances in IFC Schema Extensions for BIM Interoperability. *Applied Sciences*, 13(23), 12560. doi: 10.3390/app132312560.

Yun, Z., Chao, C., Haoling, W., Tao, L. & Hefang, J. (2022). Decentralized Identity and Password Authentication System based on Block Chain. *2022 IEEE 4th International Conference on Power, Intelligent Computing and Systems (ICPICS)*, pp. 481–485. doi: 10.1109/ICPICS55264.2022.9873634.

Zheng, Y., Shi, Y. & Wang, X. (2024). Research on Partial Model Extraction of Railway Infrastructure Based on the Industry Foundation Classes Files. *IEEE Access*, 12, 94690–94701. doi: 10.1109/ACCESS.2024.3425898.


buildingSMART™
Canada
ÉTS
Le génie pour l'industrie
notarius