Framework for embedding digital signatures into IFC-based BIMs for object-level authentication and data integrity verification

by

Mehdi FAKOUR

MANUSCRIPT-BASED THESIS PRESENTED TO ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
IN PARTIAL FULFILLMENT OF A MASTER'S DEGREE
WITH THESIS IN PERSONALIZED STUDY PROGRAM
M.A.Sc.

MONTREAL, "AUGUST 22,2025"

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

BOARD OF EXAMINERS

THIS THESIS HAS BEEN EVALUATED

BY THE FOLLOWING BOARD OF EXAMINERS

Mr. Erik Andrew Poirier, Thesis supervisor
Department of Construction Engineering, École de technologie supérieure

Mr. Julien Gascon-Samson, Chair, Board of Examiners
Department of Software Engineering and IT, École de technologie supérieur

Mr. Ali Motamedi, Member of the Jury
Department of Construction Engineering, École de technologie supérieure

THIS THESIS WAS PRESENTED AND DEFENDED

IN THE PRESENCE OF A BOARD OF EXAMINERS AND THE PUBLIC

ON "AUGUST 19,2025"

AT ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

ACKNOWLEDGEMENTS

My journey into this research was sparked by a deep personal interest in digital technologies and was shaped by both internal curiosity and external, practical demands. I have always been drawn to how software tools can facilitate, improve, and optimize existing processes across various domains to tackle real-world issues.

This research was further inspired by a pressing need raised by an industrial partner for authentication and data integrity verification in BIMs at the object level. Their practical question emphasized the importance of verifying the trustworthiness of specific model elements within collaborative digital environments. This request became a driving force in defining the direction of the work, highlighting its applicability and relevance beyond academic inquiry. As a result, this thesis represents not only a scientific exploration but also a meaningful response to a real-world challenge in the built asset industry.

This research project would not have been possible without the generous support of many people. I am profoundly grateful to my supervisor, Professor Poirier, for his scientific guidance, continuous encouragement, and unwavering support both within and beyond the academic setting. Moreover, He created invaluable opportunities for me to connect with researchers and professionals across academia and industry, which greatly enriched this work. I also extend my heartfelt thanks to the members of GRIDD for their support and encouragement throughout this process.

To my family, thank you for being my anchor. My parents and my brother have always stood behind me with strength, love, and encouragement, even from afar. Most importantly, I want to thank my wife, Masoome. Her unwavering love, support, understanding, and sacrifices helped me navigate the demanding path of this undertaking. She faced every challenge by my side, often putting aside her own needs to ensure I could keep going. And to our little boy, Kourosh—your laughter and energy reminded me every day why this work matters and for whom we build the future. You both gave this journey meaning beyond the pages of this thesis.

Cadre d'intégration de signatures numériques dans les BIM basés sur l'IFC pour l'authentification au niveau de l'objet et la vérification de l'intégrité des données

Mehdi FAKOUR

RÉSUMÉ

Les modèles d'information du bâtiment (BIM) ont considérablement amélioré la collaboration, l'efficacité et la gestion de l'information dans le secteur des actifs immobiliers. Cependant, garantir l'intégrité et l' authentification des données au niveau des objets reste un défi de taille. Les méthodes d'authentification actuelles au niveau des fichiers n'offrent pas une granularité suffisante pour vérifier efficacement chaque objet BIM individuellement.

Les Industry Foundation Classes (IFC) sont une norme ouverte et indépendante des fournisseurs, largement adoptée pour assurer l'interopérabilité entre les différentes plateformes logicielles BIM, ce qui en fait un candidat idéal pour l'intégration de mécanismes d'authentification avancés tels que les signatures numériques. Les signatures numériques ont été choisies en raison de leurs solides capacités cryptographiques, qui garantissent l'authenticité et l'intégrité des données, et offrent des fonctionnalités de vérification à long terme essentielles pour la responsabilité et la résolution des litiges.

Cette thèse explore deux approches distinctes pour intégrer des signatures numériques dans des modèles BIM basés sur l'IFC. Dans un premier temps, elle examine l'intégration directe des signatures numériques dans le schéma de données IFC, ce qui pose des défis importants en raison de la complexité du schéma, de la compatibilité des versions et les subtilités de la mise en œuvre. Par la suite, la recherche propose une méthode alternative, consistant à intégrer les signatures numériques directement dans les fichiers IFC sans modifier la dépendance au schéma de données IFC.

À l'aide d'une méthodologie de recherche axée sur le science de la conception, l'étude évalue systématiquement la faisabilité et la praticité de ces approches, pour finalement proposer un cadre pratique et évolutif permettant d'intégrer directement les signatures numériques dans les fichiers IFC. La solution qui en résulte met l'accent sur une perturbation minimale des flux de travail existants dans l'industrie et sur la conformité réglementaire, facilitant ainsi son adoption dans les pratiques BIM actuelles.

Mots-clés: Authentification, Intégrité des données, Validation de l'intégrité des données, Signature numérique, BIM, IFC, Schéma de données IFC, Sérialisation des fichiers IFC

Framework for embedding digital signatures into IFC-based BIMs for object-level authentication and data integrity verification

Mehdi FAKOUR

ABSTRACT

Building Information Models (BIM) has significantly enhanced collaboration, efficiency, and information management within the built asset industry. However, ensuring data integrity and authentication at the object-specific level remains a substantial challenge. Current file-level authentication methods do not provide sufficient granularity for verifying individual BIM object effectively.

Industry Foundation Classes (IFC) is an open, vendor-neutral standard widely adopted for interoperability among various BIM software platforms, making it an ideal candidate for integrating advanced authentication mechanisms such as digital signatures. Digital signatures were selected due to their robust cryptographic capabilities, which ensure data authenticity and integrity, and offer essential long-term verification features crucial for accountability and resolving disputes.

This thesis explores two distinct approaches to embed digital signatures in IFC-based BIM models. Initially, it investigates the direct integration of digital signatures within the IFC data schema, encountering significant challenges due to schema complexity, version compatibility, and implementation intricacies. Subsequently, the research proposes an alternative method, embedding digital signatures directly into IFC files without modifying the dependency to the IFC data schema.

Employing a design science research methodology, the study systematically evaluates the feasibility and practicality of these approaches, ultimately proposing a practical and scalable framework for embedding digital signatures directly into IFC files. The resulting solution emphasizes minimal disruption to existing industry workflows and regulatory compliance, facilitating its adoption within current BIM practices.

Keywords: Authentication, Data Integrity, Data Integrity Validation, Digital Signature, BIM, IFC, IFC Data Schema, IFC File Serialization

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

ASC	Agence Spatiale Canadienne
BCF	BIM Collaboration Format
BIM	Building Information Modeling
BIMs	Building Information Models
bSDD	buildingSMART Data Dictionary
bSI	buildingSMART International
CAs	Certificate Authorities
CBOR	Concise Binary Object Representation
CDEs	Common Data Environments
CSC	Construction Supply Chain
DLT	Distributed Ledger Technology
DSA	Digital Signature Algorithms
DSR	Design Science Research
DSRM	Design Science Research Methodology
DT	Digital Twin
EMA	European Medicines Agency
ER	Exchange Requirement
FBA	Formula-Based Authentication
FDA	U.S. Food and Drug Administration

GUID	Globally Unique Identifier
IDE	Integrated Development Environment
IDM	Information Delivery Manual
IDS	Information Delivery Specification
IFC	Industry Foundation Classes
IoT	Internet of Things
IP	Intellectual Property
ISO	International Organization for Standardization
ISPE	International Society for Pharmacoepidemiology
LOTAR	Long-Term Archival and Retrieval
LTV	Long Term Verification
MALD	Models As a Legal Document
MD5	Message Digest Algorithm 5
MFA	Multi-Factor Authentication
MVD	Model View Definitions
MVP	Minimum Viable Product
OTPs	One-Time Passwords
PBA	Password-Based Authentication
PIC/S	Pharmaceutical Inspection Co-operation Scheme
PINs	Personal Identification Numbers

PKI	Public Key Infrastructure
PoS	Proof of Stake
PoW	Proof of Work
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
SHA	Secure Hash Algorithm
SPF	STEP Physical File
SSL	Secure Sockets Layer
SSO	Single Sign-On
STEP	Standard for the Exchange of Product Model Data
TLS	Transport Layer Security
TOTPs	Time-based OTPs
UCM	Use Case Management Service
WHO	World Health Organization
XML	Extensible Markup Language

LIST OF SYMBOLS AND UNITS OF MEASUREMENTS

GHz	Gigahertz
GB	Gigabyte
MB	Megabyte

INTRODUCTION

Building Information Modeling (BIM) has significantly impacted the built asset industry by fostering a collaborative digital environment aimed at enhancing efficiency, productivity, and the quality of data exchange (Azhar, 2011). BIM adoption has reshaped the manner in which projects are coordinated and managed, profoundly influencing decision-making processes throughout the lifecycle of built assets (Hijazi, Perera, Calheiros & Alashwal, 2021).

The foundation of effective BIM as data-enriched 3D model relies heavily on interoperability to facilitate data exchange. The Industry Foundation Classes (IFC), developed by buildingSMART as an open, vendor-neutral standard for achieving interoperability among various software platforms (bSI, 2020). IFC aims to resolve longstanding challenges associated with software incompatibility and inefficient data conversion processes, thereby facilitating seamless information exchange. Despite these advances, substantial obstacles remain, particularly concerning data integrity and authentication at an object-specific level within BIMs. Current methods for authenticating BIM data, such as file-level verification using standard formats like PDF, are insufficient for detailed and reliable authentication of individual BIM objects.

The limitations inherent in existing approaches underscore the critical need for advanced methods capable of detailed object-level authentication and verification of data integrity within BIM workflows. Digital signatures have emerged as a promising technology for addressing these challenges, offering robust cryptographic verification mechanisms to ensure data authenticity, establish clear accountability, and provide essential non-repudiation capabilities (Mulder *et al.*, 2023).

In this context, the central aim of this thesis is to address existing gaps in object-level authentication within IFC-based BIM models data exchanges through the utilization of digital signatures. The research evaluates the capabilities and constraints of integrating digital signatures within the existing IFC schema, identifying appropriate container within the IFC data schema capable of

supporting digital signatures effectively without requiring significant modifications in the IFC data schema. Considering challenges of the integrating the digital signatures in the IFC data schema, the research aims to propose a solution which is independent of the IFC data schema by embedding digital signature blocks into IFC files.

Employing a design science research methodology, this thesis integrates insights from construction engineering, information management, and cybersecurity to propose a practical, scalable framework for embedding digital signatures into IFC-based BIM workflows. The developed framework prioritizes minimal disruption to current industry standards, thereby enhancing practical viability and ease of adoption. This research significantly contributes by establishing an approach to secure and reliable BIM data exchange to support authentication and data integrity at the object level.

The thesis structure encompasses a comprehensive literature review, a detailed explanation of the research methodology, an in-depth examination of IFC schema integration challenges and opportunities, and a thorough evaluation of the proposed framework. Each chapter systematically builds upon previous findings, ensuring a coherent presentation of theoretical and practical insights that directly contribute to advancing secure, reliable, and interoperable BIM practices within the built asset industry.

CHAPTER 1

OVERVIEW: RESEARCH MOTIVATIONS, DESIGN AND OUTCOMES

1.1 Introduction

This chapter provides a comprehensive overview of the research project and the resulting thesis. It lays out project motivations that inspired the work, describes the overall research design and its outcomes, and outlines the structure of this manuscript-based thesis.

Initially, the chapter presents the practical drivers behind the study. These include the escalating demand within the built asset industry for robust secure data exchange —especially in BIM-enabled projects where trust, transparency, and accountability are critical—and the rapid advancements in digital security technologies such as blockchain technology and digital signatures. These developments offer promising avenues for addressing the limitations inherent in current file-level authentication practices.

Subsequently, the theoretical motivations are discussed through a succinct review of the literature related to digital authentication and data integrity within the context of BIM and IFC standards. This review positions BIM not only as a digital representation of building projects but also as a transformative tool that facilitates interoperability and collaboration. However, existing practices largely focus on whole-file authentication, which is inadequate for the granular requirements of collaborative and multi-stakeholder environments. Hence, there is a compelling need for object-level authentication to ensure that every component of a BIM can be individually verified and secured.

From these practical and theoretical foundations, a clear problem statement emerges: the absence of an effective, standardized approach for authentication and data integrity verification of BIMs at the object level poses significant risks to data integrity. This problem sets the stage for the formulation of the research questions, which are addressed through a series of research contributions. These contributions include the development of a novel framework—detailed

in the journal paper—and are further supported by insights from three conference papers that explore various facets of authentication in BIMs.

Finally, the chapter concludes with an outline of the thesis structure, which is organized to first present the core journal paper on the proposed framework, followed by a discussion of the findings, implications, and contributions, and ending with appendices that include the related conference papers.

1.2 Practical motivation

From a practical standpoint, the motivation to explore this research area arises from both internal and external influences. Externally, at the outset of my studies, I had the opportunity to collaborate with Notarius—a subsidiary of Portage Cybertech—serving as our industrial partner. Notarius delivers secure digital and electronic signature solutions that enhance the legal reliability, integrity, and authenticity of digital documents. Supported by Portage CyberTech's expertise in trusted digital transactions, identity, and access management, Notarius helps businesses, universities, and municipalities transition seamlessly to secure, fully digitized workflows while preserving the long-term integrity of their electronic archives.

Currently, Notarius offers digital signature services for 2D PDF files and is now looking to expand its capabilities to include digital signatures for 3D BIM models. The company aims to develop a product that enables the secure transfer and exchange of the underlying data contained within 3D BIM models, rather than merely transferring static 2D drawings. Building on extensive experience acquired from collaborations with engineers from various disciplines in the built asset industry—as well as with lawyers and insurance companies—, Notarius aims to create a solution that accurately identifies which parts of each model along with its underlying data were designed by specific individuals and clearly establishes legal responsibilities for each part. This approach should be designed in a way to ensure that both data integrity and the authenticity of signatory identities are reliably maintained.

1.3 Theoretical motivation

1.3.1 The role of BIM in built asset industry

Building Information Modeling (BIM) is both a process and a digital output that fundamentally transforms how projects are conceived, designed, and managed throughout their life cycle (Adepoju, 2022; Fakour & Poirier, 2025). The digital artifact produced by the BIM process is a comprehensive, data-rich, object-oriented, and parametric representation of a facility that encapsulates both geometric details and alphanumeric information about buildings and infrastructure (Adepoju, 2022; Azhar, Nadeem, Mok & Leung, 2008). This federated model not only illustrates the complete life cycle of a building (Yu, Zhong & Bolpagni, 2023a; Azhar, 2011) but also serves as a centralized repository, enabling all project stakeholders to collaborate effectively.

In projects, BIM plays a critical role in facilitating seamless collaboration, as it promotes communication and knowledge sharing among participants and encourages the shift from fragmented, traditional practices to cohesive digital workflows (Poirier, Forgues & Staub-French, 2017; Adepoju, 2022). By federating data in a single, accessible model, BIM supports more informed decision-making throughout the planning, design, construction, and management phases of a project (Adepoju, 2022). This centralized approach not only enhances compliance and error rectification during the design stage (Poirier *et al.*, 2017; Nawari & Ravindran, 2019) but also underpins the broader digital transformation and digital delivery within the construction industry.

However, BIM implementation faces several challenges that can hinder its full potential. Interoperability issues, often stemming from software compatibility and data exchange problems, are a common barrier (Abd Jamil & Fathi, 2020; Mohammadi, Aibinu & Oraee, 2024). Additionally, legal uncertainties—such as intellectual property risks, difficulties in determining data ownership, and challenges in assigning responsibilities of designs or modifications—further complicate BIM adoption (Abd Jamil & Fathi, 2020; Adepoju, 2022; Fakour & Poirier, 2024,

2025). There is also a pressing need for robust data validation processes to protect against data loss, unauthorized modifications or tampering with the original data (Abd Jamil & Fathi, 2020). Beyond these technical and legal concerns, other issues such as a lack of trust and transparency among stakeholders, traceability challenges, and professional liability also play a significant role in impeding adoption (Fakour & Poirier, 2024, 2025). Despite these obstacles, the inherent benefits of BIM—especially its capacity to enhance collaboration, facilitate data-driven decision-making, and advance digital transformation initiatives—underscore its strategic importance in modern infrastructure projects.

1.3.2 The necessity of authentication and data integrity in BIMs

Ensuring the authenticity and integrity of Building Information Models (BIMs) is essential for the success of BIM implementation, as it guarantees that the information exchanged remains reliable and unaltered throughout a project's life cycle. Authentication plays a pivotal role in establishing trust and transparency among stakeholders by preventing tampering and unauthorized modifications. When stakeholders can rely on the authenticity of BIM data, it not only supports effective collaboration but also mitigates risks associated with miscommunication and errors. Trustworthy BIMs foster a shared understanding of project data, which is crucial for seamless integration of inputs from various disciplines, thereby reducing the likelihood of costly mistakes and design discrepancies (Hijazi, Perera, Al-Ashwal & Neves Calheiros, 2019; Hijazi *et al.*, 2021; Fakour & Poirier, 2025).

Beyond building trust, authentication significantly enhances traceability by enabling the continuous tracking of changes and modifications over time. This traceability is vital for ensuring accountability and auditability, which in turn helps resolve legal disputes and manage professional liability. With a robust authentication system in place, every alteration in the BIM can be traced back to its source, ensuring that any error or discrepancy can be quickly identified and rectified (Hijazi *et al.*, 2019, 2021; Pradeep, Amor & Yiu, 2020). Such a system not only reinforces the model's reliability but also underpins the legal frameworks that govern intellectual property and data ownership.

In addition to traceability, maintaining the data integrity of BIMs is critical for promoting interoperability. A secure and authentic BIM facilitates seamless data exchange between various software applications and among diverse project stakeholders, ensuring that all parties are working with the most accurate and up-to-date information. Robust authentication and data integrity verification measures help detect unauthorized modifications that might undermine the model's accuracy, thus ensuring that the data remains dependable for decision-making processes (Abd Jamil & Fathi, 2020; Mohammadi *et al.*, 2024).

Moreover, reliable authentication is paramount as it relates to professional liability as it ensures that every contribution to the BIM is clearly documented and attributed to its creator. This clear record of contributions reduces the risk of disputes and legal issues by providing transparent evidence of responsibility. It also helps protect the ownership and intellectual property rights of all contributors, thereby ensuring that legal agreements are adhered to and that the rights of each stakeholder are safeguarded (Abd Jamil & Fathi, 2020; Azhar *et al.*, 2008; Chong & Cheng, 2023).

Collectively, these considerations underscore the necessity of embedding robust authentication mechanisms within BIMs. By integrating advanced security measures, such as digital signatures, into BIM processes, the construction industry can achieve a higher level of data integrity. This not only enhances trust and collaboration among stakeholders but also drives digital transformation and supports efficient project delivery. The importance of these practices is well documented in the literature, highlighting their critical role in ensuring the success of building asset projects.

1.3.3 Current authentication practices for BIMs and their limitations

Current authentication practices in BIM—as well as in other industries that exchange 3D or data-enriched models, such as manufacturing and aerospace—predominantly rely on securing data by encapsulating digital models within memorandum files. This often involves converting models to 2D PDF documents or creating a cover document that aggregates a list of files and their attachments within a container, which is then digitally signed, as specified by standards

such as ARINC827-1 (Electronic Distribution of Software by Crate) (ARINC827-1, 2020), ARINC835-1 (Guidance for Security of Loadable Software Parts Using Digital Signatures) (ARINC835-1, 2014), ISO 21597-1:2020 (ISO21597-1:2020, 2020), and PDF/A-3 (PDF/A-3, 2020) (based on ISO 32000-1 (ISO32000-1:2008, 2008)). Additionally, Common Data Environments (CDEs) (ISO19650-1, 2018) act as centralized repositories that store project files and facilitate collaborative workflows through mechanisms such as access control, versioning, and auditing. These approaches generally apply digital signatures at the file or container level, thus verifying the integrity of the container as a whole, even though individual files within may not be examined separately.

Other solutions based on blockchain techniques have garnered increasing attention for their potential to enhance transparency, traceability, and non-repudiation by offering a tamper-proof ecosystem for secure data exchange. For instance, BIMCHAIN (Bimchain, 2018; Pradeep *et al.*, 2020) is a blockchain-based application that enables multi-signature, time-stamped data exchanges for BIM models. While such methods can detect modifications to entire files, they face inherent challenges in complex construction environments. These challenges include increased implementation complexity, difficulties in ensuring long-term archival and retrieval over the extended life cycles of built asset projects, and a lack of proper legal regulation (Li & Kassem, 2021).

Despite the clear benefits provided by these authentication practices—including the ability to verify data origin and maintain trust—they encounter limitations in their application to complex built asset project considering their long-term life cycle. The predominant use of file-based verification methods means that, while the integrity of the overall container can be confirmed, unauthorized changes to the individual contents may go undetected.

1.3.4 OpenBIM

OpenBIM is a universal approach that fosters collaborative design, construction, and operation of buildings through the utilization of open standards and workflows (Gomez & Gomez,

2017). By enhancing interoperability between various software platforms, OpenBIM diminishes collaborative errors and ensures the precision of multi-party collaborations, thereby boosting overall project efficiency (Gomez & Gomez, 2017; Jiang, Jiang, Han, Wu & Wang, 2019). BuildingSMART International (bSI) is at the forefront of advocating for and implementing open, international standards and solutions tailored for infrastructure and buildings, with the goal of propelling the digital transformation of the built asset industry (Jiang *et al.*, 2019; buildingSMART, 2024).

OpenBIM is a management process that enhances the benefits of BIM for collaborative projects by ensuring digital data is accessible, well-managed, and sustainable (Ciccone, Di Stasio, Asprone, Salzano & Nicolella, 2022). It streamlines interoperability among project participants throughout the project life cycle, which is essential for the digital transformation of the construction sector (Ciccone *et al.*, 2022). This is facilitated through the use of open standards such as Industry Foundation Classes (IFC), which allows for flexible software choices (Ciccone *et al.*, 2022). OpenBIM enables efficient data exchange and promotes collaboration across different platforms and among various stakeholders, giving users the flexibility to define their workflows (openBIM-bSI, 2025).

The core principles of OpenBIM include:

- Interoperability: OpenBIM ensures interoperability among different entities involved in a project's life cycle, which is essential for advancing digital transformation within the built asset industry (Jiang *et al.*, 2019; Ciccone *et al.*, 2022; Gomez & Gomez, 2017).
- Accessibility: It enhances the advantages of BIM by facilitating the accessibility, effective management, and sustainability of digital data (Jiang *et al.*, 2019; Ciccone *et al.*, 2022).
- Collaboration: OpenBIM facilitates smooth data exchange and collaborative work among various platforms and project stakeholders (Jiang *et al.*, 2019; Ciccone *et al.*, 2022).
- Flexibility: It empowers users to maintain full flexibility in defining their own workflows (Jiang *et al.*, 2019; Ciccone *et al.*, 2022).

- Vendor-neutrality: OpenBIM is an open and neutral way to improve work, allowing users to choose their own path and follow their digital destiny (Jiang *et al.*, 2019; Ciccone *et al.*, 2022).

1.3.5 buildingSMART International standards and services

bSI offers a comprehensive suite of open standards and technical services that underpin collaborative digital practices across the built asset industry. Among its core offerings are the Industry Foundation Classes (IFC), Model View Definitions (MVD), Information Delivery Manuals (IDM), the Information Delivery Specification (IDS), the BIM Collaboration Format (BCF), the buildingSMART Data Dictionary (bSDD), and the Use Case Management Service (UCM). In this research, we concentrate specifically on IFC and MVD, as they are most pertinent to our objectives and findings. Consequently, while references are made to the broader range of buildingSMART resources, such as IDM, IDS, BCF, bSDD, and UCM, they are not discussed in detail.

1.3.5.1 IFC

The Industry Foundation Classes (IFC) constitute a standardized digital framework for describing the built environment—encompassing both buildings and civil infrastructure (bSI, 2024d). Recognized as an open, international standard under ISO 16739-1:2024, IFC is designed to be vendor-neutral and applicable across various hardware devices, software platforms, and interfaces for an array of use cases (bSI, 2024d). The IFC schema specification is the primary technical deliverable from bSI in support of its mission to advance openBIM (bSI, 2024d).

IFC's development can be traced back to 1995, when work on the standard first began (van Berlo *et al.*, 2021). At that time, many now-prevalent data modeling and exchange frameworks—such as UML, XML, or JSON—either did not exist or were still in nascent stages (van Berlo *et al.*, 2021). Consequently, IFC was built around EXPRESS for defining data schemas, alongside the STEP Physical File (SPF) format for file-based exchanges (van Berlo *et al.*, 2021). In 2013, the

International Organization for Standardization (ISO) granted formal certification to IFC (Won, Kim, Yu & Choo, 2022). To date, IFC 2×3 remains the most established and widely adopted version within the industry (Gao, Lu & Fung, 2024). Meanwhile, the latest release, IFC 4x3, broadens the schema to include railways, highways, ports, and waterways, and introduces both dynamic and static expansions that specifically address the needs of railway engineering (Zheng, Shi & Wang, 2024).

The IFC schema is conceptually divided into four layers—domain, interoperability, core, and resource layers—each serving a distinct purpose (Yu, Kim, Jeon & Koo, 2023c):

- The domain layer Comprises schemas specific to particular disciplines—such as architecture, structural engineering, or facility management—and includes specialized entity definitions tailored to those fields (Yu *et al.*, 2023c).
- The interoperability layer Offers schemas that define entities shared across multiple disciplines, providing a common foundation for cross-domain interactions (Yu *et al.*, 2023c).
- The core layer Encompasses both the kernel schema, which establishes the broadest and most abstract concepts, and the core extension schemas, which generalize entity definitions common to multiple domains (Yu *et al.*, 2023c).
- Contains all resource definitions, serving as the fundamental building blocks of the IFC data model (Yu *et al.*, 2023c).

The most widely used method for exchanging IFC data today involves storing it in a file with the extension ".ifc," referred to as IFC-SPF. The acronym SPF stands for STEP Physical File, as defined by ISO 10303-21 (Sun, Liu, Gao & Han, 2015). This physical file format functions as a direct medium for information transfer among BIM platforms (Zheng *et al.*, 2024). Additionally, IFC supports the exchange of various building element data through alternative formats—including ifcXML, ifcZIP, COBie, gbXML, and LandXML—ensuring that a consistent, up-to-date version of the information is shared across different systems (Gao *et al.*, 2024).

An IFC-SPF file is organized into two main sections: a header and a data section. The header portion, demarcated by HEADER and ENDSEC, provides fundamental IFC file information—like "file description and schema version" (Du, Gu, Yang & Yang, 2020). The data portion, beginning with DATA and concluding with ENDSEC, contains multiple data instances that describe the model. Each instance commences with a number sign (#) and finishes with a semicolon (;), typically encompassing four components: an ID number, an entity name, a set of attribute values, and corresponding reference IDs (Du *et al.*, 2020).

Utilizing IFC poses several challenges. Files produced by different systems often include significant redundant information, which constrains IFC-based storage, exchange, management, and transmission of data (Sun *et al.*, 2015). A main obstacle is employing IFC as an exchange standard in large projects (Sun *et al.*, 2015). Specific technical issues encountered in IFC-based data exchange include inaccuracies in geometric representations, loss of object information, confusion arising from multidisciplinary revisions, application-specific IFC import and export workflows, and the issue of large file sizes (Sun *et al.*, 2015). Although new entities have been added to the IFC schema through continuous version updates, its coverage remains bounded to certain domains (Yu *et al.*, 2023c).

1.3.5.2 Model View Definitions (MVD)

A MVD can be understood as a defined implementation level of the IFC schema, strategically designed to support specific information exchange requirements within the built asset industry (bSI, 2024f; Chipman, Liebich & Thomas, 2016; ISO16739-1:2024, 2024). Essentially, an MVD specifies a subset of the comprehensive IFC schema that is deemed necessary to fulfill the data needs of a particular workflow or exchange scenario (Chipman *et al.*, 2016; Yu *et al.*, 2023c).

The IFC schema is inherently versatile, capable of representing building information at varying levels of detail and encompassing diverse aspects such as geometry, properties, and relationships (bSI, 2024f). MVDs serve to constrain this broad schema, identifying the relevant IFC entities,

attributes, and relationships that are pertinent to a specific information exchange, thereby enhancing the efficiency and interoperability of BIM data (Yu *et al.*, 2023c; Chipman *et al.*, 2016).

The concept of MVDs emerged to address the practical challenges of utilizing the extensive IFC schema. Initially, the creation of MVDs was largely ad-hoc, with individual parties developing their own definitions. This proliferation of non-interoperable MVDs created complexities and necessitated additional efforts for software vendors to implement and support them (bSI, 2024f). Software supporting one MVD, such as the Reference View, could not automatically support others, such as the Precast MVD, highlighting the need for standardization (bSI, 2024f). bSI has played a pivotal role in formalizing and standardizing the development and exchange of MVDs. A significant milestone in this process was the development of mvdXML, a standardized XML-based format for specifying and exchanging MVDs along with their associated Exchange Requirements and validation rules (Chipman *et al.*, 2016; Jaud & Clemen, 2024; Jiang *et al.*, 2019).

1.3.6 Authentication definition and techniques

Authentication is the process of conforming the identity of an entity (Mulder *et al.*, 2023; Patiyoot, 2024). As defined by ISO/IEC27000 (2018), authentication provides "assurance that a claimed characteristic of an entity is correct". This involves confirming that a user, device, or process is indeed who or what it claims to be prior to granting access to a system or resource (Velásquez, Caro & Rodríguez, 2018; Patiyoot, 2022, 2024). Authentication is often the first line of defense in computer security and is fundamental for access control and user accountability (Velásquez *et al.*, 2018; Patiyoot, 2022; Stallings & Brown, 2015). In fact, this process is distinct from authorization, which governs permissions post-verification, and is critical for enforcing security policies and preventing unauthorized access (Stallings & Brown, 2015).

Stallings & Brown (2015) and other resources in literature categorize authentication into four general means as individual's identity, often referred to as authentication factors, which serve as the basis for common techniques:

1. Something the individual knows (Stallings & Brown, 2015; Grassi, Garcia & Fenton, 2017; Mulder *et al.*, 2023; Velásquez *et al.*, 2018): This includes information that a user remembers, such as passwords, personal identification numbers (PINs), or answers to security questions (Stallings & Brown, 2015; Grassi *et al.*, 2017; Arutyunov, 2012). Password-based authentication, the most prevalent technique, falls under this category. While simple, its reliance on user-secrets makes it vulnerable to compromise (Stallings & Brown, 2015).
2. Something the individual possesses (Stallings & Brown, 2015; Grassi *et al.*, 2017; Mulder *et al.*, 2023; Velásquez *et al.*, 2018): This refers to physical or digital items that the user owns which are often called tokens, such as electronic key cards, smart cards, physical keys, hardware tokens, mobile devices, or software-generated one-time passwords (OTPs) (Velásquez *et al.*, 2018; Stallings & Brown, 2015; Grassi *et al.*, 2017). Token-based authentication methods, including time-based OTPs (TOTPs), align with this means, offering dynamic credentials that mitigate static password risks (Grassi *et al.*, 2017).
3. Something the individual is (Mulder *et al.*, 2023; Velásquez *et al.*, 2018; Grassi *et al.*, 2017; Stallings & Brown, 2015): This involves biometric data that is unique to the user, such as fingerprints, facial features, iris patterns, voice patterns, or other physiological traits (Velásquez *et al.*, 2018; Grassi *et al.*, 2017; Stallings & Brown, 2015; Arutyunov, 2012; van Oorschot, 2020). Biometric authentication systems validate identity using unique physiological or behavioral traits, though challenges such as spoofing and privacy concerns persist (Jain, Ross & Prabhakar, 2004; Stallings & Brown, 2015).
4. Somewhere the individual is (Mulder *et al.*, 2023; van Oorschot, 2020): This refers to the location and/or time of the entity's login, such as GPS coordinates, IP address, or cellular triangulation (Mulder *et al.*, 2023). While less common, it is increasingly used in adaptive authentication systems to flag suspicious logins from unexpected region (Grassi *et al.*, 2017).

Here are some common authentication techniques, categorized by the authentication factor they use:

- Password-Based Authentication (PBA): It uses Something you know as authentication factor (Shah, Fazl-e-Hadi & Minhas, 2009). PBA is a common authentication method where users provide a username and password to gain access (Patiyoot, 2024; Stallings & Brown, 2015; Sridhar & Mamatha, 2021; Ariffin, Abdulhalem & Husin, 2021). The system compares the provided password against a stored password hash to authenticate the user (Stallings & Brown, 2015). PBA provides straightforward implementation but can be vulnerable to attacks such as guessing, dictionary attacks, and phishing (Gupta, 2017; Jain *et al.*, 2004; Ariffin *et al.*, 2021; Grivei, 2015). To enhance security, hashed passwords and salting techniques are often employed (Stallings & Brown, 2015).
- Multi-Factor Authentication (MFA): It uses A combination of two or more factors from the categories of knowledge, possession, and inherence as authentication factor (Velásquez *et al.*, 2018; Grassi *et al.*, 2017; Shah *et al.*, 2009; van Oorschot, 2020). MFA strengthens security by mandating that users present several forms of verification (Grassi *et al.*, 2017; Velásquez *et al.*, 2018). For instance, a user may be required to input a password (something they know) and provide a one-time code generated on their mobile device (something they have) (Grassi *et al.*, 2017; van Oorschot, 2020). MFA is more robust against attacks as compromising one factor alone is insufficient, the attacker still needs to bypass the other factors (Velásquez *et al.*, 2018).
- Biometric Authentication: It uses Something you are (inherence factor) as authentication factor(Velásquez *et al.*, 2018; Grassi *et al.*, 2017; Stallings & Brown, 2015; van Oorschot, 2020). This method uses distinct physical or behavioral characteristics to verify a user's identity (Stallings & Brown, 2015; Arutyunov, 2012; van Oorschot, 2020; Grivei, 2015). Widely used biometric techniques encompass fingerprint identification, facial recognition, iris scanning, and voice authentication(Stallings & Brown, 2015; Arutyunov, 2012; van Oorschot, 2020). Biometric authentication provides enhanced security over conventional password-based methods, as biometric characteristics are inherently challenging to replicate or compromise (Arutyunov, 2012; Ju, Seo, Han, Ryou & Kwak, 2013; van Oorschot, 2020).

- Token-Based Authentication: It uses Something you have (possession factor) as authentication factor(Velásquez *et al.*, 2018; Stallings & Brown, 2015; Grassi *et al.*, 2017; van Oorschot, 2020). Token-based authentication uses physical or digital tokens to verify a user's identity (Stallings & Brown, 2015; van Oorschot, 2020; Arutyunov, 2012). Physical tokens include smart cards, USB keys, and hardware tokens that generate OTPs(Stallings & Brown, 2015; van Oorschot, 2020; Arutyunov, 2012; Guennoun, Abbad, Talom, Rahman & El-Khatib, 2009). Digital tokens can include software-based authenticators on mobile devices (Stallings & Brown, 2015; van Oorschot, 2020). When users initiate a login attempt, they must present the correct token to gain access (Stallings & Brown, 2015).
- Certificate-Based Authentication: It uses Something you have (possession factor) as authentication factor. Certificate-based authentication employs digital certificates to authenticate the identities of users, devices, or applications (Ariffin *et al.*, 2021; van Oorschot, 2020; Arutyunov, 2012). A digital certificate is an electronic document that verifies the ownership of a public key (Arutyunov, 2012). Digital certificates could be issued by trusted Certificate Authorities (CAs) under various standards or protocols such as X.509 standard. These certificates bind an entity's identity to a cryptographic key pair, enabling secure authentication in protocols suach as Secure Sockets Layer (SSL)/Transport Layer Security (TSL) for web servers. The process ensures that only entities with valid certificates can establish trusted connections (Stallings & Brown, 2015) .During authentication, the client presents its digital certificate to the server, which verifies the certificate's validity and then grants access (Arutyunov, 2012).
- Single Sign-On (SSO): It typically relies on a combination of knowledge, possession, and/or inherence factors, depending on the specific implementation. SSO enables individuals to log in once and gain access to various applications and services using the same authentication credentials (Yun, Chao, Haoling, Tao & Hefang, 2022). When a user logs into one application, the SSO system authenticates the user and then automatically grants access to other authorized applications without requiring the user to re-enter their credentials (Yun *et al.*, 2022). SSO simplifies the login process and improves user experience, but it also requires a centralized authentication system that can be a single point of failure (Yun *et al.*, 2022).

- Adaptive Authentication: Adaptive authentication considers contextual factors such as device location or the sensitivity of the data being requested to determine the authentication procedure (Mulder *et al.*, 2023). This method enhances security and usability by adjusting the authentication requirements based on the context of the login attempt (Mulder *et al.*, 2023). It calculates a risk score and determines the necessary security measures, using factors such as location and data sensitivity (Mulder *et al.*, 2023).
- Continuous Authentication: It Continuous authentication constantly monitors the user's behavior or biometric data after the initial login to ensure that the user remains the same throughout the session (Mulder *et al.*, 2023; Guennoun *et al.*, 2009). This approach addresses the vulnerabilities of traditional authentication systems by continuously verifying the user's identity (Mulder *et al.*, 2023; Guennoun *et al.*, 2009). It uses methods such as behavioral biometrics (e.g., keystroke dynamics, mouse patterns) or physiological biometrics (e.g., electrocardiogram data) to ensure ongoing authentication (van Oorschot, 2020; Guennoun *et al.*, 2009).
- Formula-Based Authentication (FBA): It uses Something you process, in combination with something you know as authentication factor (Shah *et al.*, 2009). FBA involves users recalling a mathematical formula (password) and computing the result upon each login (Shah *et al.*, 2009). This method enhances security by requiring both memory and processing ability, making it resistant to shoulder surfing attacks (Shah *et al.*, 2009).

1.3.7 Data integrity and its verification techniques

Data integrity refers to the maintenance and assurance of data accuracy, consistency, and reliability throughout its life cycle, including creation, processing, storage, and transmission (ISO/IEC2501, 2008). It ensures data is unaltered except by authorized actions and remains intact against corruption or unauthorized modifications. A loss of data integrity can result in data unavailability and other security issues. Therefore, maintaining data integrity is crucial for building trust in information systems and ensuring reliability in decision-making processes. Key characteristics of data integrity include:

- Accuracy: Data is correct, reliable, and certified free of error. Accuracy ensures that the information reflects the true state of what it represents, which is vital for making informed decisions (FDA, 2018; Batini & Scannapieca, 2006; ISO/IEC2501, 2008).
- Completeness: All required data elements are included. Without completeness, the information might be misleading or insufficient for its intended purpose (FDA, 2018; Batini & Scannapieca, 2006).
- Consistency: Data is coherent and reliable across systems. Consistency ensures that the same data is represented uniformly across different databases and applications (FDA, 2018; Batini & Scannapieca, 2006).
- Currency: Data is up-to-date. Timeliness of data is essential, especially in dynamic environments where decisions depend on the latest available information (Batini & Scannapieca, 2006).
- Traceability: The relationships between data and their metadata should be preserved in a secure and traceable manner. Traceability allows for auditing and verification of data, ensuring accountability and transparency (FDA, 2018).

The ALCOA principles outline fundamental requirements for data integrity, specifying that records must be Attributable, Legible, Contemporaneous, Original, and Accurate (Girard & Watkin, 2021). Originally developed as a framework for best practices in life science data management, ALCOA has been endorsed by multiple advisory and regulatory bodies (Girard & Watkin, 2021). For example, the U.S. Food and Drug Administration (FDA), European Medicines Agency (EMA), and International Society for Pharmacoepidemiology (ISPE) have each released guidance centered on data integrity, while the Pharmaceutical Inspection Co-operation Scheme (PIC/S) and the World Health Organization (WHO) have drafted additional guidelines in alignment with ALCOA (Girard & Watkin, 2021). The ALCOA principles include:

- Attributable: Activities are documented and can be traced to a specific individual (FDA, 2018; Girard & Watkin, 2021). This principle ensures that all data modifications and operations can be attributed to a responsible party, promoting accountability (FDA, 2018).

- Legible: Records are clear and readable (FDA, 2018; Girard & Watkin, 2021). Legibility ensures that data is easily understood and accessible for review and verification (FDA, 2018).
- Contemporaneous: Activities are documented at the time of performance (FDA, 2018; Girard & Watkin, 2021). Documenting activities in real-time reduces the risk of errors and omissions, providing an accurate record of events (FDA, 2018).
- Original: Data is the original source or a true copy (FDA, 2018; Girard & Watkin, 2021). Maintaining the originality of data ensures its authenticity and reliability for decision-making (FDA, 2018; Girard & Watkin, 2021).
- Accurate: Data is correct, reliable, and free of errors (FDA, 2018; Girard & Watkin, 2021). Accuracy is fundamental to data integrity, ensuring that information is trustworthy and dependable (FDA, 2018; Batini & Scannapieca, 2006).

ALCOA+ recommends that data is also Complete, Consistent, Enduring, and Available (Girard & Watkin, 2021). This extends the original ALCOA principles to ensure more robust data management (Girard & Watkin, 2021).

- Complete: All data elements, including metadata, are included to reconstruct events (FDA, 2018; Girard & Watkin, 2021).
- Consistent: Data is coherent and reliable across all records and applications (Girard & Watkin, 2021; Batini & Scannapieca, 2006).
- Enduring: Data is maintained securely throughout the record's retention period (FDA, 2018; Girard & Watkin, 2021).
- Available: Data is accessible when needed for review and reporting (Girard & Watkin, 2021).

To meet the principles, it is important to capture complete and consistent data, including metadata such as process values, batch details, history, and audit trails, all stored together FDA (2018); Girard & Watkin (2021). Elements of analysis should be date/time stamped and in the expected sequence, including deviations and changes made FDA (2018); Girard & Watkin (2021). This holistic approach ensures that data is not only accurate but also fully contextualized and auditable (FDA, 2018).

To ensure data integrity, various techniques are employed. These techniques help detect and prevent data corruption, unauthorized modifications, and other integrity violations (Chauhan, Jain & Pandey, 2022). common Methods include:

- Digital Signature Algorithms (DSA): Mathematical techniques used to validate the authenticity and integrity of digital data (Chauhan *et al.*, 2022; Stallings & Brown, 2015). Digital signatures ensure that sensitive information is signed by the actual sender and verified by the recipient (Chauhan *et al.*, 2022; Stallings & Brown, 2015). They are used to achieve authentication, non-repudiation, and integrity over digital data (Chauhan *et al.*, 2022; Stallings & Brown, 2015). Digital signatures employ asymmetric cryptography to authenticate data origin and integrity. A sender uses a private key to generate a signature, which is verified using the corresponding public key (Chen, Moody, Regenscheid & Robinson, 2023).
- Merkle Hash Trees: This technique is widely used in distributed systems and cryptocurrencies to verify the integrity and authenticity of data (Chauhan *et al.*, 2022). It ensures that data is not accidentally or maliciously tampered with, deleted, or corrupted during storage, transmission, and processing (Chauhan *et al.*, 2022). The transaction information in systems such as Bitcoin is verified using Merkle Hash Trees. Each block comprises multiple transactions, the block index, previous block's hash value, a timestamp, the current block's hash, and a nonce (Perera, Nanayakkara, Rodrigo, Senaratne & Weinand, 2020). Any modification to a block within the chain will instantly alter its corresponding hash value (Perera *et al.*, 2020).
- Blockchain-Based Decentralization: This involves utilizing decentralized data storage and verification techniques (Yu, Zhang, Yu & He, 2023b). Blockchain helps achieve trusted verification without relying on third parties (Yu *et al.*, 2023b). The immutability and transparency of blockchain technology make it well-suited for ensuring data integrity in distributed systems (Yu *et al.*, 2023b). Blockchain technology divides data into blocks and links these blocks together to form a chain. Each block contains information and a hash value associated with the information in that block and the previous block.
- Smart Contracts: These refer to agreements that are executed automatically based on business rules programmed within blockchain code (Vadgama, 2019). The execution of actions via smart contracts is upheld by the members of the network (Vadgama, 2019). Smart contracts

rely on the immutability of blockchain to ensure data integrity and prevent tampering (Huang, Bian, Li, Zhao & Shi, 2019; Li & Kassem, 2021). They can be used to update information models, automate compensation events, and streamline contract administration, facilitating the linking of physical and digital worlds (Li & Kassem, 2021).

1.3.8 Synergy between authentication and data integrity

The interplay between authentication and data integrity is foundational to modern information security frameworks, as both concepts mutually reinforce trustworthiness in data and identity management.

Authentication mechanisms validate the legitimacy of entities interacting with systems, while data integrity ensures the reliability of the information those entities access or modify. For instance, authentication factors such as biometrics (something the user is) inherently support data integrity principles such as attributability by linking actions to verified identities, thereby ensuring accountability in audit trails (FDA, 2018; Grassi *et al.*, 2017). Similarly, cryptographic techniques such as digital signatures—rooted in asymmetric authentication—simultaneously authenticate users and safeguard data integrity by detecting unauthorized alterations (Chen *et al.*, 2023; Stallings & Brown, 2015). Blockchain technology exemplifies this synergy by integrating decentralized authentication (via consensus mechanisms) with Merkle trees to ensure immutable, tamper-evident records, thereby satisfying ALCOA+ principles such as originality and endurance (Yu *et al.*, 2023b; Perera *et al.*, 2020).

Adaptive authentication further enhances data integrity by dynamically adjusting security protocols based on contextual risks (e.g., geolocation anomalies), reducing opportunities for unauthorized data manipulation (Mulder *et al.*, 2023). Multi-factor authentication (MFA) strengthens this relationship by layering verification methods (e.g., passwords + tokens), which mitigates risks of compromised credentials that could otherwise corrupt data (Velásquez *et al.*, 2018). Conversely, data integrity verification methods such as Merkle proofs and smart contracts rely on authenticated identities to enforce tamper-resistant workflows, ensuring only authorized

entities can alter data (Huang *et al.*, 2019; Chauhan *et al.*, 2022). Thus, the interdependence of authentication and data integrity creates a cohesive security posture where identity assurance and data reliability are mutually reinforcing, critical for compliance in regulated sectors (Girard & Watkin, 2021; ISO/IEC2501, 2008).

The Table 1.1 compares data integrity verification methods, focusing on their interplay with authentication concepts, implementation and maintenance considerations, regulatory alignment, and distinctive advantages.

Table 1.1 Comparison of data integrity verification methods

Method	**Authentication Method**	**Authentication Factor**	**Implementation (Cost/Complexity)**	**Maintenance (Cost/Complexity)**	**Legal Acceptance**
Digital Signatures	Certificate-Based Authentication	Something you have (possession factor)	Low	Moderate	Widely accepted
Merkle Trees	Not inherently tied to authentication	N/A	Low	Moderate	Industry-specific (e.g., blockchain)
Blockchain	Consensus mechanisms (e.g., Proof of Work/Proof of Stake)	Cryptographic keys (possession factor)	High (network infrastructure)	High	Evolving
Smart Contracts	Decentralized identity	Something you have (possession factor)	High (coding, auditing)	High	Evolving

1.4 Problem statement

The contemporary built asset industry is witnessing a rapid digital transformation, largely driven by the increasing adoption of BIM. Serving as a centralized model enriched with data that captures both the physical attributes and operational features of a facility, BIM greatly enhances collaboration, information exchange, and decision-making throughout project life cycles. Its potential is further amplified by the Industry Foundation Classes (IFC), an open standard developed by buildingSMART to enable data exchange and interoperability across a wide spectrum of software platforms. By eliminating format incompatibility issues, IFC encourages seamless sharing of BIM content among stakeholders, thereby reducing errors and inefficiencies in construction workflows.

Yet, BIM's digital nature introduces significant challenges related to data integrity and authentication. Ensuring that BIM models remain both unaltered and verifiably sourced is critical for preserving stakeholder trust and preventing costly disputes or project delays. In practice, today's authentication methods commonly focus on validating or digitally signing 2D deliverables. Although data-rich 3D BIM models are increasingly prevalent, the authentication process often relies on memorandums or wrappers that bundle various files together—an approach typically limited to the package level or file level. Such methods lack the fine-grained control needed to authenticate individual objects and their associated data, leaving BIM models vulnerable to unauthorized modifications, data inconsistencies, and uncertainty regarding professional liability and intellectual property rights.

To address these shortfalls, more granular authentication processes that function at the object level are needed. Digital signatures are already widely used for electronic documents and provide robust data integrity verification, but implementing them for object-level elements in BIM remains comparatively underexplored.

Hence, a critical problem persists in the lack of an effective method to authenticate BIM data at the object level. Current file-level authentication schemes fail to ensure the authenticity and integrity of each discrete model object, undermining accountability, regulatory compliance, and risk management. The ramifications include possible design flaws, construction errors, and legal entanglements, all of which jeopardize project success. To resolve these risks, this research proposes a comprehensive framework for embedding digital signatures in IFC-based BIM, enabling fine-grained authentication.

1.5 Research questions and contributions

Building on the problem statement, this section defines three core research questions aimed at addressing the limitations in current authentication practices for data-enriched models in the built asset industry. These questions collectively form the logical pathway to demonstrate why a more granular authentication mechanism is needed, what characteristics an effective solution

should possess, and how to realize such a solution in practice. They also serve as the basis for defining specific objectives and expected contributions, helping to ensure the research is both methodically sound and practically relevant.

Research Question 1: Why is object-level authentication and data integrity verification of data-enriched models necessary in the built asset industry?

This first question stems directly from the observed reliance on file-level verification and associated vulnerabilities. Data-enriched models often contain multiple specialized objects, each carrying critical information for design, construction, and maintenance. The inability to authenticate these components individually has led to persistent issues such as unauthorized modifications, data inconsistencies, and lack of accountability when errors occur. As the industry becomes increasingly reliant on digital collaboration, such gaps pose substantial risks, including legal disputes, professional liability concerns, and intellectual property conflicts. By asking why object-level authentication is required, the research seeks to identify and articulate the underlying needs that surpass the limitations of existing file-centric methods. Recognizing the necessity of object-level authentication clarifies the broader context: until stakeholders can securely verify individual parts of a complex model, the data remains at risk of alteration, compromise, or confusion regarding provenance.

Research Objective 1: To identify the purposes for implementing object-level authentication in data-enriched models.

Contribution of Research Objective 1:

- In Practice: Helps decision-makers grasp the concrete benefits of moving beyond file-level verification, potentially spurring investment in more granular authentication methods and tools.
- In theory: Offers a focused rationale by synthesizing literature and field challenges, thereby laying the groundwork for subsequent inquiry into the characteristics of an optimal solution.

Research Question 2: What are the essential functionalities of an ideal solution for object-level authentication and data integrity verification of data-enriched geometric models in the built asset industry?

Having established why object-level authentication is necessary, the next logical question is what functionalities such a solution should encompass. Current digital workflows in the built asset industry demand a tool set that can verify authenticity while preserving or even enhancing existing collaboration methods. This question prompts an exploration of interoperability with various authoring software, the capacity to detect tampering at a granular level, scalability for complex projects, and user-friendliness to encourage broad adoption. Further, the solution must account for legal considerations, ensuring alignment with industry regulations and providing a robust audit trail. By identifying these essential features, the research offers stakeholders and developers a blueprint for evaluating or creating effective authentication mechanisms.

Research Objective 2:To identify the functionalities that represent an ideal solution for object-level authentication and data integrity verification of data-enriched geometric models in the built asset industry.

Contribution of Research Objective 2:

- In Practice: Supplies clear design criteria that development teams can reference when selecting or building authentication solutions.
- In theory: Consolidates diverse needs into a structured framework, guiding future research on comparing or improving authentication solutions in built asset industry.

Research Question 3: How can object-level authentication and data integrity verification be effectively implemented within data-enriched geometric models?

Finally, having established the necessity and outlined the essential functionalities, the research now focuses on how to structure and implement the solution in practice. This phase involves determining which authentication and data integrity verification techniques can suitably address the highlighted requirements, while acknowledging technical and operational

complexities—ranging from designing a solution without excessive overhead to maintaining compatibility with existing tools. Overcoming these obstacles necessitates a systematic framework that seamlessly integrates the chosen authentication and data integrity verification methods into the model with minimal disruption to current workflows.

Research Objective 3: Design and develop a framework that effectively integrates object-level authentication and data integrity verification into data-enriched models. This framework should address practical complexities such as minimizing overhead, ensuring compatibility with existing tools, and maintaining usability for diverse stakeholders.

Contribution of Research Objective 3:

- In Practice: This objective delivers an approach for implementing authentication and data integrity techniques at a granular level, enabling practitioners to adopt these solutions with minimal disruption to established workflows. It clarifies the design considerations—such as avoiding undue file bloat and ensuring interoperability—that help industry stakeholders integrate object-level safeguards into their models.
- In theory: By investigating the interplay between authentication requirements, data format structures, and everyday BIM processes, this objective advances current understandings of how to embed security mechanisms in data-intensive environments. It sheds light on the technical and operational trade-offs involved in deploying object-level authentication and data integrity verification, offering insights that can shape future standards and best practices in the built asset industry.

1.6 Research Scope

The research focuses on the development of a technical solution for integrating digital signatures at a granular level in IFC-based BIMs. It addresses the need to move beyond file-level verification, where complex, multidisciplinary projects often require more refined methods to attribute responsibility for specific model objects. By examining how digital signature information can be appended or embedded without altering typical BIM workflow and processes, the research

underscores a practical path to stronger authentication and data integrity verification. Emphasis is placed on ensuring that the framework aligns with widely used IFC standard and that it can be adopted with minimal workflow disruption, making it feasible for real-world industry application.

1.6.1 Research limitations

The design proposed for embedding signatures is modular enough to accommodate various cryptographic libraries and algorithms for hashing or decryption/encryption, so the research does not commit to a single cryptographic approach. It also does not specify which BIM objects must be signed, who should sign them, or how responsibilities should be allocated in a project's contractual framework; those choices are left to project stakeholders based on context. Moreover, the research does not explore every possible legal or regulatory outcome once a signature has been applied, and it does not address in detail the potential repercussions of a signature later becoming invalid for reasons such as subsequent model alterations. Instead, the focus remains on providing a flexible technical method for performing and verifying object-level authentication and data integrity verification, with users determining whether and how it meets specific legal or regulatory requirements.

The final solution introduced for practical performance reasons - particularly the size of the signed model - is not strictly at the level of individual objects, but rather at the level of collections or subgroups of objects. Although this approach substantially reduces file size and processing overhead relative to truly per-object signing, it offers less granular tamper detection and may not suffice for projects that require absolute verification of each object. Additionally, while the framework is shown to be conceptually and technically viable, it is not presented as a fully commercialized product; industry practitioners may need to adapt and refine it further before large-scale deployment in live production environments.

1.7 Design Science Research Methodology as research methodology

This research employs a Design Science Research Methodology (DSRM) approach. DSRM offers a robust and structured approach for conducting research that aims to create innovative artifacts to address real-world problems. Its strength lies in providing a clear and systematic framework that integrates principles, practices, and a well-defined process, thereby enhancing the rigor and relevance of design-oriented research and facilitating effective communication of research outcomes (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007; Hevner, March, Park & Ram, 2004).

DSRM can be defined as a "coherent system comprising principles, practices, and procedures" (Peffers *et al.*, 2007) specifically developed for undertaking design science research (DSR). This methodology synthesizes fundamental concepts that delineate DSR, practical guidelines for its implementation, and a structured process for conducting and reporting the research (Peffers *et al.*, 2007).

One of the major strengths of the DSRM approach lies in its iterative nature, facilitating continuous refinement of artifacts through multiple cycles of design, development, demonstration, and evaluation ((Peffers *et al.*, 2007). This iterative process supports progressive learning and improvement, enabling researchers to adapt their artifacts in response to emerging insights, practical constraints, stakeholder feedback, and environmental changes. Such an iterative approach is particularly beneficial in the context of this research, where developing a solution for object-level authentication and data integrity verification within data-enriched models inherently involves addressing complex technical and operational challenges that are likely to require multiple refinement cycles.

The DSRM approach involves the following key steps (Peffers *et al.*, 2007):

1. Problem Identification and Motivation: Articulate the research problem explicitly and and demonstrate the importance of resolving it.

2. Definition of the Objectives for a Solution: Clearly define the desired outcomes of the research. These objectives should be consistent with the problem and serve as evaluation criteria.
3. Design and Development: The creation of the artifact itself. The artifact can take various forms, including constructs, models, methods, or instantiations.
4. Demonstration: The artifact must be demonstrated in an appropriate context to show its feasibility and potential value.
5. Evaluation: Rigorously assess the utility, quality, and effectiveness of the designed artifact using suitable evaluation methods.
6. Communication: Effectively communicate the research findings to relevant audiences.

The overall DSRM process, as applied in this research, is illustrated in the figure 1.1. Each phase of this process and its detailed implementation within the research will be thoroughly discussed in the subsequent section.

1.7.1 Problem identification

The Problem Identification phase in Design Science Research Methodology (DSRM) serves as the foundational step to recognize, define, and contextualize a significant research challenge that warrants innovative solutions (Peffers *et al.*, 2007). This phase requires a systematic exploration of existing knowledge gaps, alignment with real-world needs, and validation through stakeholder engagement to ensure relevance and rigor (Hevner *et al.*, 2004).

The Problem Identification phase centers on defining and contextualizing a significant challenge through collaboration with stakeholders to establish a clear understanding of the issue. This involves synthesizing insights from both academic literature and practical domains to align the problem with existing knowledge gaps and real-world needs. A review of prior work is conducted to explore current practices, theoretical frameworks, and unresolved issues within the field, ensuring the problem is grounded in evidence and relevance. The significance of the challenge is further validated through empirical data or direct engagement with stakeholders,

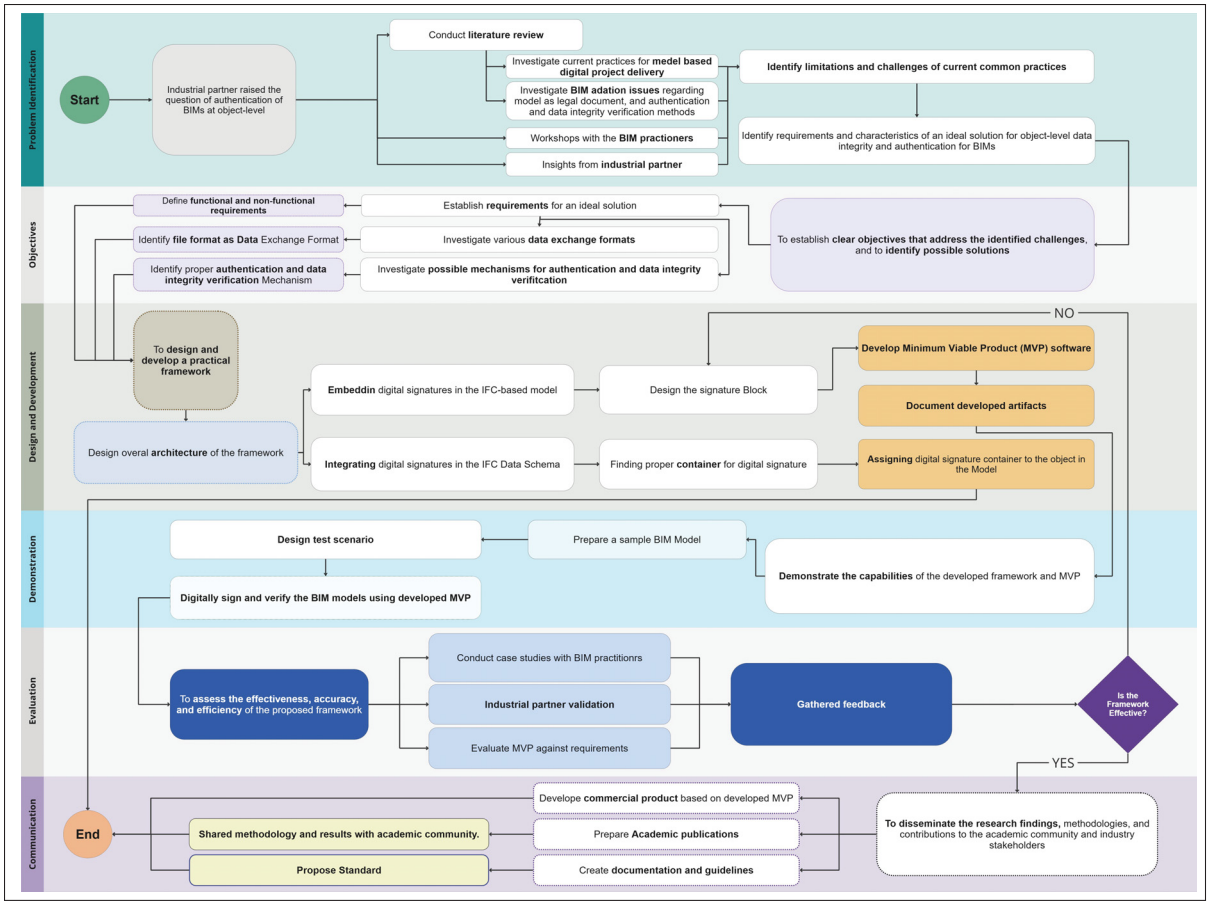

Figure 1.1 Overall applied DSRM process in the research

such as industry practitioners, to confirm its practical urgency and alignment with operational demands. This phase guarantees that the problem holds both academic originality and practical relevance within its intended application contexts.

The research problem emerged from an industrial partner's concern regarding the authentication of BIMs data at the object level, particularly in multi-stakeholder digital delivery workflows. To rigorously define the problem, the research started with a literature review across three domains: (1) current practices for model-based digital delivery, (2) BIM adaption issues particularly in legal and contractual aspects and (3) authentication and data integrity verification methods.

Collectively, these domains were selected to holistically address the technical, legal, and procedural dimensions of object-level authentication challenges. The synthesis of findings

revealed a critical gap: the absence of a comprehensive framework that integrates authentication and data verification at object-level with legal compliance and practical BIM workflows. This insight established the foundation for defining the research problem and guiding subsequent artifact design.

To align the industrial partner's concerns with practitioner needs, 9 semi-structured working meetings were conducted with BIM practitioners representing diverse roles and expertise as summarized in Table 1.2. Participants included representative from three U.S. Departments of Transportation, a BIM consultant, two BIM software developers, two academic experts specializing in OpenBIM and IFC standards, a buildingSMART International (bSI) technical expert, and two advisors from buildingSMART Canada, who contributed through regular project meetings. These working meetings were designed to triangulate insights from public infrastructure agencies, software developers, standards bodies, and academia, ensuring a comprehensive understanding of cross-sector challenges.

Table 1.2 Summary of working meetings participants and stakeholder representation

Stakeholder Group	**Participants**
Public Infrastructure Agencies	Representatives from three U.S. Departments of Transportation
Software Industry	Two BIM software developers
Consulting Sector	One independent BIM consultant
Academic Institutions	Two academic experts specializing in OpenBIM and IFC standards
Standards Organizations	One technical expert from buildingSMART International (bSI)
National Standards Committee	Two advisors from buildingSMART Canada, engaged through regular project meetings

The working meetings served three primary objectives: validating the practical relevance of object-level authentication challenges, identifying limitations in current workflows, and defining requirements for an ideal solution. Discussions revealed widespread recognition of vulnerabilities in data and model exchange, particularly. Practitioners highlighted recurring barriers, such as fragmented software interoperability, inconsistent audit trails which result in lack of trust

and transparency. Additionally, participants emphasized the need for solutions prioritizing scalability to accommodate large infrastructure projects, interoperability with existing tools, and compliance with evolving legal frameworks governing digital construction data.

The synthesis of working meetings findings and literature review confirmed that object-level authentication remains a critical yet inadequately addressed issue in BIM workflows. Key insights indicate a growing demand for decentralized, tamper-evident systems to enhance accountability in digital delivery processes. These outcomes crystallized the research problem and informed the subsequent design of a framework addressing technical, legal, and operational gaps in BIM data integrity.

1.7.2 Solution objectives

The Solution Objectives phase translates the challenges identified during problem validation into a focused set of objectives and actionable pathways for addressing object-level authentication and data integrity in collaborative BIM environments. The primary goal is to establish a technical framework that meets the dual demands of robust security and practical usability, without disrupting existing project workflows or business processes.

Central to this phase is the definition of functional and non-functional requirements for an ideal solution. Functional requirements emphasize enabling object-level authentication and ensuring data integrity verification while preserving interoperability. Non-functional requirements prioritize performance to accommodate large models, ease of maintenance over decades-long asset life cycle, and compliance with legal regulations and common processes standards.

To anchor the solution in industry practices, IFC format is selected as the data exchange format. As an open, ISO-standardized schema, IFC provides a vendor-neutral foundation that enhances interoperability across diverse BIM platforms. This choice directly addresses fragmented software interoperability—a key barrier identified in stakeholder working meetings.

The evaluation of authentication and data integrity verification mechanisms prioritizes digital signatures over alternatives such as blockchain. Digital signatures, are easy to implement and maintain, legally recognized under standards which ensures the solution remains viable across the decades-long life cycle of built assets.

1.7.3 Design and development

In this phase, the research focuses on designing and developing a practical framework for object-level authentication and data integrity verification. Initially, an overall architecture was proposed to conceptualize how digital signatures could be integrated into existing model-based workflows without disrupting widely used tools and formats. Two detailed design possibilities were then investigated.

First, a potential approach involved integrating digital signatures within the current IFC data schema by reusing existing entities rather than introducing new entities to avoid complexity of changing a established standard as well as consistency and compatibility with software tools. To accomplish this, required metadata for digital signatures were identified, followed by a mapping of those metadata to the IFC schema to find proper entity as digital signature container. Various candidate entities were examined in two major rounds to determine which ones could best accommodate the additional digital signature information and best candidate was identified.

The next challenge was determining an effective method for extracting subsets of the model associated with each object to be signed. Multiple techniques were considered—ranging from graph-theory-based graph traversal to leveraging MVDs or Information Delivery Specifications (IDS). Despite these explorations, the inherent complexity of IFC data schema including various types of relationships proved difficult to manage for robust object-level data exchange.

Consequently, the research opted for a second approach that does not directly depend on IFC's standardized data schema. Instead, the framework employs the optional sections in the ISO 10303-21 data exchange structure to embed digital signatures into the IFC files. An initial signature block design sought to authenticate and verify data integrity for each object. However,

this strategy produced a considerable increase in the overall file. To address this concern, the signature block was restructured to provide authentication and data integrity for collections of objects. This approach significantly reducing file size overhead while maintaining meaningful granularity.

This iterative design process underscores the phase's emphasis on practicality, ensuring the framework aligns with industry norms while addressing the technical and operational constraints identified in earlier research stages.

1.7.4 Demonstration

The Demonstration phase in DSRM validates the developed solution's functionality within realistic or representative settings, confirming its practical utility and alignment with research objectives. In this study, a standalone software tool was developed to embed and verify digital signatures within data-enriched BIMs. Designed with modular architecture, the tool operates independently while remaining adaptable for future integration into other tools.

To assess efficacy, the tool was tested using multiple IFC models simulating real-world scenarios. Each test involved digitally signing all objects in the model, followed by verification under two scenarios. In the first scenario, the signed model remained unaltered, and the tool confirmed the validity of all signatures, demonstrating its ability to authenticate data integrity when no unauthorized modifications were present. In the second scenario, deliberate tampering was done in the DATA section of the signed model. The tool successfully detected these unauthorized changes, flagging affected signatures as invalid.

The demonstration highlights the framework's technical feasibility, as signatures embedded in ISO 10303-21 optional sections preserved IFC data integrity without disrupting interoperability with existing software. By signing collections of objects, the tool balanced granular security with computational efficiency, addressing scalability concerns inherent to large models.

1.7.5 Evaluation

The evaluation phase in DSRM focuses on appraising the effectiveness, accuracy, and practical alignment of the proposed solution. In this study, the framework's validity was explored through tests with BIM practitioners, validation by the industrial partner, and evaluating against predefined requirements. The industrial partner's feedback confirmed the solution's potential for commercial development. Furthermore, comparing the developed solution with the specified ideal requirements revealed that most criteria were met, with the exception of fully granular authentication—currently supporting collections of objects rather than individual ones.

1.7.6 Communication

The Communication phase of DSRM focuses on disseminating research outcomes, insights, and contributions to academic and industry audiences, ensuring the work advances both theoretical knowledge and practical applications. In this study, the framework's results are communicated through three interconnected avenues to maximize impact and adoption.

A commercial product will be developed based on the Minimum Viable Product (MVP) created during earlier phases, enabling real-world adoption and refinement. This product will prioritize compatibility with widely used BIM platforms, ensuring seamless integration into existing workflows.

Concurrently, academic publications are being prepared to share the methodology, findings, and theoretical contributions with the scholarly community. By documenting challenges such as schema-agnostic signature embedding and optimized object grouping, the research aims to advance discourse on data integrity in collaborative built asset environments.

To support practical implementation, comprehensive documentation and guidelines will outline best practices for deploying the framework. These resources will serve as a foundation for future standardization efforts. Collaborations with organizations such as bSI will advocate for formal recognition and adaptation of the solution.

By bridging academia and industry, these communication efforts ensure the framework drives innovation while addressing real-world needs. The commercial product targets practitioners seeking reliable tools, academic publications enrich theoretical frameworks, and standardization initiatives promote trust and adaptation of the solution.

1.8 Structure of the thesis

This thesis is structured around four primary contributions: three conference papers and one journal article. Although each work can stand alone, they collectively offer a holistic response to the research questions outlined in the problem statement, forming a continuous progression from conceptual motivations to a fully realized framework for object-level authentication in BIMs. Table 1.3 summarizes how each paper aligns with the research questions (RQ1, RQ2, RQ3).

Table 1.3 Contribution of publications to research questions

Publication / RQ	**RQ1**	**RQ2**	**RQ3**
Paper 1 (Chapter 2)	✓	✓	
Paper 2 (Chapter 3)			✓
Paper 3 (Chapter 4)			✓
Article 1 (Chapter 5)		✓	✓

1.8.1 Paper 1 - Exploring the potential of digital signatures of Building Information Models to improve trust, transparency, and traceability in Construction projects

Conference Paper 1 serves as an initial investigation into why BIM data demands a more sophisticated framework for authentication and integrity verification. It critically examines and emphasizes current issues surrounding the use of BIM and the exchange of data-enriched models in relation to authentication and data integrity, illustrating how effectively tackling these issues offers significant benefits. The paper subsequently establishes a conceptual foundation regarding data integrity and corresponding verification methods—most notably digital signatures and blockchain techniques—demonstrating their potential for mitigating the identified challenges and providing a high-level comparison of these approaches. Concluding this examination, the

paper presents key requirements and attributes for an optimal solution, alongside a concise overview of the methods presently employed in the construction industry, which primarily depend on file-level authentication. In highlighting the advantages of digital signatures for resolving existing gaps, the paper lays the essential groundwork for implementing object-level authentication strategies.

1.8.2 Paper 2 - Exploring the digital authentication of built asset information models at the object level

Conference Paper 2 extends the conceptual foundation established in Paper 1 by examining potential technical pathways for implementing object-level authentication. Following the requirements and characteristics defined in the earlier work, the paper centers on using the IFC data schema as an open standard for model exchange and employs digital signatures for authentication and data integrity verification. The investigation focuses on existing IFC entities to identify a suitable container for storing digital signature information without altering the standard itself. This is achieved by specifying the metadata required for digital signatures and mapping those elements to the IFC data schema, ultimately concluding that IfcObjectReferenceSelect could serve as the container. Although the immediate objective is to integrate digital signatures into the existing IFC schema and then assign them to individual objects, the paper demonstrates that the complexity inherent in the IFC schema makes a new solution, independent of the schema, a more viable option for practical adoption.

1.8.3 Paper 3 - Exploring the possibility of integrating digital signatures into IFC-based built asset information models to achieve authentication and data integrity verification at the object-level

Conference Paper 3 marks another iteration of research on integrating digital signatures directly into the existing IFC data schema for BIM authentication. Building upon the same mapping methods introduced in Paper 2, it evaluates whether object-level authentication can be conducted by matching required signature metadata to three candidate containers in the IFC schema (IfcApproval, IfcOwnerHistory, and IfcObjectReferenceSelect). Although the paper identifies

IfcApproval as the most suitable option—because it effectively handles signature metadata and supports multiple signers—it also highlights the structural challenges of integrating signatures at an object level. Determining how to assign those signatures specifically to an object, including associated data and relationships, becomes the next crucial step. To address that need, the paper explores both the IDS and MVD approaches, concluding that MVD is more practical for maintaining consistent exchanges. Ultimately, the research recommends leveraging the Approval Association concept template, combined with an IDM/MVD methodology, as a future direction for reliably assigning digital signatures at the object level within IFC-based BIMs.

1.8.4 Article 1 - Framework for embedding digital dignatures in IFC-based BIMs for authentication and data integrity verification at the object-level

Article 1 presents a practical solution that shifts away from the IFC data schema-dependent methods previously discussed in paper 2 and paper 3. While earlier efforts focused on directly integrating digital signatures into existing IFC entities (e.g., IfcApproval), this article proposes a schema-independent approach by defining signature blocks that reside in the optional part in ISO 10303-21 standard which is the basis of the IFC exchange structure . These blocks reference the targeted objects within the data section without dependency to the IFC schema itself. As a result, object-level authentication is achieved with minimal impact on existing BIM authoring tools or data exchange workflows. The article demonstrates how each signer's responsibilities, hashing processes, and digital certificates can be consolidated into a well-defined structure at the end of the file, making them invisible to most BIM software yet fully detectable and verifiable by a specialized signing and verification toolkit.

The paper's Introduction articulates the persistent challenge of object-level data integrity in complex, collaborative BIM environments and reiterates the limitations of file-level solutions. In Research Objectives, it outlines three key goals: (1) demonstrating the necessity for granular authentication, (2) establishing requirements for an ideal solution, and (3) designing and testing an IFC data schema-independent method. Limitations and Delimitations clarifies that the article does not address how to select which objects to sign in a project, and it does not prescribe

cryptographic details at length—both are left flexible to accommodate varied industry needs. The research is not going to interfere existing workflows and software tools. The Significance of the Research positions these signature blocks as a means to preserve performance, avoid IFC schema revisions, and promote long-term validation in line with industry and legal standards.

A Background section covers major issues from prior investigations, including the complexity of embedding signatures at the object level and the constraints identified in IFC-based data exchange. A Methodology chapter explains the design science research approach, describing how the signature block structure evolved through iterative testing and feedback from software prototypes and domain experts. The paper's Proposed a modular Framework details how the new signature blocks are appended to the IFC file after the data section, mapping signers' metadata, object lists, and hashing processes into a single, standalone structure. This design avoids conflicts with existing BIM platforms that stop parsing at the data section, thereby preserving interoperability. The article finally presents Conclusions and Future Work, arguing that while schema independence greatly eases adoption, further case studies and user feedback are necessary to refine the approach for a commercialized product.

CHAPTER 2

EXPLORING THE POTENTIAL OF DIGITAL SIGNATURES OF BUILDING INFORMATION MODELS TO IMPROVE TRUST, TRANSPARENCY, AND TRACEABILITY IN CONSTRUCTION PROJECTS

Mehdi Fakour[a] , Erik A. Poirier[b]

[a,b] Department of Construction Engineering, École de Technologie Supérieure, 1100 Notre-Dame West, Montreal, Quebec, Canada, H3C 1K3

Paper published in Advances in Information Technology in Civil and Building Engineering (ICCCBE 2024), March 2025[1]

2.1 Abstract

The way projects are planned, constructed, and managed in the built asset industry is currently being transformed by the utilization of Building Information Modeling (BIM). BIM has emerged as a powerful set of policies, processes and tools that provides a collaborative ecosystem for stakeholders to share and manage project information. However, the digital nature of information models presents unique challenges, particularly in terms of data integrity and authentication. This paper aims to review the existing literature on the authentication of BIMs in construction projects and explore the potential of adding digital signatures to BIM models as a solution to address identified challenges around data compliance and integrity. The paper will explore the benefits of digital signatures in terms of enhancing trust, accountability, traceability, and transparency in construction projects by ensuring that the digitally signed content has not been tampered with and that they originate from a verified source. This is crucial in a collaborative environment where multiple stakeholders and teams contribute to creating, modifying, and using the model. Furthermore, digital signatures could be beneficial in resolution of conflicts like contractual disputes by providing a non-reputable, verifiable, and traceable record of model changes and approvals.

---

[1] This paper was presented at ICCCBE 2024, held at the École de technologie supérieure (ÉTS) in Montréal, Québec, Canada, from 25 to 28 August 2024.

2.2 Introduction

2.2.1 Background

The construction industry is a complex and diverse sector that delivers its products and services through the collaboration of multiple teams, experts, and subcontractors (Kamara, Augenbroe, Anumba & Carrillo, 2002). The construction process is supported through significant amounts of information, and recent advances in software technology and tools like Building Information Modeling (BIM) or Digital Twin (DT) are implied to improve collaboration, information integration, and communication among teams (Jallow, Demian, Baldwin & Anumba, 2014). BIM enables the creation of "a digital representation of a building or infrastructure project" (Azhar, 2011), incorporating various data elements such as geometry, spatial relationships, and properties of building components (Azhar *et al.*, 2008). The digital model functions as a collaborative knowledge repository for all involved parties in the project, enhancing decision-making, coordination, and communication across the project lifecycle (Kotula, 2023).

Despite the great potential of BIM, the current mechanisms used to exchange project information for official use are limited mostly to exchange drawings and PDF files rather than communicating information and other deliverables between stakeholders (Tribelsky & Sacks, 2011). In fact, the digital nature of BIM models poses challenges related to data integrity and authentication. As multiple stakeholders and teams contribute to creating and modifying the model, ensuring the trustworthiness and authenticity of the information becomes crucial. Unauthorized modifications or tampering of the model can lead to errors, disputes, and delays in the construction process. Therefore, there is a need for mechanisms that can enhance trust, transparency, and traceability in BIM models. Finding a solution which can tackle BIM related challenges for exchanging data enriched models alongside addressing legal and jurisdiction problems would have significant impact on the domain.

2.2.2 Objectives

This paper aims to explore the potential of adding digital signatures to BIM models as a solution to address the challenges associated with authenticating and ensuring the integrity of BIMs at object level in construction projects. Additionally, it will highlight requirements of the ideal solution for adding a digital signature to BIMs at object level to boost secure digital data delivery.

2.3 The imperative of authenticating and ensuring the integrity of BIMs

The construction industry has raised concerns about the limitations of 2-dimensional and entity-based tools, impacting various aspects such as spatiality and communication (Olatunji, 2011). Building information modeling (BIM) is considered a solution to these problems, promoting collaboration among participants from various disciplines through the project life cycle (Volker & Chao-Duivis,M.A.B., 2010). In fact, BIM has demonstrated innovative attributes based on effective collaboration among project teams throughout the lifecycle of projects. However, challenges still exist in its implementation; various studies have focused on different aspects of challenges in implementing BIM, including "technocentric and process change" (Yu *et al.*, 2023a; Holzer, 2011), legal and contractual risks (Olatunji, 2011; Abd Jamil & Fathi, 2020; Mohammadi *et al.*, 2024) and have suggested some solutions based on different parameters such as projects delivery methods, contracting systems or specific application in project life cycle such as digital delivery methods (Maier, 2020; Hwang, Ngo & Her, 2020) or construction supply chain (CSC) data delivery (Hijazi *et al.*, 2021). It is worth mentioning that some risks and challenges are not exclusive to BIM-based projects; they are common in construction projects. In fact, exchanging artifacts is a part of the construction project lifecycle, whether BIM is present or not. The Figure 2.1 illustrates the overall steps and phases in the construction project lifecycle, focusing on the need to sign off on produced artifacts. These phases are based on the guidelines presented in The Canadian Handbook of Practice for Architects (RAIC, 2020/2022) and the COBie (Construction to Operations Building Information Exchange) v3 Standard (NBIMS-USTM, 2023) by NBIMS-US (National BIM Standard-United States). In

addition, A summary of the highlighted issues related to the importance of authentication and integrity of BIMs is presented in Table 2.1.

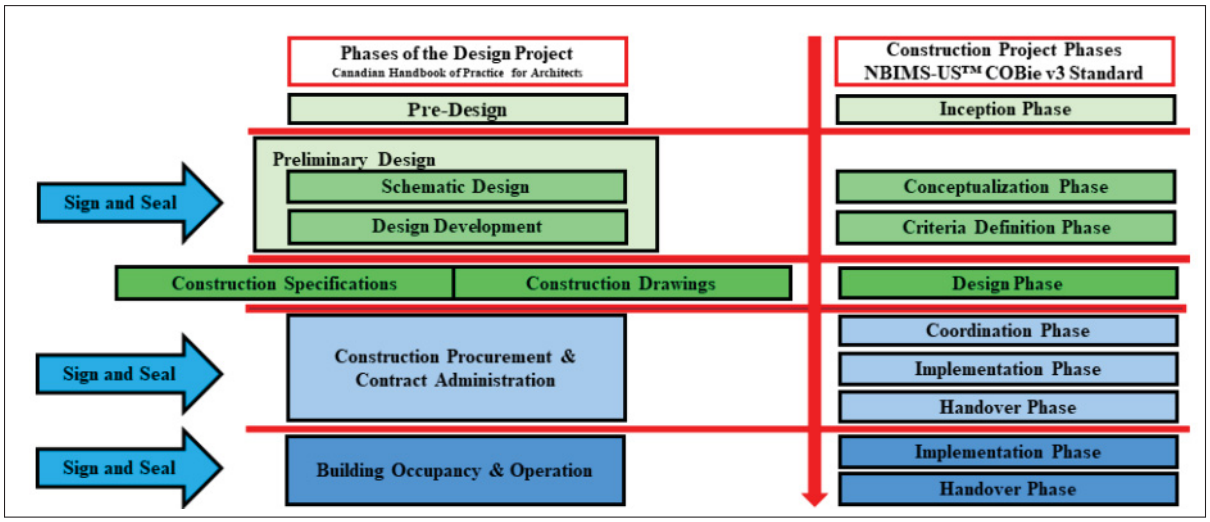

Figure 2.1 Steps and phases in construction project life-cycle (RAIC, 2020/2022; NBIMS-USTM, 2023)

Ensuring the authenticity and integrity of BIMs is crucial for BIM implementation success. Here's an explanation of the imperative of authenticating and ensuring the integrity of BIMs, considering the mentioned issues:

1. Authenticating BIMs establishes trust and transparency among stakeholders by ensuring that the information contained in the model is reliable and has not been tampered with. Trust is essential for effective collaboration (Hijazi *et al.*, 2021; Saini *et al.*, 2019), mitigating risks (Saini *et al.*, 2019).
2. Authentication enables traceability, allowing stakeholders to track changes and modifications made to the construction project via BIMs (Hijazi *et al.*, 2021; Deng *et al.*, 2019). Moreover, traceability is critical for accountability, auditability, particularly in case of legal claims and disputes (Bodea, 2018).
3. Since BIM promotes collaboration between involved parties (Arensman & Ozbek, 2012), trustworthy and intact BIMs facilitate effective communication and collaboration among project participants. Authenticating the information promotes a shared understanding of project data, reducing the risk of miscommunication and errors.

Table 2.1 Summary of highlighted issues of applying BIM

NO.	Issue	Context	Reference
1	Trust (transparency)	Data delivery	Hijazi *et al.* (2021); Saini, Arif & Kulonda (2019); Deng, Gan, Das, Cheng & Anumba (2019)
2	Traceability	Legal and contractual, Data delivery	Bodea (2018); Celoza, de Oliveira & Leite (2023); Hijazi *et al.* (2021); Deng *et al.* (2019)
3	Communication and Collaboration	Legal and contractual, Data delivery	Arensman & Ozbek (2012); Hijazi *et al.* (2021); Saini *et al.* (2019)
4	Interoperability	Legal and contractual, Data delivery	Olatunji (2011); Abd Jamil & Fathi (2020); Alwash, Love & Olatunji (2017); Mohammadi *et al.* (2024); Hijazi *et al.* (2021)
5	Integrity of Shared Information	Legal and contractual	Alwash *et al.* (2017); Bodea (2018)
6	Professional liability	Legal and contractual	Alwash *et al.* (2017); Arensman & Ozbek (2012); Arshad, Thaheem, Nasir & Malik (2019); Celoza *et al.* (2023)
7	Indefatigability of e-doc as evidence	Legal and contractual	Olatunji (2011); Alwash *et al.* (2017); Arshad *et al.* (2019); Mohammadi *et al.* (2024)
8	Stamping and sealing 2D drawings only	Legal and contractual	Celoza *et al.* (2023)
9	Ownership and intellectual property (IP) rights	Legal and contractual, Data delivery	Olatunji (2011); Abd Jamil & Fathi (2020); Alwash *et al.* (2017); Arensman & Ozbek (2012); Arshad *et al.* (2019); Bodea (2018); Mohammadi *et al.* (2024); Hijazi *et al.* (2021)

4. Interoperability has various types including "person-person" (Turk, 2020), "person-system" (Turk, 2020), and "system-system" (Turk, 2020). The research focuses on the system-system interoperability, which in the construction industry encompasses various dimensions and level, including "technology or technical" (Turk, 2020; Sattler *et al.*, 2021), "process" (Poirier, Forgues & Staub-French, 2014), "organization" (Turk, 2020; Sattler *et al.*, 2021),

"legal" (Turk, 2020; Shehzad *et al.*, 2021) and "semantic" (Turk, 2020; Shehzad *et al.*, 2021; Sattler *et al.*, 2021). Ensuring the integrity of BIMs promotes interoperability, enabling different software applications and stakeholders to work seamlessly with the shared information, aligning with other mentioned concerns. Interoperability issues can lead to data corruption or loss, impacting the overall effectiveness of collaborative efforts.

5. Authenticating BIMs maintains the integrity of shared information, preventing unauthorized changes that could compromise the accuracy of the model. This is vital for the reliability of the information used by different stakeholders (Alwash *et al.*, 2017).
6. Professional liability concerns the legal responsibility of individuals or organizations for their actions and decisions during the project lifecycle (Arensman & Ozbek, 2012). Since BIMs could be output of collaborative efforts with multiple experts from different disciplines participating in the design process, assigning a responsible professional for each object in the model is crucial (Celoza *et al.*, 2023). Authentication supports professional liability by ensuring that contributions to the BIMs are clearly identified, thereby reducing the risk of disputes and legal issues.
7. Ensuring the integrity of BIMs is crucial for using them as reliable electronic documents in legal and contractual matters. Indefatigability ensures that BIMs can serve as trustworthy evidence, supporting claims, disputes, and compliance with regulations.
8. BIM goes beyond traditional 2D drawings, encompassing 3D models and comprehensive data. Ensuring the integrity of the entire BIM, not just 2D drawings, is essential. In some jurisdictions, stamping and sealing (Celoza *et al.*, 2023) serve as formal endorsements of the authenticity and accuracy of the information, offering a level of assurance in compliance with regulations.
9. Authenticating BIMs helps establish and protect ownership and intellectual property rights of the contributors. Clear identification of the contributors and their contributions ensures proper attribution and adherence to legal agreements.

2.4 Data integrity and its verification techniques

BIMs, as with any other data-intensive system, contain significant amounts of data and processes involving the creation, modification, exchange, and storage of data. In this context, data integrity emerges as a crucial concern in both legal and technical aspects, with overlapping properties in their definitions. From a technical perspective, the 802.1AE-2018 - IEEE Standard defines data integrity as "A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored." (IEEE 802.1AE-2018, 2018). Legally, the Act to establish a legal framework for information technology in Quebec [31] emphasizes the importance of ensuring technology-based document integrity, involving the verification of unaltered content and stability throughout its lifecycle. Security measures play a vital role in safeguarding the document from creation to archiving or destruction, ensuring its integrity during transfers, consultations, and transmissions (legisquebec, 2024). Another definition of data integrity, providing more precise details about characteristics of data integrity, is proposed by the US Food and Drug Administration (FDA) as "data integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA)." (FDA, 2018). To the ALOCA principles of data integrity, Complete, Consistent, Enduring, and Available were added to create the ALOCA+ principles (Girard & Watkin, 2021). The summary of ALOCA+ principles is illustrated in Figure 2.2. Two common techniques for verifying data integrity in construction industry are Digital signature algorithms and Blockchain-based techniques. In the next sections, the related concepts of these techniques are explored; however, technical details and algorithms are not in the scope of this research.

2.4.1 Digital signature

Exchanging data through unsecure channel has been an age-old issue, resulting in the development of cryptographic algorithms (Anghel, Rădulescu & Marinescu, 2023). A digital signature is defined as "the use of cryptographic methods and asymmetric cryptography to sign data and provide origin authentication, data integrity, and signer non-repudiation." (Mulder *et al.*, 2023).

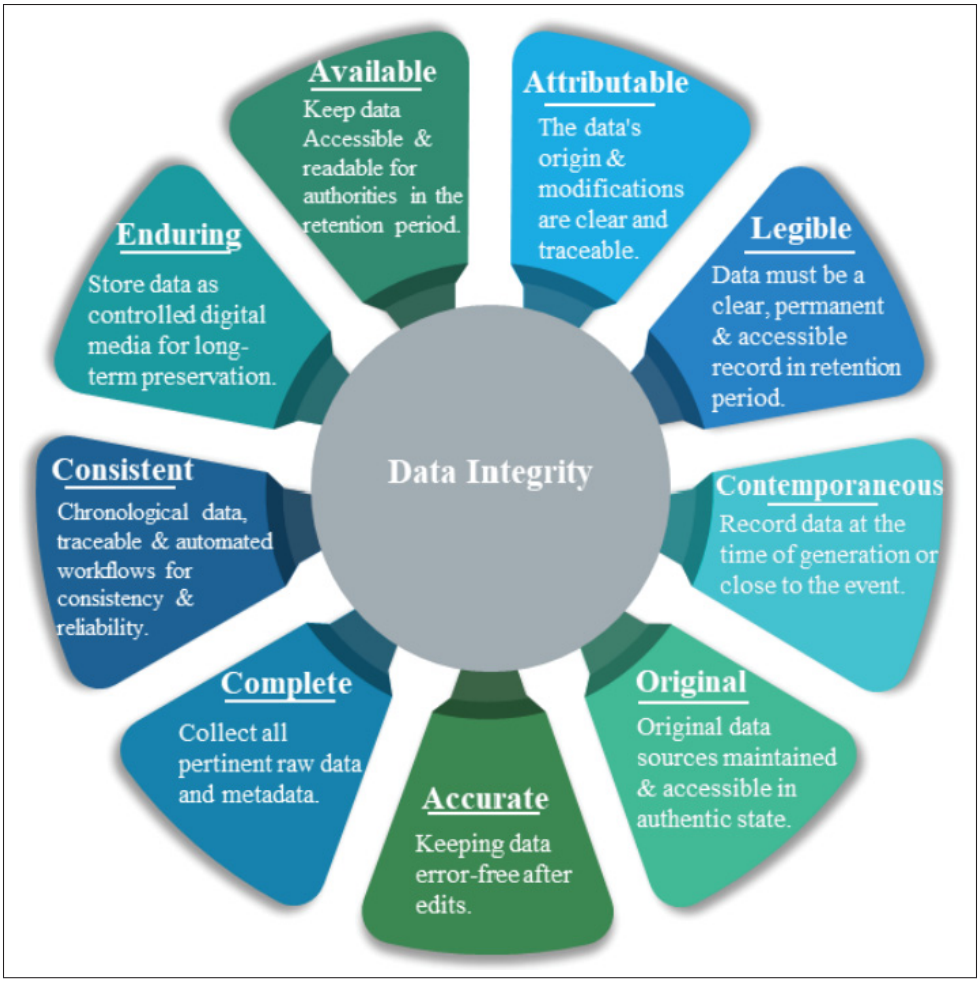

Figure 2.2 Summary of ALOCA+ Principles (FDA, 2018; Yemm, 2019)

In fact, digital signatures mimic the characteristics of handwritten signature to securely sign digital documents (Gamalielsson *et al.*, 2015; Sultana, 2021). The characteristics of hand written signatures include authenticity, non-repudiation, irreversibility, non-reusability, and inalterability (Sultana, 2021).

The signing process includes creating a data hash through a cryptographic hash algorithm, encrypting the hash with the signer's private key, which contains the digital identity of the signer, and then sending both the plain data and encrypted hash to the verifier. The verifier assesses the signature's validity by creating a hash of the data and comparing it to the received hash (Mulder *et al.*, 2023). It is worth noting that a timestamp is included in the signing process;

therefore, every time that a signatory signs the same content, the digital signature would be different. Figure 2.3 adapted from (Mulder *et al.*, 2023), illustrates the digital signing and verifying process.

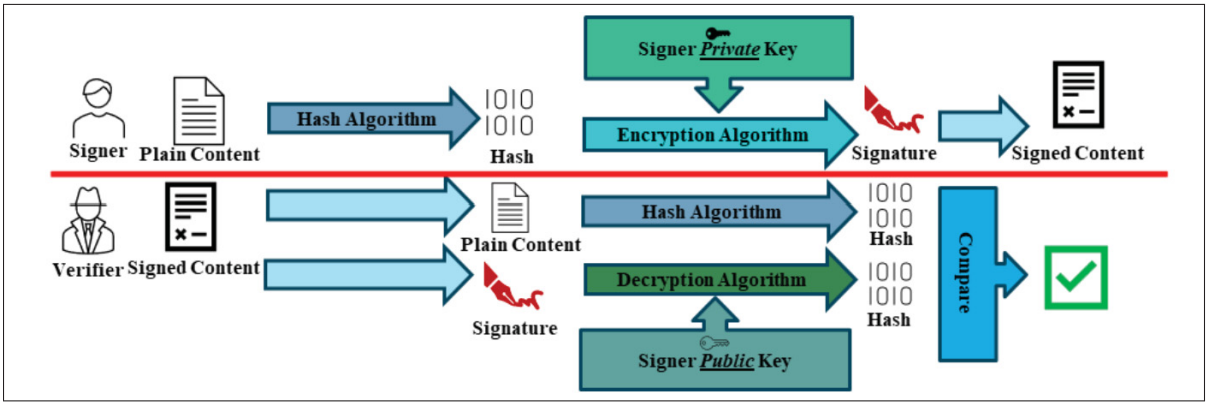

Figure 2.3 Summary of digital signing and verifying process
Adapted from (Mulder *et al.*, 2023)

Various research studies have enumerated the characteristics of digital signature, as described in the Table 2.2. Considering these characteristics is crucial because it demonstrates the potential of digital signatures in addressing challenges related to the use of BIM, particularly in authentication and data integrity.

2.4.2 Smart contracts and blockchain

A smart contract refers to an executable code that performs automatic operations on blockchain technology. It is designed with the purpose of expediting, validating or ensuring a pre-determined agreement between parties involved in a transaction (Huang *et al.*, 2019). By managing and recording changes made to BIMs, a smart contract is capable of enforcing certain behaviors by the parties involved in a transaction (McNamara & Sepasgozar, 2021). This can reduce opportunistic behavior that may arise as a result of any deficiencies present within the initial BIM contract (Chong & Cheng, 2023). Although smart contracts have the potential to improve BIM-enabled projects, there are challenges that must be addressed. Legal considerations pose a significant obstacle to their adoption and implementation (Li & Kassem, 2021), while

Table 2.2 Properties of a valid digital signature

NO.	Property	Description	Reference
1	Data integrity	data has not been tampered with, damaged, or lost during transmission and storage.	Anghel *et al.* (2023); Yu *et al.* (2023b); Mulder *et al.* (2023); Iswari & Rudy (2023); Chauhan *et al.* (2022); Sadkhan & Sadkhan (2022); R. Alagheband & Mashatan (2022); Roy & Karforma (2012)
2	Authenticate the origin	The signatory signed the document	Anghel *et al.* (2023); Yu *et al.* (2023b); Mulder *et al.* (2023); Iswari & Rudy (2023); Chauhan *et al.* (2022); Sadkhan & Sadkhan (2022); R. Alagheband & Mashatan (2022); Roy & Karforma (2012)
3	Non-repudiation	The signatory cannot deny the signature. Digital signature only provides non-repudiation of the source or signer.	Anghel *et al.* (2023); Yu *et al.* (2023b); Mulder *et al.* (2023); Iswari & Rudy (2023); Chauhan *et al.* (2022); Sadkhan & Sadkhan (2022); R. Alagheband & Mashatan (2022); Roy & Karforma (2012); Sultana (2021)
4	Not reusable	A signature cannot be used for another document	Sultana (2021); Chauhan *et al.* (2022); Sadkhan & Sadkhan (2022)
5	Not forged	Only signatory can create valid signature	Sultana (2021); Sadkhan & Sadkhan (2022)
6	Audit Trail	digital signatures indicate a snapshot with the signer's identity and timestamp.	Saurabh Bhausaheb Gawali (2023)

technology integration complexities and multiple stakeholders further compound these issues (Nawari & Ravindran, 2019).

Blockchain, a type of distributed ledger technology (DLT), relies on decentralized data notion in which all transactions are kept in a chain - continuous sequence - of blocks (Zheng, Xie, Dai, Chen & Wang, 2018). This characteristic has significant implications for activities in

the construction and understanding it is crucial to comprehend blockchain's potential impact (Li, Greenwood & Kassem, 2019; Perera *et al.*, 2020). Data has traditionally been maintained in a centralized database that is administered and controlled by a single organization. This arrangement often causes conflicts between stakeholders due to the absence of transparency regarding how the data is processed and distributed (Hijazi *et al.*, 2019).

Within blockchain technology, data is duplicated throughout a network consisting of various stakeholders. These parties can access and enter information into the ledger from its point of origin all the way through to storage, processing, and operation stages (Hijazi *et al.*, 2021; Vadgama, 2019). Blockchain supports diverse types of data such as historical records, stakeholder identification details or ownership information along with logistics monitoring providing greater value when combined with supply chain activities workflows which leads to improved reliability and tractability (Hijazi *et al.*, 2021).

The blockchain data structure is capable of supporting auditability for activities (Hijazi *et al.*, 2019) without central authority (Chiu & Koeppl, 2019), making it a perfect solution for environment with zero-trust basis among involved parties. Therefore, every actor working with a blockchain ledger has access to the same source of information and can query or invoke the ledger at any time, where all transactions are bundled into blocks (Hileman & Rauchs, 2017). Each block in this chain links back to its predecessor through cryptographic hash functions, enhancing trust between different entities, increasing cooperation opportunities, and overcoming transparency issues ultimately leading towards reliable service delivery outcomes (Holland, Stjepandić & Nigischer, 2018). Regardless of great potential in the blockchain-based solutions, there are some challenges in implementing them including lack of legal regulations (Li & Kassem, 2021), complexity of technical issues in implementation such as "scalability" (Zheng *et al.*, 2018), "privacy leakage" (Zheng *et al.*, 2018). A summary of the properties of blockchain-based solution is listed is Table 2.3.

Table 2.3 Properties of blockchain-based solutions

NO.	Property	Description	Reference
1	Data tamper-proof	Changing a block alters the following block's hash, indicating potential misconduct.	Yu *et al.* (2023b)
2	Traceability	Each block contains hash values, timestamps, and transaction data, ensuring the data's origin and integrity.	Yu *et al.* (2023b); Hijazi *et al.* (2021)
3	Data confidentiality	It encrypts data using public and private keys, limiting access to authorized users.	Yu *et al.* (2023b)
4	Trust (Transparency)		Hijazi *et al.* (2021, 2019); Holland *et al.* (2018)
5	Authenticate the origin	Only signatory can create valid signature	Hijazi *et al.* (2021); Vadgama (2019)
6	Auditability	digital signatures indicate a snapshot with the signer's identity and timestamp.	Zheng *et al.* (2018); Hijazi *et al.* (2019)
7	Non-repudiation	It creates Non-repudiation of Origin and Non-repudiation of Receipt.	Fang *et al.* (2020)

2.4.3 Capabilities of digital signature and blockchain to address issues of applying BIM

Digital Signature and Blockchain are two technologies that can be utilized to address mentioned issues of applying BIM in the construction projects, as outlined in Table 2.1. Table 2.4 represents how each technology can contribute based on discussions in previous sections. However, applying digital signature and blockchain technology to 3D BIMs at object level is a complicated issue that has not been addressed yet, and this paper identified that as a research gap.

Table 2.4 Capabilities of digital signatures and blockchain to address issues when applying BIM

Issue	**Digital signature capability**	**Blockchain capability**
Trust (transparency)	Ensures that content originates from a verified and authorized entity.	Its decentralized nature provides transparency to all authorized participants.
Traceability	Creates a traceable record of who made changes to the content and when.	Creates an unchangeable chain of transactions, ensuring a transparent and traceable history of all modifications.
Communication and collaboration	Secures communication by verifying the sender's identity and preserving the integrity of exchanged content.	All involved parties can access identical and up-to-date data.
Interoperability	Guarantees the integrity of data exchanged between different software tools.	—
Integrity of shared information	Verifies that shared information has not been tampered with during transmission or collaboration.	Ensures the immutability of data.
Professional liability	Creates a verifiable link between the professional and the signed content.	Determines accountability by providing an unalterable record of actions.
Indefatigability of e-doc as evidence	Provides a secure, verifiable, and durable signature.	Tamper-resistant nature and modification traceability make it reliable.
Stamping and sealing 2D drawings only	—	—
Ownership and intellectual-property (IP) rights	Establishes ownership by associating the signature with a specific individual or entity.	Provides a transparent and unchangeable record of ownership.

2.4.4 High level comparison of digital signature and blockchain in context of verifying data integrity

Digital signatures and blockchain are technologies used to verify data integrity, ensuring the authenticity and security of digital information. Digital signatures primarily applied to individual

messages or documents, offering a way to verify or authenticate the identity of the signer and confirm that the content has not been tampered with during exchange. Digital signatures typically require a central authority to define and assign signatory's identity and verify the validity of the signature. Digital signatures provide traceability by creating a snapshot of the document at the time of signature.

Blockchain is a decentralized technology that enables secure and transparent recording of transactions through a network of blocks, where each block includes a list of transactions. As a result, there is no need for centralized authority. Moreover, blockchain technology offers transparency, traceability, non-repudiation for both the source and recipient, and guarantee that the content is not forged. This is achieved because, in each transaction, information related to the identity of the initiator and the transaction date is recorded in the network.

Another aspect in the comparison of digital signatures and blockchain technology is the legal perspective, which affects the acceptance, validity, and enforceability of each solution. In the case of digital signatures, many countries have enacted laws that recognize the legal validity of digital signatures, while blockchain technology requires more regulatory attention.

Final consideration is the complexity of implementing and maintaining both techniques. The implementation and maintenance of blockchain technology involves more complexity and overhead, as it consists of multiple nodes in the network, and any change must be transmitted to all nodes. Additionally, legal requirements and the nature of construction projects imply that any solution used must support "long-term validation" (Secretariat Treasury Board of Canada, 2021). Keeping a blockchain network alive for a long time entails complex and costly solutions.

2.5 Requirements and attributes of a potential solution

The requirements of a potential solution aimed at authenticating and verifying the data integrity of BIMs at object level. have been distilled through analysis of literature and existing solutions within the asset building industry for data exchange, as well as insights from analogous industries like manufacturing industry and aviation. Additionally, consideration has been

given to established standards in the domain of digital information exchange and relevant laws. Furthermore, interviews with domain experts in this field contribute valuable perspectives to inform the delineation of essential requirements for the potential solution.

The Utah Department of Transportation (UDOT) in the United States has been actively engaged in advancing BIM-based projects, striving for a fully digital implementation to utilize models as a legal document (MALD) for the projects. In their 2020 research report, they present the attributes of a digital delivery framework (Maier, 2020). The Figure 2.4 adapted from (Maier, 2020), illustrates a summary of the attributes of digital delivery framework. It is worth noting that these attributes are mostly align with the ALOCA+ principles for data integrity.

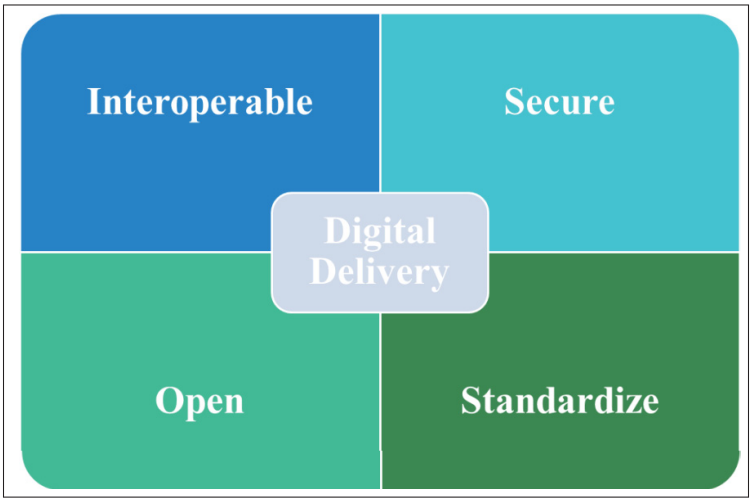

Figure 2.4 Attributes of digital delivery framework
Adapted from (Maier, 2020)

2.6 Conclusion

This paper has delved into the imperative of authenticating and ensuring the integrity of BIMs at object level in the asset building industry. The highlighted issues underscore the importance of addressing challenges such as trust, traceability, communication, interoperability, and professional liability in the context of BIMs. The paper has explored two promising technologies, namely digital signatures and blockchain, to mitigate these challenges and enhance the authentication and integrity of BIMs. Digital signatures, leveraging cryptographic methods,

provide data integrity, origin authentication, non-repudiation, and traceability. On the other hand, blockchain, with its decentralized and tamper-proof nature, offers transparency, traceability, data confidentiality, and trust. The comparison between digital signatures and blockchain has revealed their strengths. Additionally, a high-level comparison has considered legal aspects and implementation complexities.

Moving forward, the identified gap in authenticating 3D BIMs at the object level presents an opportunity for future research. The future solution should address the complexities of the construction industry, legal requirements, and the need for long-term applicability. Insights from industry experts and existing standards for digital information exchange have informed the requirements for a potential solution, emphasizing interoperability, data preservation, and security.

CHAPTER 3

EXPLORING THE DIGITAL AUTHENTICATION OF BUILT ASSET INFORMATION MODELS AT THE OBJECT LEVEL

Mehdi Fakour[a] , Erik A. Poirier[b]

[a,b] Department of Construction Engineering, École de Technologie Supérieure, 1100 Notre-Dame West, Montreal, Quebec, Canada, H3C 1K3

Paper published in ITC Digital Library[1], October 2024 [2]

3.1 Abstract

Building Information Modeling (BIM) provides a significant opportunity to enhance the performance of the asset building industry by enabling efficient collaboration and information exchange among stakeholders. Developed by buildingSMART, the Industry Foundation Classes (IFC) has been established as an open standard, facilitating data exchange and interoperability. The adoption of IFC offers several advantages for BIM data exchange. It promotes interoperability among different software platforms, allowing stakeholders to seamlessly exchange BIMs without format conversion issues. However, ensuring the authenticity and integrity of BIM data remains a critical concern. Various solutions and standards for exchanging and authenticating BIMs have been developed, yet certain flaws persist including limited support for object-level authentication, implementation complexity, and maintenance consideration like long-term verification. This research explores the potential of adding digital signatures to BIMs at the object level by investigating the IFC schema and highlights the existing challenges regarding IFC structure to implement a fully functional solution.

---

[1] Digital library of construction informatics and information technology in civil engineering and construction.

[2] This paper was presented at the CIB W78 and buildingSMART International Summit, held in Marrakech, Morocco, from 1 to 3 October 2024.

3.2 Introduction

One of the significant advantages of applying BIM in projects is the improvement in efficiency and productivity by facilitating collaboration among all multidisciplinary parties and stakeholders involved throughout project life cycle (Poirier *et al.*, 2017; Song, Zhang & Marks, 2021). In fact, BIM serves as a platform to improve collaboration (Zhang, Pan, Wu & Skibniewski, 2021) providing the possibility of generating and managing data (Mohammad, Abdullah, Ismail & Takim, 2019), as well as exchanging and sharing reliable information, which results in better decision-making (Zhang *et al.*, 2021). However, there are many challenges in adopting BIM in practice, including lack of trust and transparency (Saini *et al.*, 2019), Traceability (Celoza *et al.*, 2023), Interoperability (Mohammadi *et al.*, 2024), security and integrity of the shared information (Bodea, 2018), professional liability (Arshad *et al.*, 2019), and Ownership and intellectual property (IP) rights (Hijazi *et al.*, 2021).

Addressing the challenges mentioned above requires a solution ensuring authenticity and integrity of BIMs. Additionally, any solution should be compatible with existing (and emerging) processes and standards, aligned with regulatory and legal concerns, while supporting interoperability between software tools. One such approach, openBIM as an open standard which is "a collaborative process that is vendor neutral" (bSI, 2020) and its related concepts and standards, should be considered as a solution for regarding technical interoperability between software platforms as well as semantic and syntactic interoperability between business processes (Jiang *et al.*, 2019). The research presented in this paper explores the possibility of applying data integrity techniques at the object level on BIMs in IFC format.

3.2.1 Research methodology

The research begins with a literature review by exploring multiple academic databases like Scopus and Google Scholar to understand BIM adaption challenges in context of legal concerns, digital delivery, data integrity, data integrity verification techniques, OpenBIM eco-system, and related standards particularly IFC standards, focusing on how digital signatures can be integrated

within the BIMs. This involves examining required digital signature meta-data and mapping their components onto the IFC structure to ensure compatibility with existing BIM processes.

In order to understand the practical requirements of an ideal solution, workshops were conducted with Cybersecurity professionals and BIM experts. The next phase involves analyzing the IFC schema to identify suitable containers for digital signatures at the object level. This includes exploring the hierarchical structure and relationships within IFC data to determine the feasibility of embedding digital signatures without significant modifications, as well as identifying practical challenges and limitations.

3.2.2 Research objective

This paper aims to explore the IFC schema to examine the possibility of adding digital signatures to BIMs at the object level by identifying the appropriate container and place in the IFC schema. It also highlights the challenges of exchanging information at the object level in BIMs using the IFC format. The research endeavors to contribute to the discourse on enhancing the integrity of BIM data through the integration of digital signature mechanisms within BIMs in IFC format. This serves as a conceptual foundation for developing a software toolkit, thereby facilitating reliable information exchange and collaboration in the building asset industry.

3.3 Background

The ideal solution for authenticating and verifying BIM data integrity should be interoperable, secure, open, and standardized (Maier, 2020). Additionally, based on professional opinion, it should ensure durability and long-term verification while being a standalone solution with minimal dependency on other tools and minimal intervention in existing tools and processes, to facilitate the adoption of the new solution in practice. Experts also emphasize the need for the ability to authenticate BIM objects in use cases where the model is created by multiple engineers, each responsible for their part as well as vouching other's work.

Current solutions mostly are based on standards that involves creating a memorandum file, either by converting the model to 2D pdf or by using a document as a cover that contains a list of files and attached files in a container (ARINC827-1, 2020; ARINC835-1, 2014; ISO21597-1:2020, 2020; PDF/A-3, 2020). Even BIM Common Data Environments (CDE) act as repositories for storing files. In fact, existing solutions support file-based authentication and would not support the mentioned cosigning or vouching scenarios.

Various techniques exist to verify data integrity, including digital signature algorithms and blockchain-based techniques, which are commonly employed. Block-chained solutions and their integration in BIM-based projects have received significant attention recently and there are some implemented solutions which support both file level (Pradeep *et al.*, 2020) and object level (Xue & Lu, 2020) data integrity verification. Despite the various advantages of Block-chained solutions, including transparency (Hijazi *et al.*, 2019; Holland *et al.*, 2018), traceability (Hijazi *et al.*, 2021; Yu *et al.*, 2023b), and non-repudiation for both the source and recipient (Fang *et al.*, 2020) as well as providing a tamper-proof eco-system (Yu *et al.*, 2023b) to protect data, there are still many shortcomings, particularly in construction projects.

In fact, the adoption of Block-chained solutions in practice requires more thought in terms of regulatory and legal concerns (Li & Kassem, 2021). Moreover, the current technical complexity inherent in deploying block-chain makes them hard to implement and maintain (Nawari & Ravindran, 2019). More specifically, existing regulations and norms in construction projects require that any solution for authentication and data integrity support long-term validation (legisquebec, 2024; Secretariat Treasury Board of Canada, 2021). This can be challenging to achieve using blockchain techniques, which consist of a decentralized network of blocks. In other words, blockchain solutions are more suitable for real-time data exchange and sharing and may be less suitable for digital authentication. Indeed, most frameworks and solutions in the literature point to the suitability of blockchain for ongoing construction projects or for data delivery within the construction supply chain (CSC) (Hijazi *et al.*, 2021).

On the other hand, digital signatures are widely used to identify signatories and verify the integrity of digital documents (Lax, Buccafurri & Caminiti, 2015). Digital signatures are accepted and used formally in many jurisdictions and industries. They are easier to implement and maintain compared to blockchain-based solutions. In fact, there are common standards, processes, and tools for applying digital signatures for digital documents and 2D drawings. Therefore, this paper focuses on digital signature and explores the possibility of integrating them in BIMs at the object level. It is worth noting that digital signatures do not create a tamper-proof eco-system. Instead, they allow the creation of a snapshot of the model at a specific date and time in order to detect any unauthorized modification afterwards. A summary of the high-level comparison between digital signatures and blockchain techniques in the context of this research is presented in Table 3.1.

Table 3.1 High-level comparison of digital signatures and blockchain techniques

Aspect	**Digital Signatures**	**Blockchain**
Legal Acceptance	Widely recognized	Requires more regulations
Implementation and Maintenance Complexity	Relatively simple	Higher complexity
Long-Term Validation (LTV)	Support LTV	Complex and costly solutions

Based on the preferred requirements of ideal solution and comparison presented, digital signatures emerge as a more promising solution compared to blockchain techniques for verifying data integrity in the built asset industry.

3.3.1 Digital signatures and their required Meta-Data

A digital signature employs cryptographic methods to verify the authenticity and integrity of digital content (Goswami, Singh & Rahman, 2021; Rai *et al.*, 2023; Seetha, 2017). Adding a digital signature to digital content is done following two main processes: signing and verifying (Mulder *et al.*, 2023). The details of these processes, such as digital signature types, hashing and cryptographic algorithms, certificates, key management algorithms and their implementation

are not within the scope of this research. The focus of the research is to highlight a mapping between the meta-data in the digital signature or certificate related to signatory and IFC data schema.

Table 3.2 presents combination of partial structure of the X.509 certificate structure, as a common "public-key certificate framework" (ITU, 2019) and XML Advanced Electronic Signatures (XAdES) (ETSI, 2010) as a standard for specific type of digital signature, which are required for the signing process. The naming or detail of the parameters may vary in different standards; however, the selected parameters would fulfill the general requirements of this research.

Table 3.2 Required meta-data for signing process

Field	**Sub-Field**	**Description**	**Source**
Issuer	"**Labelling attribute types** (Common name, Surname, Given Name, Initials), **Geographical attribute type** (Country name, Locality Name, State or Province Name), **Organizational attribute types** (Organization Name, Organizational Unit Name, Title/Role)"	The name of the entity issuing the certificate. The sub-fields are based on X.520 (X.520, 2019).	X.509
Subject	"**Labelling attribute types** (Common name, Surname, Given Name, Initials), **Geographical attribute type** (Country name, Locality Name, State or Province Name), **Organizational attribute types** (Organization Name, Organizational Unit Name, Title/Role)"	The subject is the certificate owner's name. The sub-fields are based on X.520 (X.520, 2019).	X.509
Validity	valid from or valid after; valid to or valid before	The validity period of the certificate.	X.509
Signing Time	—	The time the signer completed the signing process.	XAdES

3.3.2 openBIM overview

BIM is a "data-intensive process" (Xu *et al.*, 2023) which covers various aspects of a construction project's life cycle including design and construction to operation and maintenance. Since

various disciplines with multiple software tools are involved in the process, the "proprietary vendor data formats" (bSI, 2020), and in general, system to system interoperability, emerges as a challenge. buildingSMART has developed the openBIM concept taking the form of international open standards and working procedures to create "common alignment and language" (bSI, 2020). The combination of these standards would support various aspects of projects in terms of people, processes, and tools. The summary of the buildingSMART (bSI, 2023a) open standards and services is presented in Table 3.3.

3.3.3 IFC Data Schema

IFC is defined by buildingSMART International and certified by the International Organization for Standardization (ISO) - ISO 16739-1 (ISO16739-1:2024, 2024) - as an international standard file format to facilitate BIM data exchange between and interoperability among software tools (Kim, Lee, Han, Kim & Choi, 2020; Won *et al.*, 2022). Architectural information within IFC files is represented through the "relationships between a building object and its property information" (Kim *et al.*, 2020). IFC is a STEP physical file format -ISO 10303-21- and uses Express language -ISO 10303-1- for schema publication (bSI, 2023b).

Based on (bSI, 2023b), The architecture of the IFC data schema comprises four conceptual layers: Resource, Core, Interoperability, and Domain layers. Figure 3.1 illustrates an overview of the IFC architecture. At the lowest level, the Resource layer contains individual schemas base definitions. The definitions in Resource layer do not have a globally unique identifier (GUID), therefore they cannot be used independently. The next layer, the Core layer contains Kernel schema and core extensions. Entities defined at the core layer or above are assigned a GUID, and they can be initiated independently. The third layer, the Interoperability layer, encompasses schemas containing entity definitions customized for specific product, process, or resource specializations that cover various disciplines. The definitions in the Interoperability layer are usually employed for sharing and exchanging construction information between different domains. The top layer, the Domain layer, contains schemas related entity definitions specialized for products, processes, or resources within specific disciplines. The definitions are primarily

Table 3.3 Summary of the buildingSMART openBIM standards and services

Name	**Type/Standard**	**Description**
IFC (Industry Foundation Classes)	ISO 16739-1:2024	A vendor-neutral data model schema that provides a digital description of built asset projects (ISO16739-1:2024, 2024).
IDS (Information Delivery Specification)	buildingSMART Standard	XML-based computer-interpretable format used to define and check information requirements derived from IFC models (bSI, 2019b, 2024b).
IDM (Information Delivery Manual)	ISO 29481-1:2010	A methodology for defining and documenting information flow and delivery processes throughout a project lifecycle (bSI, 2024e).
BCF (BIM Collaboration Format)	buildingSMART Standard	A structured format that enables the exchange of issue-related information between BIM applications based on shared IFC data (bSI, 2019a).
MVD (Model View Definitions)	buildingSMART Standard	A defined subset of the IFC schema used to fulfill specific model exchange requirements (Jiang *et al.*, 2019; bSI, 2024f) .
bsDD (buildingSMART Data Dictionary)	buildingSMART Technical Service	A federated dictionary system built on ISO 12006-3 (IFD), enabling identification and validation of object names and attributes (bSI, 2024a).
IFC Validation Service	buildingSMART Technical Service	A cloud-based tool for checking the conformity of an IFC file against the IFC standard (bSI, 2024c).
UCM (Use Case Management Service)	buildingSMART Technical Service	A service built on IDM methodology to define, manage, and exchange use cases and implementation practices (bSI, 2024g).

utilized for sharing and exchanging information within the same domain. The IFC data schema architecture is a hierarchical structure in which entities and definitions in higher layers can reference and use those in the lower layers (Won *et al.*, 2022).

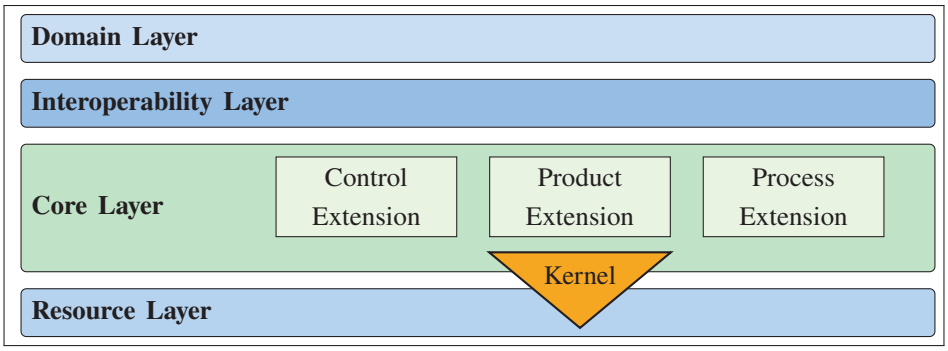

Figure 3.1 IFC data schema layered architecture
Adapted from (bSI, 2023b)

3.4 Findings and results

Various studies suggest different approaches to extend IFC Schema including creating a new entity or extending properties by adding new attributes to existing entities (Yu *et al.*, 2023c). Another approach is reusing an existing entity in the IFC schema which holds all the necessary information for the specific purpose (Won *et al.*, 2022). Since defining new entities or properties and adding them into the schema implies long and complex processes to become part of formal IFC standard, which them lead to modifications in existing tools, the research focuses on finding an existing entity in the schema to reuse it as a container for the digital signature.

3.4.1 Integrating digital signature into the IFC Data Schema

Integrating digital signature into IFC data schema involves ensuring that the signatures are embedded in a manner that is compatible with existing IFC data schema and common standards for digital signatures. As shown in Figure 3.2, the basic definitions of required meta-data for digital signatures can be found in the resource layer. The IfcActorResource schema represents persons or organizations and their relationships and the IfcDateTimeResource schema contains generic definitions of date and time (bSI, 2023b).

To effectively utilize the inheritance structure in the IFC data schema, the digital signature container should be at the lowest possible level in the layered architecture. This ensures that

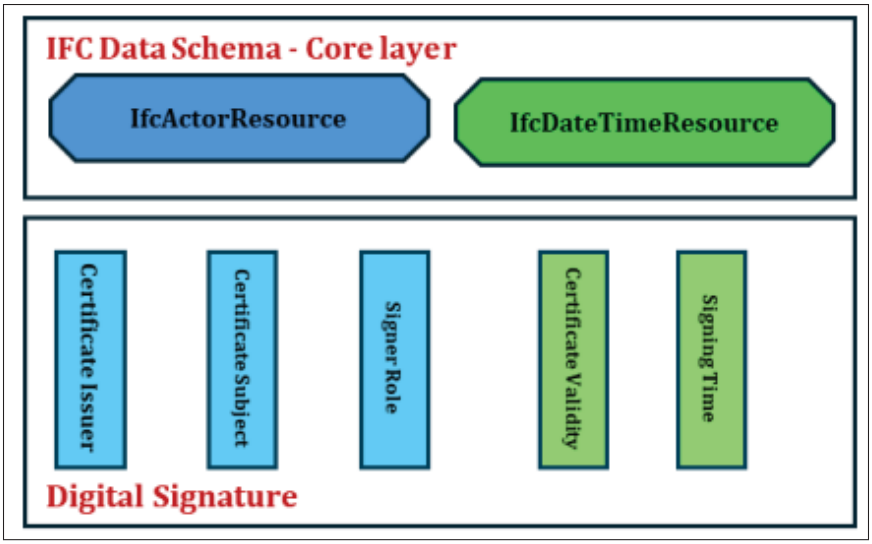

Figure 3.2 High-level mapping between IFC data schema core definitions and digital signature data parameters

the container can be accessed by the maximum number of entities within the schema in higher layers. Interoperability layer and Domain layer are not suitable because some definitions in these layers are specific to a particular concept which are unrelated to other entities, and they are placed in the section of the schema which cannot be inherited by higher levels. Moreover, some entities in lower layers need to have digital signature but they cannot inherit from definitions in higher layers. Consequently, using definitions in these layers requires repeating definition in various places in the IFC data schema. Therefore, the appropriate candidate for this placement would be the Core layer or Resource Layer.

As shown in Figure 3.2, IfcActorResource and IfcDateTimeResource cover the meta-data related to certificate issuer or signer and date and time of digital signature, however adding digital signature to an element requires a container which covers all meta-data together, including the digital signature. By exploring the IFC data schema in the resource layer, the IfcObjectReferenceSelect is found as a potential container for digital signature. Listing 3.1 illustrates the formal representation of IfcObjectReferenceSelect in Express language with highlighted required type values for the digital signature. "IfcObjectReferenceSelect is a select type, that holds a list of resource level entities that can be used as property values for

an IfcPropertyReferenceValue being a property within an IfcPropertySet." (bSI, 2022). The IfcPropertySet is in the Kernel part of Core layer of IFC data schema and serves as a container for properties in property tree which ends in IfcRoot as illustrated in Figure 3.3. In fact, the relation of IfcObjectReferenceSelect with IfcPropertySet and consequently with IfcRoot, as the most abstract and foundational class for all entity definitions originating in the kernel or in higher layers of the IFC specification, ensure that IfcObjectReferenceSelect would be accessible by all entities in the IFC data schema.

IfcObjectReferenceSelect contains type values in relation with other entities and types in IFC data schema which supports adding more detailed meta-data for the digital signature. Additionally, calculated digital signature could be placed in IfcTable which supports having multiple digital signatures with customized table structure on specific object.

Listing 3.1: Representation of IfcObjectReferenceSelect (bSI, 2022)

```
1  TYPE IfcObjectReferenceSelect =
2  SELECT
3    (IfcAddress,
4     IfcAppliedValue,
5     IfcExternalReference,
6     IfcMaterialDefinition,
7     IfcOrganization,
8     IfcPerson,
9     IfcPersonAndOrganization,
10    IfcTable,
11    IfcTimeSeries);
12 END_TYPE;
```

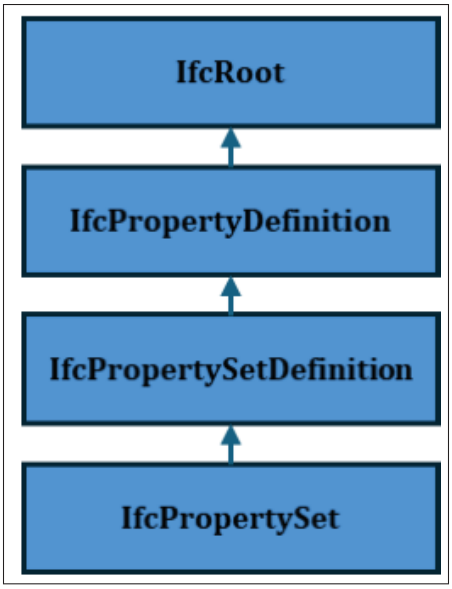

Figure 3.3 Entity inheritance of IfcProertySet (bSI, 2022)

3.4.2 Challenges of using the IFC Data Schema for digital signature of BIMs

Adding digital signatures to specific objects within IFC BIMs involves several significant challenges. In fact, similar to the signing process in the paper-based building models or digitalized 2D models, where the signatory would place the signature on a specific view of the model, this process requires the precise selection of specific objects and their related data in the model. The key challenges associated with this task and IFC Schema are highlighted as follows:

3.4.2.1 Backward and forward compatibility issue in the IFC Data Schema

Backward and forward compatibility refers to the capability of an exchange structure to function correctly with both previous and future versions of a specification (bSI, 2023b). In the current version, IFC 4.3.2, there are new definitions that did not exist in previous versions, as well as definitions that are now obsolete or candidates for obsoletion in the next version. Therefore, using certain definitions in the schema carries the risk that they may not exist in previous or future versions of the IFC data schema. For instance, IfcObjectReferenceSelect, proposed as a

container for digital signatures, is a new type in IFC 2.0, and IfcTable was added to its definition in IFC 4.0 (bSI, 2023b).

3.4.2.2 Exchange of BIM data through the utilization of IFC MVD

MVDs can be considered as "IFC view definition" (Afsari, Eastman & Shelden, 2016) that are extracted from IFC schema to facilitate data exchange based on specific Exchange Requirement (ER) (Chipman *et al.*, 2016). In practice, when the BIM model is developed in an authoring tool, it is exported to IFC format based on selected MVD (Afsari *et al.*, 2016; Yu *et al.*, 2023c). The MVDs and their related exchange requirements are presented by the buildingSMART standard mvdXML. This standard contains predefined templates for the sub-set of IFC schema as a graph, including all required entities and attributes (Chipman *et al.*, 2016).

Whitin the scope of this research, two issues arise when using MVD IFC files to authenticate an object and its related entities: 1) There is a possibility of referencing entities that are not included in the files. This creates potential legal issues since an engineer might be responsible for an object that does not exist in the exported MVD IFC file. 2) predefining all possibilities for all entities and their combinations in the IFC schema is almost impossible.

3.4.2.3 Relationships in IFC schema

Relationships between entities play a significant role in IFC data structure in terms of consistency in definitions and creating flexible and extendable structures. However, the various types of relationships, including inverse relationships and objectified relationships along with related concepts attached to them including references, cardinality, make IFC BIMs complex for analyzing and navigation. In fact, this complexity creates challenges for "object-based use of IFC data" (van Berlo *et al.*, 2021).

One approach to explore the issue of navigating IFC model starting from a selected object toward extracting all related objects is applying graph-based theories and methods to BIMs data because of IFC models object-oriented nature (Ismail, Nahar & Scherer, 2017; Tauscher & Crawford,

2018). By considering an IFC model as a graph, we need to find all possible path starting from specific object and ending with an object that has no related object. If the graph can be considered as a tree or directed acyclic graph, finding those paths is possible, however the relationships in the IFC schema implies that there are possibilities to have undirected circuits - loops - (van Berlo *et al.*, 2021). Therefore, it seems that extracting related objects and data for a selected object in the IFC model is hard to achieve considering the current IFC data schema.

3.4.2.4 Redundant instances in IFC Models

IFC files produces by different software platforms often include considerable amount of redundant information from import and export processes (Du *et al.*, 2020; Sun *et al.*, 2015; Zheng *et al.*, 2024). The direct consequence of redundant data in excessive file size and various studies focus on compressing the IFC file by eliminating redundant data. From an authentication point of view, duplicate instances could cause ambiguity in assigning responsibility.

3.4.2.5 Optional data and elective implementation of the IFC schema in software tools

The IFC Schema contains various optional data elements, moreover, IFC authoring tools, whether native or proprietary, which convert models to IFC based on specific MVDs, may not always populate all required data. When integrating digital signatures into BIM objects, appropriate functionality can resolve this issue by automatically extracting necessary data from the signatory certificate and filling in the relevant properties.

3.5 Conclusion

This research explored the feasibility of integrating digital signatures at the object level within BIMs using the IFC data schema. The goal was to address the need for information exchange and collaboration in the built asset industry by ensuring the authenticity and integrity of BIM data. The investigation identified both promising opportunities and significant challenges associated with this approach.

One promising aspect is the potential for adding a digital signature to the IFC model through an existing entity, providing a foundational basis for incorporating necessary metadata related to digital signatures. However, the highlighted challenges, particularly the extraction of specific objects and their related objects and data in the model poses a critical barrier to integrating digital signature in the IFC model at the object-level. In fact, the current IFC data schema is designed to be optimized for file-based data exchange (van Berlo *et al.*, 2021). There is an ongoing effort to address part of some of these issues by buildingSMART throughout the new version of IFC schema -IFC 5-. Until then, adopting an intermediary solution capable of authenticating objects in an IFC model, independent of the current IFC data schema, may be a more practical approach. The future work of this research will focus on proposing solution in which the digital signatures will add to the IFC file over a container within the file with reference to the selected objects in the model.

Acknowledgments

This work is supported through MITACS Grant IT31364 with the collaboration of buildingSMART Canada and Portage CyberTech. We thank all those involved for their support and collaboration.

CHAPTER 4

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

Mehdi Fakour[a] , Štefan Jaud[b] , Erik A. Poirier[c]

[a,c] Department of Construction Engineering, École de Technologie Supérieure, 1100 Notre-Dame West, Montreal, Quebec, Canada, H3C 1K3
[b] Jaud IT GmbH, Moorenweis, Germany

Paper submitted for publication, May 2025[1]

4.1 Abstract

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

4.2 Introduction

Building Information Model (BIM) is transforming the built asset industry, moving beyond traditional 2D CAD workflows to incorporate data-enriched 3D models (Kaewunruen *et al.*, 2024). Acting as a common standardized language, BIM models streamline collaboration among all project stakeholders, thereby enhancing decision-making, minimizing errors, and improving overall quality (Adepoju, 2022). Nevertheless, BIM adoption can face several notable

[1] This chapter was presented at the EC3 - CIB W78, held in Porto, Portugal, from 7 to 17 July 2025.

challenges as noted by Fakour & Poirier (2024): lack of trust and transparency (Saini *et al.*, 2019), traceability (Celoza *et al.*, 2023), interoperability (Mohammadi *et al.*, 2024), security and integrity of the shared information (Bodea, 2018), professional liability (Arshad *et al.*, 2019), and ownership and intellectual property (IP) rights (Hijazi *et al.*, 2021).

This research aims to address these challenges by investigating the feasibility of integrating digital signatures as a technical mechanism for authentication and data integrity verification in IFC-based exchanges at the object level forming part of a future software toolkit (whose high-level abstract architecture is illustrated in Figure 4.1. This approach can be integrated by BIM practitioners into existing processes, respecting regional regulations and legal frameworks without prescribing who should sign, when in the workflow signing should occur, or which objects must be signed, offering a path toward enhanced trust, data integrity, and security in collaborative built asset projects. Compared to current solutions (Fakour & Poirier, 2024) that primarily operate at the file level—requiring the entire model file to be signed—object-level signing provides greater granularity and flexibility. It allows individual objects to be independently authenticated, thereby ensuring more granular traceability. The IFC standard, chosen for its open format, fosters system-to-system interoperability. While this research focuses on establishing a theoretical approach to integrate digital signatures in BIMs at the object-level, one evident concern is file size expansion if each object is individually signed. Practical performance and scalability considerations remain outside the immediate scope. Also, the scope of the research does not delve into technical details of digital signatures like cryptographic or hashing algorithms.

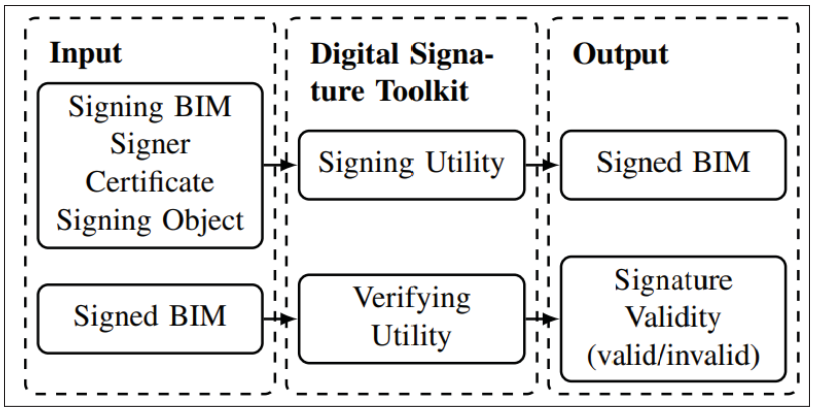

Figure 4.1 The high-level architecture of future BIM digital signature toolkit

4.3 Background

4.3.1 Authentication in data exchange

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

4.3.2 Data integrity

Data integrity can be defined as "*the property whereby data remains unaltered from creation to consumption, ensuring it is not modified in any unauthorized manner during storage or transmission*" (IEEE 802.1AE-2018, 2018). Ensuring data integrity is a fundamental aspect of managing digital information, especially in collaborative and data-intensive environments dealing with sensitive data. Data integrity verification techniques seek to detect unauthorized modifications, confirm data authenticity, and safeguard data reliability. Although these techniques

do not prevent unauthorized alterations, they are essential for identifying and documenting any changes. The common approaches include digital signatures and blockchain technology. Digital signatures are chosen in this research because, compared to alternatives like blockchain, they are simpler to implement and maintain, have broad legal recognition, and can more readily support long-term validation in built asset projects. In contrast, blockchain technology, while decentralized and transparent, involves higher complexity, requires multiple nodes to stay active over an extended period, and entails considerable operational costs (Fakour & Poirier, 2024, 2025).

4.3.3 Digital signature

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

4.3.4 IFC

IFC is an open, vendor-neutral standard data model used to represent data about the built environment (bSI, 2023b; ISO16739-1:2024, 2024) and is adopted to ensure interoperability among various BIM tools. The IFC data schema employs a layered architecture to support

modularity and extensibility (Venugopal, Eastman, Sacks & Teizer, 2012). The IFC schema follows a four-layer architecture: the Resource layer holds foundational definitions like geometry and measures; the Core layer governs core structural entities. The Interoperability layer supports cross-domain interactions; and the Domain layer provides specialized classes for architecture, engineering, and building services (bSI, 2023b; ISO16739-1:2024, 2024).

4.3.5 Information Delivery Specification (IDS)

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

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

4.3.6 Model View Definition (MVD)

MVD is a specialized subset of the IFC schema that specifies the exact entities, attributes, relationships, and properties needed for particular information exchanges (Luttun & Krijnen, 2021). When creating an IFC model in native or proprietary software and exporting it to IFC,

the exported file aligns with the chosen MVD. This alignment ensures that the data conforms to the MVD's specific requirements, thus promoting consistent and accurate information exchange (Luttun & Krijnen, 2021; Lee, Eastman, Solihin & See, 2016a). mvdXML (Chipman *et al.*, 2016) is a data model and format for defining MVDs, ensuring that BIM data exchanges remain structured and consistent for specific use cases (Lee, Shariatfar, Ghannad, Zhang & Lee, 2020; Lee, Eastman & Solihin, 2016b). mvdXML's ConceptTemplate is a modular element that describes relevant entities, attributes, relationships, and properties, thereby minimizing redundancy and promoting uniform data requirements. These templates are reusable, allowing for efficient development of new MVDs and improving accuracy in data exchanges (Lee *et al.*, 2020; Afsari & Eastman, 2016). mvdXML provides the structured format for defining an MVD, while ConceptTemplates serve as the modular building blocks within that format.

4.4 Research methodology

The research methodology as shown in Figure 4.2 began with a series of workshops involving industry practitioners, providing insights into the current gap - identified in Fakour & Poirier (2025) - that no solution currently exists for authentication and data integrity verification at the object level in BIMs. These sessions clarified both the requirements for BIM data authentication and the practical constraints. In addition, the study benefited from the expertise of an industry partner specializing in digital identity and cybersecurity, further refining the scope of research and feasibility considerations. A subsequent literature review examined data integrity practices, authentication mechanisms, and IFC schema details, allowing the identification of common metadata requirements essential for robust authentication and data integrity verification. The next phase involved mapping these metadata elements to the resource layer of the IFC schema—specifically chosen because it hosts foundational entities (e.g., IfcPerson, IfcDateTime) used throughout the entire model. However, since resource layer entities cannot be instantiated directly, a suitable container was needed to encapsulate this information, one capable of encompassing the widest range of non-abstract objects in the IFC data schema. Potential containers were evaluated based on multiple criteria, including their capacity to store

computed digital signatures, support for multiple signatures on a single object (reflecting shared responsibility among multiple engineers), semantic alignment with authentication needs, and practical implementation considerations. As IFC-based models are exchanged adhering to an MVD, the final step addressed how to embed the chosen container within an MVD-based workflow. This goal was achieved by pinpointing a relevant MVD concept template, ensuring that the container could be integrated smoothly during IFC file export or import processes.

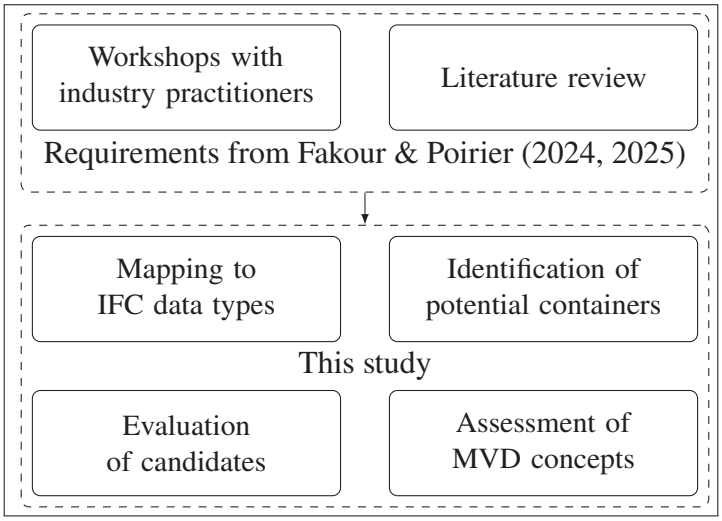

Figure 4.2 The methodology followed in this study building on top of results from Fakour & Poirier (2024, 2025)

4.5 Exchanging digital signatures with IFC

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

thereby maintaining compatibility with existing BIM software and minimizing implementation difficulties (Fakour & Poirier, 2024).

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

4.5.1 Required metadata for digital signatures

Integrating digital signatures necessitates the inclusion of specific metadata that encapsulates essential information about the signer, the signature, and the context of the signing event. Based on common standards and regulations, there can be various optional fields (X.520, 2019) for the metadata included in a digital certificate and digital signature. However, the required metadata generally includes (Fakour & Poirier, 2024):

- Signer Information or Subject (ITU, 2019): Information about the individual or entity owning the digital certificate and signing the data, such as name, organization, and role (X.520, 2019);
- Certificate Issuer (ITU, 2019): Details of the entity issuing the digital certificate used;
- Certificate Validity Period (ITU, 2019);
- Signature Timestamp or Signing Time (ETSI, 2010): The date and time when the signature was applied; and
- Digital Signature Value: Actual calculated hash or similar.

4.5.2 Mapping metadata to the IFC Data Schema

Mapping the required digital signature metadata to the IFC data schema involves identifying suitable existing entities and attributes within the schema that can effectively represent this

information. The IFC data schema provides standardized entities and attributes that can be leveraged for this purpose in the resource layer (bSI, 2023b).

Table 4.1 illustrates a summary of how each piece of required metadata can be effectively mapped to existing elements within the IFC data schema. While individual metadata elements can be represented in various parts of the IFC schema, the challenge lies in finding a container that can encapsulate all these elements cohesively and support connection with other elements in the IFC data exchange.

Table 4.1 Mapping of required digital signature metadata to IFC data schema entities and types (Fakour & Poirier, 2024)

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

4.5.3 Candidate containers for integrating digital signatures within the IFC Data Schema

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

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

4.5.3.1 IfcApproval

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

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

In terms of connection to other entities as illustrated in Figure 4.3 , IfcApproval can be associated with IfcRelAssociatesApproval, which connects to IfcDefinitionSelect and subsequently to IfcObjectDefinition and IfcPropertyDefinition. However, in the current IFC data schema, relationships defined via IfcRelationship cannot be connected to IfcApproval. This is significant because relationships in IFC-based models are treated as objects—meaning each one may require a signature in its own right. IfcApproval is capable of direct storage of the digital signature and all required metadata, support for multiple signatures on the same object via multiple

IfcApproval instances which can be linked through IfcApprovalRelationship, semantic alignment with approvals and verifications, and practical implementation using existing schema entities.

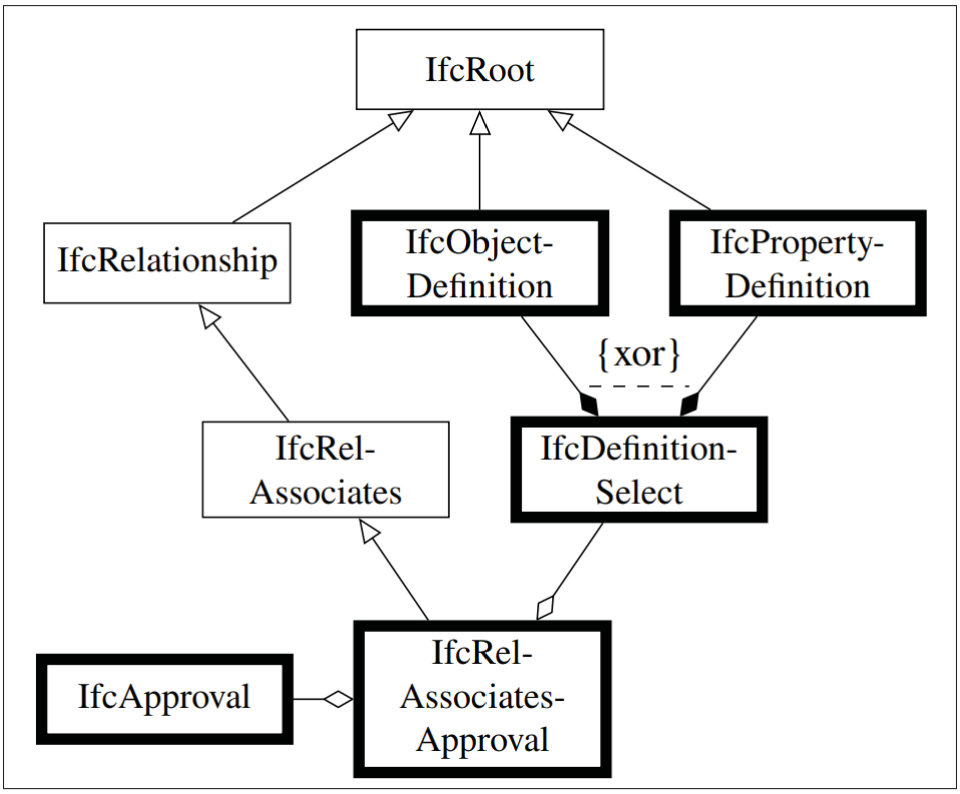

Figure 4.3 Relationship diagram for IfcApproval to IfcRoot in IFC data schema

4.5.3.2 IfcOwnerHistory

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

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

- Signer Information is partially represented by OwningUser.

- Certificate Validity Period and Signature Timestamp are represented by LastModifiedDate or CreationDate.

In terms of its connection to other entities in the IFC data schema, the optional attribute OwnerHistory of the entity IfcRoot employs IfcOwnerHistory type as shown on Figure 4.4. Consequently, it is directly referenced by IfcRoot and thus available to all derived entities. However, IfcOwnerHistory has several limitations: it lacks fields for detailed digital signature metadata (e.g., certificate information, signature value), it only allows one instance per IfcRoot (cardinality constraint), and it is primarily intended for ownership tracking rather than approvals or signatures.

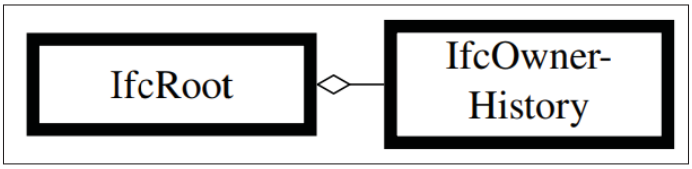

Figure 4.4 Relationship diagram for IfcOwnerHistory to IfcRoot in IFC data schema

4.5.3.3 IfcObjectReferenceSelect

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

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

In terms of its connection to other entities in the IFC data schema, IfcObjectReferenceSelect is associated through IfcPropertySet and IfcRelDefinesByProperties to IfcObjectDefinition as

illustrated in Figure 4.5. However, IfcObjectReferenceSelect is not connected to IfcRelationship and IfcPropertyDefinition, therefore if it is used as container for digital signature, relationships and property definitions cannot be signed. Moreover, the limitations of IfcObjectReferenceSelect include indirect storage of digital signature data requiring referencing other entities, complexity in managing and retrieving signature data, and less semantic alignment with digital signatures.

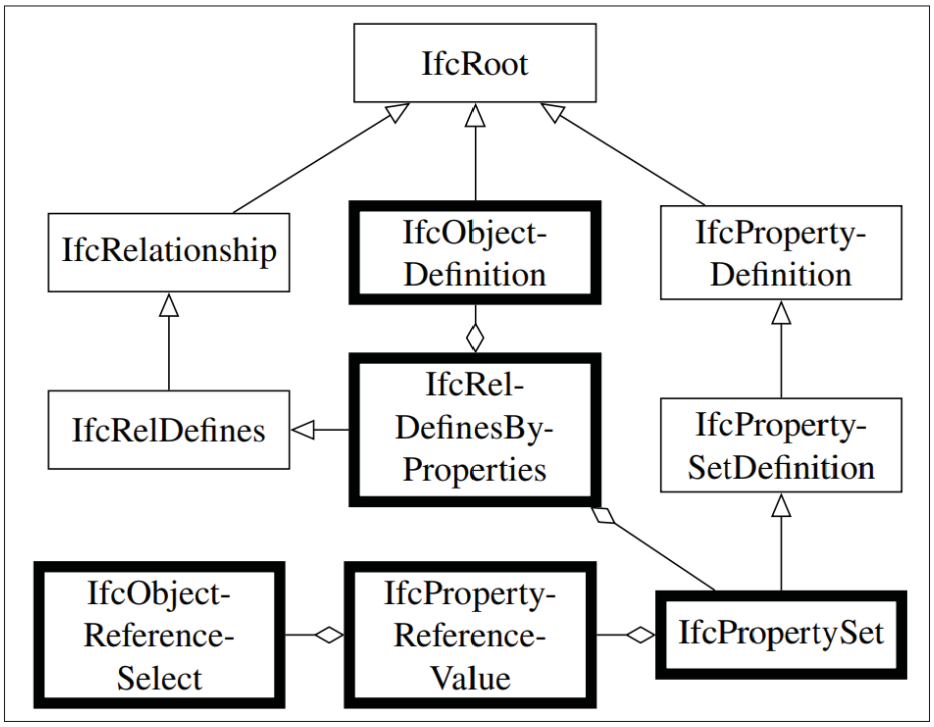

Figure 4.5 Relationship diagram for IfcObjectReferenceSelect to IfcRoot in IFC data schema

4.5.4 Comparative analysis of candidate containers

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

is essential. The evaluation is conducted against parameters derived from Fakour & Poirier (2024, 2025) research and the core requirements of a robust digital signing solution.This evaluation considers their ability to store all required metadata and other optional metadata, support multiple signatures, relation with the broad range of entities, and semantic alignment with digital

signatures. A summary of this comparison is presented in Table 4.2, highlighting the strengths and limitations of each container for digital signatures.

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

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

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

4.5.5 Integration of the chosen container into model based data exchange

To associate the chosen container with specific objects, two main possibilities arise: developing an IDS or an MVD. While IDS provides a lightweight means of defining information requirements, its current facets (e.g., PartOf and Property) primarily address simpler relationships and do not readily support more complex constructs like IfcRelAssociatesApproval or reference-based properties such as IfcPropertyReferenceValue. Consequently, IDS cannot handle deeply nested entities or general associations within the IFC data schema without further extensions. Given these limitations as shown in Table 4.3, this research instead adopts an MVD-based approach.

Table 4.2 Comparison of candidate containers for integrating digital signatures into IFC data schema

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

Table 4.3 Comparison of IDS and MVD capabilities to associate digital signature candidate containers to specific objects

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

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

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

4.6 Conclusions

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

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

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

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

Acknowledgments

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

CHAPTER 5

FRAMEWORK FOR EMBEDDING DIGITAL SIGNATURES IN IFC-BASED BIMS FOR AUTHENTICATION AND DATA INTEGRITY VERIFICATION AT THE OBJECT-LEVEL

Mehdi Fakour[a] , Štefan Jaud[b] , Erik A. Poirier[c]

[a,c] Department of Construction Engineering, École de Technologie Supérieure, 1100 Notre-Dame West, Montreal, Quebec, Canada, H3C 1K3
[b] Jaud IT GmbH, St.-Sixtus-Straße 6, 82272, Moorenweis, Germany

Paper submitted for publication, May 2025[1]

5.1 Abstract

Ensuring data integrity and authentication at the object level within Building Information Models (BIMs) is critical for enhancing trust and collaboration in the built asset industry. File-level security measures are inadequate for granular control, leading to unauthorized modifications and data inconsistencies. This paper addresses the necessity of object-level authentication in BIMs and proposes a practical solution utilizing digital signatures.

This research establishes the necessity for object-level authentication, defines the requirements of an ideal solution, and develops a framework that leverages digital signatures for object-level data integrity in BIMs. The proposed solution focuses on the widely adopted IFC-SPF format while ensuring compatibility with other formats.

The solution addresses challenges associated with the IFC schema by utilizing a method independent of the IFC data schema. By enhancing data integrity and authentication in BIMs, it promotes trust among stakeholders while maintaining performance and minimal disruption, contributing to improved practices in the built asset industry.

---

[1] This paper has been submitted as an article for publication to Automation in Construction. Submitted on May 05, 2025. Manuscript Number: AUTCON-D-25-01866.

5.2 Introduction

The built asset industry has witnessed a transformative shift with the advent of BIMs, "a digital representation of physical and functional characteristics of facilities" (Liu & Xie, 2014; Vitiello *et al.*, 2019). BIM facilitates coordination and collaboration (Sun, Jiang, Skibniewski, Man & Shen, 2017), and increases productivity and efficiency (Sun *et al.*, 2017; Ibrahim, Shariff, Esa & Rahman, 2019) across the building life-cycle. However, as BIM models become increasingly complex, ensuring the integrity and authenticity of the data within these models emerges as a critical concern, especially in collaborative digital workflows. Unauthorized modifications, data inconsistencies, and lack of accountability can lead to significant project risks, including design flaws, construction errors, and legal disputes. This issue is particularly pressing when the model is intended to serve as a legal document.

Digital signatures present a robust solution for data integrity and authentication. By allowing stakeholders to cryptographically sign individual objects or groups of objects, digital signatures ensure non-repudiation and enable detection of unauthorized alterations. This approach aligns with industry best practices and legal frameworks that recognize digital signatures as valid methods of verification.

Current data management methods in BIM often focus on file-level security, which is insufficient for granular control and verification of individual model components. This limitation hinders the ability to precisely attribute responsibility, track changes, and maintain trust among stakeholders. The need for object-level data integrity and authentication becomes paramount to address these challenges, promoting transparency, accountability, and reliability in collaborative environments.

The Industry Foundation Classes (IFC), as part of the openBIM initiative, offer an open, standardized, and interoperable data format widely adopted in the built asset industry. Leveraging IFC facilitates the development of solutions compatible with various software platforms and enables integration into existing workflows with minimal disruption. The comprehensive data schema and extensible architecture of IFC make it an ideal foundation for implementing object-level digital signatures.

5.2.1 Research objectives

This study focuses on addressing three key research questions, aiming to develop a comprehensive understanding and practical solution for object-level data integrity and authentication in IFC-based BIMs:

1. What are the requirements and characteristics of an ideal solution for object-level data integrity and authentication in IFC-based BIMs?
2. What is a practical solution for implementing object-level data integrity and authentication in IFC-based BIMs?

5.2.2 Limitations and scope

While this research aims to propose a comprehensive solution for object-level data integrity and authentication in BIM using digital signatures, certain limitations are acknowledged to define the scope and focus of the study.

The solution is designed to be modular and independent of specific cryptographic algorithms. Details of hashing and cryptographic algorithms, including their steps, security, and performance, are beyond the scope of this research. This allows for more modular design and flexibility in choosing or updating algorithms without affecting the overall system.

The research does not specify methodologies for selecting which objects to sign within a BIM model. This decision is context-dependent and varies based on project requirements and stakeholder responsibilities. In fact, the proposed solution is aimed to be flexible enough to fulfill technical requirements and create the possibility for experts in each required domain to decide over business or process related requirements.

Detailed strategies for integrating the proposed solution into specific existing BIM software tools are not provided. The focus is on developing a standalone solution that aligns with industry standards, which can be adapted for integration in future work.

The solution aims to enhance current BIM processes without introducing significant changes. It is designed to align with existing workflows, ensuring minimal disruption and promoting adoption.

5.2.3 Significance of the research

By developing a software toolkit that employs digital signatures for object-level data integrity and authentication in BIM, this research addresses a critical need in the built asset industry. The proposed solution enhances trust, accountability, and collaboration among stakeholders while maintaining performance and minimizing disruptions to existing workflows. Focusing on IFC and ensuring compatibility across formats promotes widespread adoption and facilitates collaboration and interoperability.

This work bridges the gap between theoretical frameworks and practical implementation, providing a framework for integrating authentication mechanisms into BIM processes. It supports the industry's progression toward more secure, reliable, and interoperable digital practices, ultimately improving project outcomes, trust and transparency.

5.2.4 Structure of the paper

The paper begins by outlining the rationale for authenticating and verifying the integrity of BIM data at the object level. Section 5.3 continues with an in-depth look at key concepts such as data integrity, verification techniques, and digital signatures, setting the foundation for the proposed solution. It then reviews current solutions and their limitations.

A concise overview of the research methodology is provided in section 5.4 , explaining how Design Science Research, an extensive literature review, and working meetings with industry experts shaped both the requirements and the artifact itself.

Next, section 5.5 outlines the characteristics and requirements of an ideal approach, informed by literature, expert insights, and practical considerations. Then section 5.6 introduces the

design and implementation of the proposed solution, including a performance evaluation and comparison with initial alternatives.

Finally, section 5.7 reflects on how the solution aligns with previously defined requirements, and concludes with future directions for extending this work.

5.3 Background

BIMs has transformed the built asset industry by enabling the creation and management of digital representations of physical and functional characteristics of facilities. As BIM adoption increases, ensuring the authenticity and integrity of BIM data becomes critical, especially in the context of digital delivery and collaborative digital workflows. This section provides a background on the imperative of authenticating BIMs, explores data integrity verification techniques, reviews current solutions, and discusses the IFC different serializations.

5.3.1 The importance of BIMs authentication and data integrity verification

BIM has significantly enhanced collaboration and information sharing in the construction industry (Jallow *et al.*, 2014). However, several issues underscore the necessity of authenticating and ensuring the integrity of BIM data for successful adaptation and implementation of BIM throughout the projects. Authenticating BIMs at the object level is critical for several reasons that significantly impact the construction industry's efficiency, legal compliance, and collaborative processes.

Ensuring data integrity addresses trust issue (Hijazi *et al.*, 2021; Saini *et al.*, 2019; Deng *et al.*, 2019; Yushasman, Rizal, Lee & Rahman, 2024) among stakeholders by verifying that the information is accurate and unaltered, which is essential for effective collaboration (Hijazi *et al.*, 2021; Saini *et al.*, 2019). It mitigates traceability issues (Celoza *et al.*, 2023; Bodea, 2018; Hijazi *et al.*, 2021; Deng *et al.*, 2019) by allowing the tracking of changes to specific components throughout the project life cycle, supporting accountability and legal auditability (Bodea, 2018).

Maintaining data integrity in BIMs reduces the risk of errors due to miscommunication, facilitating accurate communication and collaboration among project participants (Arensman & Ozbek, 2012). It supports overcoming potential system to system (Turk, 2020) interoperability issues (Oluwole Alfred,OLATUNJI, 2011; Abd Jamil & Fathi, 2020; Alwash *et al.*, 2017; Mohammadi *et al.*, 2024; Hijazi *et al.*, 2021) by ensuring consistent data exchange across different systems, which is vital for seamless integration among various software applications used in the industry.

Authenticating BIMs also addresses professional liability concerns (Alwash *et al.*, 2017; Arensman & Ozbek, 2012; Arshad *et al.*, 2019; Celoza *et al.*, 2023) by clearly identifying responsible parties for each element within the model, thus reducing legal disputes and enhancing accountability. It safeguards ownership and intellectual property rights (Oluwole Alfred, 2011; Abd Jamil & Fathi, 2020; Alwash *et al.*, 2017; Arensman & Ozbek, 2012; Arshad *et al.*, 2019; Bodea, 2018; Mohammadi *et al.*, 2024; Hijazi *et al.*, 2021) issues by establishing ownership and proper attribution of contributions. Ensuring BIM integrity is essential for compliance with regulatory requirements and industry standards, confirming that data meets necessary requirements be relied upon as legal document (Oluwole Alfred, 2011; Alwash *et al.*, 2017; Arshad *et al.*, 2019; Mohammadi *et al.*, 2024).

5.3.2 Data integrity

Data integrity refers to the maintenance and assurance of the accuracy, consistency, and reliability of data over its entire life-cycle, ensuring that data remains unaltered and trustworthy from creation to consumption (IEEE 802.1AE-2018, 2018; Cawthra, Ekstrom, Lusty, Sexton & Sweetnam, 2020; Nieles, Dempsey & Pillitteri, 2017).

In the context of BIM, data integrity is of paramount importance due to the collaborative nature of construction projects. BIM models serve as a single source of truth (Hijazi *et al.*, 2021) for all project information. Maintaining data integrity ensures that all participants have access to accurate and consistent information, which is essential for effective collaboration

and decision-making (Gu, Singh & Wang, 2010; Park, 2024; Preidel, Borrmann, Mattern, König & Schapke, 2018).

Maintaining data integrity entails ensuring that data is accurate and consistent over time (Sumukha Krishna, Hemanth Kumar & Gangadharappa, 2020; Raglin & Moraffah, 2023; Lakshmi Triveni, Balamuralidhara & Pramod Kumar, 2017), complete by capturing all necessary information without omissions (Raglin & Moraffah, 2023; Zhang & Chen, 2010), reliable by remaining dependable and free from corruption or unauthorized alterations (Raglin & Moraffah, 2023; Decker, 2009), and traceable by documenting the origin and history of any modifications (Zhang & Chen, 2010; Longhurst, 2010).

To uphold these characteristics of data integrity consistently, a set of guiding principles has been established. One of the most widely recognized frameworks is the ALCOA principle, which originated from regulatory guidelines in the pharmaceutical industry, particularly from the U.S. Food and Drug Administration (FDA) (FDA, 2018; Sumukha Krishna *et al.*, 2020; Sabale *et al.*, 2024; Kavasidis *et al.*, 2023; Jaiswal, Muddukrishna & Kulyadi, 2020). The ALCOA acronym stands for Attributable, Legible, Contemporaneous, Original, and Accurate. These principles have been further expanded to ALCOA++ to include Complete, Consistent, Enduring, and Available, addressing additional aspects crucial for data integrity (Sumukha Krishna *et al.*, 2020; Sabale *et al.*, 2024; Kavasidis *et al.*, 2023; Jaiswal *et al.*, 2020).

the short description of these principles are presented as follows:

- Attributable: Every piece of data should clearly indicate who recorded it and when. This ensures accountability and traceability (Kavasidis *et al.*, 2023; Charitou, Lallas, Gerogiannis & Karageorgos, 2024).
- Legible: Data must be recorded permanently in a clear and readable manner. Legibility ensures that data can be accurately interpreted now and in the future (Kavasidis *et al.*, 2023; Charitou *et al.*, 2024).

- Contemporaneous: Information should be documented at the time the activity occurs.This ensures that the data is accurate and reflects the actual events (Kavasidis *et al.*, 2023; Charitou *et al.*, 2024).
- Original: Original records or verified true copies should be maintained. This preserves the authenticity of the data (Kavasidis *et al.*, 2023; Charitou *et al.*, 2024).
- Accurate: Data must be correct, truthful, and free from errors. This principle ensures the reliability of the data (Kavasidis *et al.*, 2023; Charitou *et al.*, 2024).
- Complete: All data, including any repeat or reanalysis, should be included. Completeness ensures no information is lost (Charitou *et al.*, 2024; Sabale *et al.*, 2024).
- Consistent: Data should be presented in a consistent manner, following the same format and standards throughout its life-cycle (Charitou *et al.*, 2024; Sabale *et al.*, 2024).
- Enduring: Data should be recorded on durable media and preserved for the required retention period. This ensures that data remains accessible and intact over time (Charitou *et al.*, 2024; Sabale *et al.*, 2024).
- Available: Data should be readily accessible for review and audit throughout its retention period. This ensures that data can be retrieved when needed (Charitou *et al.*, 2024; Sabale *et al.*, 2024).

By integrating these characteristics and principles, organizations can establish robust data integrity practices. This integration ensures that BIM data remains trustworthy and can be confidently used by all stakeholders involved in a project.

5.3.3 Data integrity verification techniques

To verify data integrity, several techniques are employed. These techniques help detect unauthorized changes, ensure data has not been corrupted, and confirm the authenticity of the data source. It is worth noting that these techniques are unable to prevent unauthorized alternation. Digital signatures and blockchain technology are primary data integrity verification techniques.

5.3.3.1 Digital signatures

A digital signature is a mathematical mechanism that enables the verification of the authenticity and integrity of digital data (Rai *et al.*, 2023; Seetha, 2017). It is based on public key infrastructure (PKI), where the sender signs a message digest (hash) of the document using their private key, and the recipient verifies it using the sender's public key (Kishore, Raina, Nayar & Thakur, 2021; Rai *et al.*, 2023). Digital signatures ensure that the data originates from a known sender (authentication) (Ramadhan, Mandala & Yulianto, 2023; Kishore *et al.*, 2021), has not been altered (integrity) (Ramadhan *et al.*, 2023; Mogos, 2008), and that the sender cannot repudiate the authorship of the signed content (non-repudiation) (Kishore *et al.*, 2021; Rai *et al.*, 2023).

The process of creating a digital signature begins with the data to be signed undergoing a cryptographic hash function (Rai *et al.*, 2023). The signer then encrypts this hash value using their private key, creating the digital signature (Rai *et al.*, 2023). The private key is securely held by the signer, ensuring that only they can generate their signature. The original data and the digital signature are then transmitted to the recipient. The recipient performs the verification process by computing the hash value of the received data using the same hash function used by the signer (Rai *et al.*, 2023). Next, the recipient decrypts the digital signature using the signer's public key, which is publicly available and often provided via a digital certificate issued by a trusted Certificate Authority (CA) (Rai *et al.*, 2023; Kishore *et al.*, 2021). This decryption yields the hash value originally computed by the signer. If the hash value computed from the received data matches the decrypted hash value, the recipient can confirm that the data has not been altered and that it was signed by the holder of the private key (Rai *et al.*, 2023; Kishore *et al.*, 2021).

5.3.3.2 Blockchain technology

Blockchain is a decentralized, distributed ledger technology that records transactions across a network of computers, ensuring that records cannot be altered retroactively without the alteration

of all subsequent blocks and the consensus of the network (Guru, Perumal & Varadarajan, 2021; Kabiri & Sharifzadeh, 2022; Alketbi, Nasir & Abu Talib, 2020).

Blockchain's key characteristics include decentralization, immutability, transparency, and security. Decentralization ensures that the ledger is maintained across multiple nodes with equal authority, eliminating a single point of control (Guru *et al.*, 2021; Kabiri & Sharifzadeh, 2022). Immutability means that once data is recorded, it cannot be altered without affecting all subsequent blocks and requiring network consensus, thus ensuring data integrity (Kabiri & Sharifzadeh, 2022; Ghiro *et al.*, 2021). Transparency allows all participants to view transactions, promoting trust within the network (Kabiri & Sharifzadeh, 2022; Ghiro *et al.*, 2021). Security is provided through cryptographic techniques that protect data and transactions from unauthorized access (Kabiri & Sharifzadeh, 2022; Dong, Yaqiong, Huaiguang & Duan, 2022).

Based on (Guru *et al.*, 2021; Kabiri & Sharifzadeh, 2022; Xu *et al.*, 2024) the overall process in a blockchain begins when a user initiates a transaction, which is then broadcast to the network. Network nodes validate the transaction using consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS). Once validated, the transaction is grouped into a block, which is added to the blockchain in a linear, chronological order. Each block contains a cryptographic hash of the previous block, linking them together and ensuring that any alteration in a block would invalidate all subsequent blocks. The updated blockchain is then distributed across the network, ensuring consistency among participants.

Despite its advantages, blockchain faces several challenges. Scalability remains a significant concern (Guru *et al.*, 2021; Kim, 2020), as handling a large number of transactions efficiently is difficult, leading to slower processing times and higher operational costs. Interoperability between different blockchain systems and integration with traditional systems is complex, hindering broader adoption (Guru *et al.*, 2021). Balancing transparency with user privacy is challenging (Ghiro *et al.*, 2021); while transparency promotes trust, it can conflict with the need for confidentiality. Security vulnerabilities, such as denial-of-service attacks, also exist despite the overall robustness of blockchain technology (Guru *et al.*, 2021). Additionally, regulatory

and legal frameworks are still evolving, creating uncertainty and potential compliance issues (Dong *et al.*, 2022; Jayawardhana & Colombage, 2020).

5.3.3.3 Comparative analysis of data integrity verification techniques

Digital signatures and blockchain technology are prominent techniques used for verifying data integrity. A comparative analysis of these methods highlights their suitability for BIM applications based on factors such as legal acceptance, implementation complexity, maintenance, long-term validation, efficiency, and other relevant aspects.

Digital signatures provide a well-established method for data integrity verification by generating a unique hash of the content, which is encrypted with the sender's private key (Rai *et al.*, 2023; Sagar Hossen *et al.*, 2021) and authenticate the signer and the content using public-key cryptography (Rai *et al.*, 2023; Sagar Hossen *et al.*, 2021; Khan, Gupta & Gola, 2017). They are widely accepted in legal frameworks and are supported by international standards, making them suitable for compliance with regulatory requirements (Iswari & Rudy, 2023). The implementation and maintenance of digital signatures are relatively straightforward, requiring a PKI for key management (Rai *et al.*, 2023; Sagar Hossen *et al.*, 2021). They require Low maintenance once implemented (Rai *et al.*, 2023; Sagar Hossen *et al.*, 2021). Digital signatures offer long-term validation capabilities, as digital signatures can be timestamped and verified even after the original signing keys have expired, provided that appropriate archival processes are in place.

Blockchain provides immutable records of transactions, ensuring data integrity and authentication through consensus mechanisms and cryptographic hashes (Sabeena & Vijila, 2024; B. Rawat, Chaudhary & Doku, 2021; Lakshmanan & Anandha Mala, 2024). However, legal acceptance of blockchain is still emerging, with regulatory frameworks varying across jurisdictions (B. Rawat *et al.*, 2021; Phansalkar, Mishra, Chaube & Sonkamble, 2023; Perera *et al.*, 2020). The complexity of implementing and maintaining a blockchain network is high, involving the setup of distributed networks, consensus algorithms, and potentially smart contracts (Sabeena & Vijila,

2024; Lakshmanan & Anandha Mala, 2024; B. Rawat *et al.*, 2021). Scalability issues arise due to the size of data and the overhead of consensus mechanisms (Sabeena & Vijila, 2024; Lakshmanan & Anandha Mala, 2024; B. Rawat *et al.*, 2021). Long-term validation is inherent in blockchain, as the ledger is designed to be persistent and tamper-proof (Sabeena & Vijila, 2024; Lakshmanan & Anandha Mala, 2024; B. Rawat *et al.*, 2021). However, maintaining blockchain network over long period of time is expensive due to high transaction fees, increasing storage costs, and significant operational costs. Efficiency can be a concern, as blockchain networks may experience latency and require significant computational resources (Zheng *et al.*, 2018).

Other aspects to consider include interoperability, scalability, and security. Digital signatures are highly interoperable with existing systems and standards (Rai *et al.*, 2023), making them easy to integrate into current BIM workflows. Blockchain technology poses significant interoperability hurdles, as all participants must adopt the same blockchain platform, and integration with existing BIM software may be complex. In terms of scalability, digital signatures scale well for individual files. Blockchain scalability is limited by network capacity and consensus algorithms, which can hinder performance in large-scale applications (Croman *et al.*, 2016).

Table 5.1 Comparison of data integrity verification techniques

Aspect	**Digital Signatures**	**Blockchain Technology**
Data Integrity	Ensures data has not been altered using cryptographic hashes	Provides immutable record through cryptographic linking
Authentication	Verifies identity of the signer (non-repudiation of the source)	Non-repudiation of Origin and Non-repudiation of Receipt
Legal Acceptance	Widely accepted	Emerging acceptance
Implementation Complexity	Moderate	High
Maintenance Complexity	Low to moderate	High
Long-Term Validation	Supported	Inherent
Scalability	Scales well	Limited scalability
Interoperability	High; compatible with existing systems and standards	Low to moderate; interoperability challenges
Security	Strong cryptographic security	Strong security but potential vulnerabilities exist
Suitability for BIM	High	Variable; promising but faces significant challenges

Given these considerations which are summarized in Table 5.1, digital signatures emerge as the preferable choice for this research. They offer strong data integrity assurance and authentication, fulfilling both technical and legal requirements essential for BIM applications.

5.3.4 Current solutions for authentication and data integrity verification in built asset industry

Ensuring authentication, data integrity, and clear responsibility assignment in digital models is crucial across various industries, including construction, manufacturing, and aerospace. Current practices and research offer various solutions, each with its advantages and limitations. This section examines current solutions used in practice and academia, analyzing their effectiveness based on criteria such as level of authentication, traceability, complexity of implementation, and suitability for long-term archival and retrieval (LOTAR).

A common approach involves using standards focused on interoperability and data preservation while aiming to secure data origin and integrity. These standards often use containers or packages that encapsulate original files along with metadata. For example, the PDF/A-3 standard allows embedding files within PDF documents for long-term archiving and includes features that support embedding digital signatures and revocation information (PDF/A-3, 2020; ISO32000-1:2008, 2008). Similarly, ISO 21597-1:2020 (ISO21597-1:2020, 2020) specifies creating an Information Container for linked Document Delivery (ICDD), facilitating the exchange of linked files in construction projects.

In the aerospace industry, standards such as ARINC827-1 and ARINC835-1 are used for the secure exchange of software parts and data. ARINC827-1 defines the "Electronic Distribution of Software by Crate (EDS Crate)", which creates a container or "crate" that holds the required files for distribution (ARINC827-1, 2020). ARINC835-1 provides guidance on securing loadable software parts using digital signatures, ensuring the integrity and authenticity of the software components exchanged (ARINC835-1, 2014).

In the approaches mentioned above, digital signatures are applied to the container or list of files, but not to the individual files within. This means that while the container's integrity can be verified, unauthorized changes to the files inside may go undetected.

Another practice in BIM based project is using Common Data Environments (CDEs) which serve as centralized repositories for storing and managing project data. CDEs support collaborative workflows by providing access control, versioning, and auditing capabilities (ISO19650-1, 2018). However, authentication and data integrity are often applied at the file level, and CDEs may lack mechanisms for object-level authentication within BIM models.

Moreover, given the extended life cycles of built asset projects—from design through decommissioning—any CDE-based data management mechanism used for LOTAR must remain sustainable over the long term, thereby increasing its complexity and ongoing maintenance costs.

Blockchain technology has been proposed to enhance trust and transparency in data exchange. BIMCHAIN, for example, is a blockchain-based application enabling multi-signature and time-stamped data exchanges for BIM models (Bimchain, 2018; Pradeep *et al.*, 2020). Operating at the file level, it can detect if a file has been modified but cannot identify specific changes within the file. The research has looked at tracking differential changes on BIM objects using a semantic differential transaction model to minimize information redundancy (Xue & Lu, 2020). However, this method faces challenges when multiple stakeholders modify the same object. Moreover, the complexity of implementing blockchain solutions can hinder adoption.

Embedding digital signatures directly within 3D models in model-based manufacturing has been explored to achieve object-level authentication and traceability. Hedberg, Krima & Camelio (2017) and Hedberg,Thomas, Helu, Krima & Barnard Feeney (2020) propose using X.509 digital certificates embedded in models, enabling multiple experts to assume responsibility for specific objects or to endorse each other's work. While this method provides strong authentication and traceability at the object level, it requires significant changes to existing data schemas which are used in data exchange. Table 5.2 represents a comparative summary of current authentication solutions.

Table 5.2 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, time-stamped 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

5.3.5 IFC Data Schema and IFC serializations

The IFC data schema is a standardized, open, and vendor-neutral data model designed to facilitate interoperability in BIMs across various applications and domains within the build asset industry (Venugopal *et al.*, 2012; Borrmann, Beetz, Koch, Liebich & Muhic, 2018; Antunes,

César,Júnior, Ribeiro, Oliveira & Carvalho, 2024). It is comprehensive and extensible, defining entities, attributes, and relationships to represent building components and their interactions (Venugopal *et al.*, 2012; Borrmann *et al.*, 2018; Antunes *et al.*, 2024). The schema is specified as a UML class diagram delivered in XMI format; from this master description an EXPRESS schema compliant with ISO 10303-11 is generated, together with additional machine-readable representations in XSD, RDF/OWL, and JSON (bSI, 2023b).

The IFC schema is organized hierarchically to support extensibility, data extraction, and ease of implementation. This hierarchical structure allows for the representation of complex building elements and their relationships in a structured manner (Dong, Lam, Huang & Dobbs, 2007; Shi, Liu, Gao, Gu & Li, 2018). IFC employs an object-oriented approach, where building elements are defined as objects with attributes and relationships. This method supports the creation of detailed and interconnected models of building components (Park, Chen & Cho, 2020).

IFC data can be stored and exchanged using several file formats, each used to cater to different needs and preferences within the BIM community. The main official IFC file formats are: IFC-SPF (STEP Physical File) Format, IFC-XML Format, and IFC-ZIP Format (bSI, 2024). Below is a detailed explanation of each format, their applications, and a comparison in terms of usability, file size, interoperability, and other relevant aspects.

5.3.5.1 IFC-SPF Format

The IFC-SPF format, also known as IFC STEP or IFC SPF, is the most widely used format for storing and exchanging IFC data. It is based on the ISO 10303-21 standard (bSI, 2024; Roddis, Matamoros & Graham, 2006; Laakso, 2009) , which specifies the STEP (Standard for the Exchange of Product Model Data) physical file format (Kassim, Yusof & Awang, 2016). Files in this format have the extension .ifc. In fact, IFC-SPF files are plain text files that represent data using a line-by-line structure. Each line typically corresponds to an entity instance, defined by a unique identifier and a set of attribute values. The plain text nature of IFC-SPF files makes them human-readable to some extent, allowing users to open and inspect the files using a text

editor. However, the files can become quite large and complex with redundant data (Sun *et al.*, 2015), making manual interpretation impractical for extensive models as well as impacting in their efficiency in data storage and exchange.

5.3.5.2 IFC-XML Format

The IFC-XML format represents IFC data using the Extensible Markup Language (XML), following the ISO 10303-28 standard. Files in this format have the extension .ifcXML (bSI, 2024). IFC-XML encodes the IFC schema in XML format using XML tags and elements, making it compatible with web-based applications and easier to parse compared to the traditional STEP file format (Afsari, Eastman & Castro-Lacouture, 2017; Baranova, 2021). IFC-XML is suitable for applications that utilize XML parsing and processing, such as web-based data transfer, supporting cloud-based BIM applications (Afsari *et al.*, 2017), web services, data integration platforms, and systems that leverage XML-based technologies. XML's self-describing nature enhances readability and allows for easier data manipulation using standard XML tools and libraries. However, the verbosity of XML leads to larger file sizes compared to IFC-SPF by a factor of magnitude (Frei, 2019).

5.3.5.3 IFC-ZIP Format

The IFC-ZIP format compresses IFC-SPF or IFC-XML files into a ZIP archive, reducing file size. Files in this format have the extension .ifcZIP. An IFC-ZIP file contains a single IFC-SPF or IFC-XML file compressed using standard ZIP compression algorithms (bSI, 2024). In fact, combining IFC with ZIP compression could significantly reduce the file size, making it easier to store, share, and transmit BIM data (Sun *et al.*, 2015; Xu, Kim & Chen, 2022).

5.3.5.4 Comparison of IFC File Formats

A comparative summary of the IFC file formats is presented in Table 5.3. This research primarily focused on the IFC-SPF format for its widespread adoption which results in higher degree of

interoperability between software tools. However, the importance of supporting other formats is also recognized to ensure flexibility and adaptability of the solution.

Table 5.3 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	Standardized; ISO 10303-21	Standardized; ISO 10303-28	Uses standard ZIP compression; underlying format standardized

5.4 Research methodology

This research as illustrated in Figure 5.1 employs Design Science Research Methodology (DSRM) as a methodological framework. DSRM provides a structured framework for developing and evaluating the proposed solution. The DSRM process encompasses problem identification, defining objectives, design and development of the artifact, demonstration, evaluation, and communication (Hevner *et al.*, 2004; Peffers *et al.*, 2007).

Across these phases, the research benefited from three complementary methods. First, a thorough literature review helped establish a foundation for identifying technical and industry-aligned requirements. Second, a series of nine working meetings brought together a diverse group of BIM practitioners—including representative from three U.S. Departments of Transportation, two BIM software developers, a BIM consultant, two academic experts in OpenBIM and IFC, a buildingSMART International technical expert, and two advisors from buildingSMART Canada. These sessions played a crucial role in shaping and validating the design decisions. Lastly,

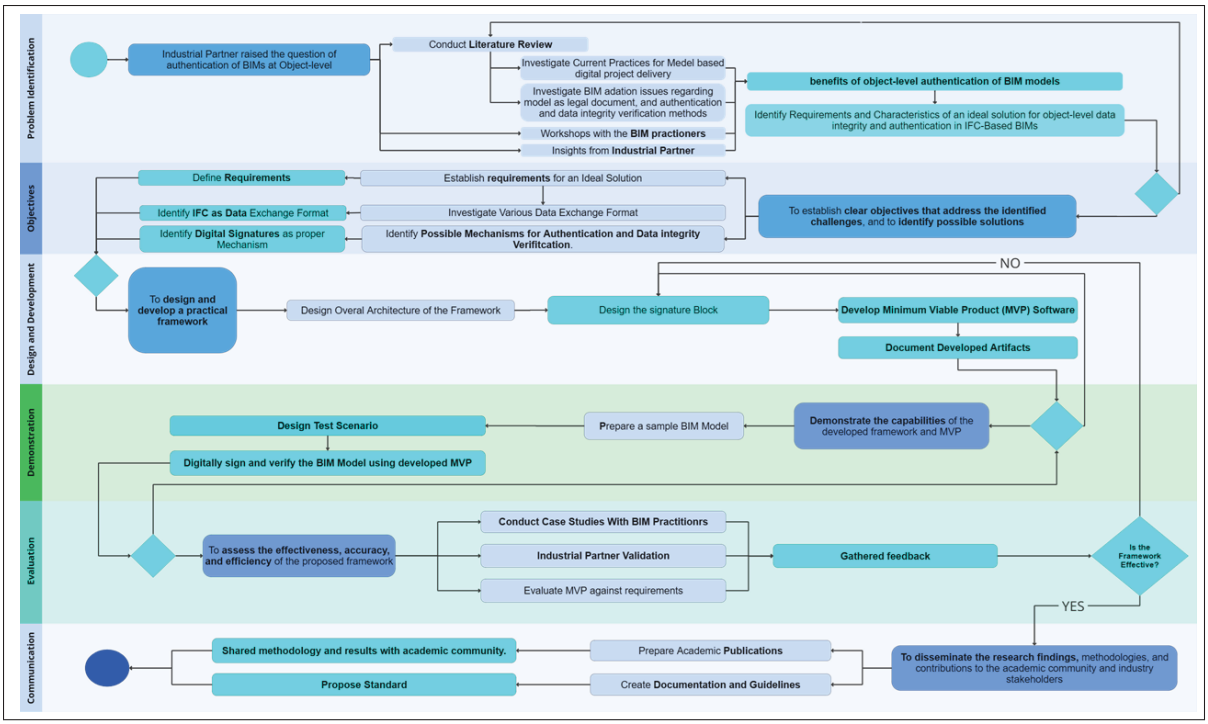

Figure 5.1 Overall structure of the research methodology

ongoing collaboration with an industry partner specialized in digital identity and cybersecurity ensured the proposed solution remained both practical and technically robust.

The research began with an inquiry from an industrial partner concerning the feasibility of authenticating BIMs at the object level. A literature review was subsequently conducted to explore model-based delivery practices, procurement approaches, legal issues in BIM, and existing solutions. These findings, together with insights from the industrial partner and BIM practitioners, informed a set of requirements for an IFC-based solution that would maintain data integrity without substantially disrupting current workflows.

Building on these requirements, an overall architecture for an object-level authentication solution was designed. A signature block was conceived through 2 rounds of developments and testing, and integrated into a minimum viable product (MVP) software toolkit, which was tested on a sizable BIM model to demonstrate its potential for embedding and verifying digital signatures.

5.5 Characteristics and requirements of an ideal solution for object-level data integrity verification and authentication in BIMs using digital signatures

This section outlines the characteristics and requirements of an ideal solution that leverages digital signatures for object-level data integrity and authentication. It draws on industry practices, relevant standards, expert consultations, and software-design principles, and it integrates the digital-delivery framework proposed by Maier (Maier, 2020), mapping its foundational attributes to the ALCOA++ principles.

Integration with existing tools and processes. A primary requirement is that the software toolkit should seamlessly integrate with current BIM tools and workflows. Minimal intervention ensures that users can adopt the solution without extensive retraining or significant changes to their established processes. This promotes user acceptance and facilitates smoother implementation across various organizations.

Object-Level authentication and data integrity verification. The toolkit must provide robust mechanisms for authenticating and verifying data integrity at the object level within BIM models. This granular approach addresses the limitations of file-level authentication, allowing for precise attribution of authorship and responsibility for individual model components. Digital signatures ensure that each object is signed by its creator or modifier, providing non-repudiation and integrity verification. This enhances accountability and enables stakeholders to detect and trace unauthorized modifications to specific objects.

Support for hierarchical signings and metadata attachment. To facilitate complex and collaborative processes, the toolkit should enable signers to be co-signer or vouch for existing signatures, supporting multi-path hierarchical signing structures. This means that Toolkit must allow a signer to endorse or validate other signatures, reflecting the hierarchical relationships often present in construction projects where approvals may come from multiple levels of authority (Hedberg *et al.*, 2020).

Additionally, the toolkit should allow signers to attach metadata to their signatures. This metadata documents the signature details and captures information about any transformations the file

has undergone. By including metadata, the solution enhances transparency and traceability, providing context for the signature and any associated changes (Hedberg *et al.*, 2020).

Independence from engineering disciplines and regional regulations. To ensure flexibility and broad applicability, the solution must be independent of specific disciplines and regional regulations, allowing it to be adapted for various disciplines in different jurisdictions.

By being discipline-agnostic and jurisdiction-independent, the toolkit can cater to a wide range of use cases, promoting wider adoption and facilitating collaboration among multidisciplinary teams in various jurisdictions.

Alignment with digital delivery framework and ALCOA++ principles. Maier (Maier, 2020) presents a digital delivery framework with foundational characteristics—Interoperable, Secure, Open, and Standardized—which intersect to form specialized qualities essential for efficient digital delivery in construction. These attributes closely align with the ALCOA++ principles—Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available—which are critical for maintaining data integrity and reliability.

Maier's framework maps to the ALCOA++ principles as follows. (1) Interoperable ensures compatibility across different platforms without data loss, supporting the Consistent and Available principles by enabling seamless access. (2) Secure protects data against threats, aligning with the Original, Accurate, and Enduring principles through safeguards for integrity and longevity. (3) Open promotes transparency and public availability, corresponding to the Legible and Available principles by ensuring data is both understandable and accessible. (4) Standardized uses consistent standards for reliability and efficiency, relating to the Consistent and Complete principles by ensuring comprehensive and uniform data recording.

By mapping Maier's framework to the ALCOA++ principles, we can ensure that the software toolkit not only meets technical requirements but also adheres to industry best practices for data integrity and reliability.

Functional requirements. The software toolkit should cater to the needs of various actors involved in BIM projects, providing functionalities that support their roles. These actors

have generalization relationships, where each subsequent actor inherits the functionalities of the previous ones and adds new capabilities specific to their responsibilities, for instance the functionalities for Designers and Engineers are included in Project Managers and Coordinators functionalities. This hierarchical structure ensures that all necessary features are accessible to the appropriate stakeholders while maintaining a clear delineation of roles.

Designers and Engineers need tools to digitally sign objects upon creation or modification, ensuring their contributions are authenticated and protected. Because they often handle numerous objects, the toolkit should support batch signing: each signed object triggers extraction and signing of additional related objects and data. In practice, signers prefer this batch approach to efficiently authenticate all relevant elements, streamlining the signing process and ensuring consistency. Project Managers and Coordinators require dashboards and reports to monitor authentication status, apply filters (such as signed vs. unsigned objects), verify data integrity, and review audit trails. Contractors and Subcontractors depend on authenticated model elements that accurately reflect relevant data. Regulatory Authorities and Clients must be able to validate and review authenticated BIM data for compliance checks and informed decision-making.

Non-Functional requirements. The toolkit must be effective and sustainable by meeting several non-functional requirements. Performance Efficiency demands fast processing of digital signature generation and verification without significant delays or resource consumption. Scalability ensures handling increasing data volumes and users without performance degradation, accommodating large BIM models with numerous objects. Usability requires intuitive interfaces and workflows, minimizing the learning curve for signing and verification. Maintainability involves ease of maintenance and updates, including the ability to manage digital certificates throughout their life cycle without extensive downtime. Compatibility necessitates support for various BIM software platforms and industry-standard file formats, ensuring interoperability when applying digital signatures.

5.6 Proposed framework

This research proposes a framework for embedding digital signatures within IFC-based BIMs to achieve object-level authentication. The framework addresses technical challenges associated with embedding digital signatures into BIMs and provides a foundation for developing software toolkit that can be integrated into existing BIM authoring platforms or function as standalone applications.

The overall structure of the software toolkit is presented in Figure 5.2. It contains two processes: signing and verifying. The input to the signing process includes an IFC-based model, which can be in .ifc or .ifcxml format; a certificate for each signer; and a list of objects that each signer is responsible for. The output of the signing process is a signed IFC-based model. The input to the verifying process is a signed IFC-based model, and the output is a list of elements indicating the ObjectID, digital signature, and validity status of the digital signature.

The Digital Signature toolkit consists of three main components: the Signing Utility, which handles the signing functionalities; the Verifying Utility, which handles the signature verification functionalities; and the Common Libraries or Utilities, which contain various functionalities such as certificate management, file management, and hashing and cryptography libraries.

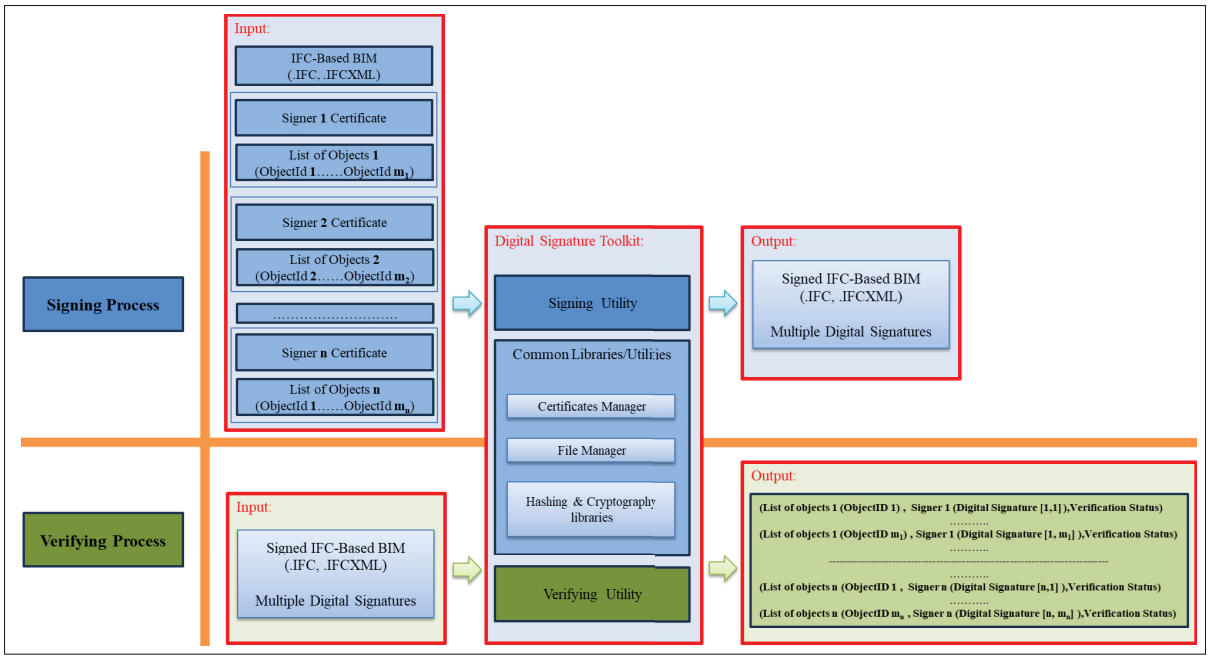

Figure 5.2 Overall structure of the software toolkit for adding Digital Signatures in IFC-based BIMs

5.6.1 Options for embedding digital signature in IFC-based BIMs

Based on the requirements, each digital signature is bound to a specific block that wraps signature metadata and references the objects that the signatory chooses to take responsibility for. Several approaches can be adopted for embedding digital signatures in IFC-based BIM. Each signature is associated with a block containing the relevant metadata and references to the objects under the signatory's responsibility, either stored within the same file or in a separate file. Storing signatures in the same file ensures all signature information, along with references, remains in one place, simplifying file management and long-term archival. Alternatively, maintaining signature blocks in a separate file can allow multiple signatures to be managed without modifying the original BIM file.

Two further distinctions arise from how many signatures reside within each block. In one-signature-per-block configurations, each block contains a single signature and explicit references to the relevant objects, supporting precise attribution but risking redundancy if multiple

signatories sign the same object. Conversely, placing multiple digital signatures in a single block can reduce repetition but complicates the extraction of objects signed by individual signatories.

Combining these variations yields four possibilities as illustrated in Figure 5.3: (1) one signature per block in the same file, (2) one signature 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. Embedding signatures in the same file keeps all data in one location, minimizing external references and promoting traceability and accountability. Consequently, the approach of embedding one digital signature per block within the same file is chosen to proceed, as it ensures each signature remains bound to a specific block and identifies the signatory's responsibilities unambiguously.

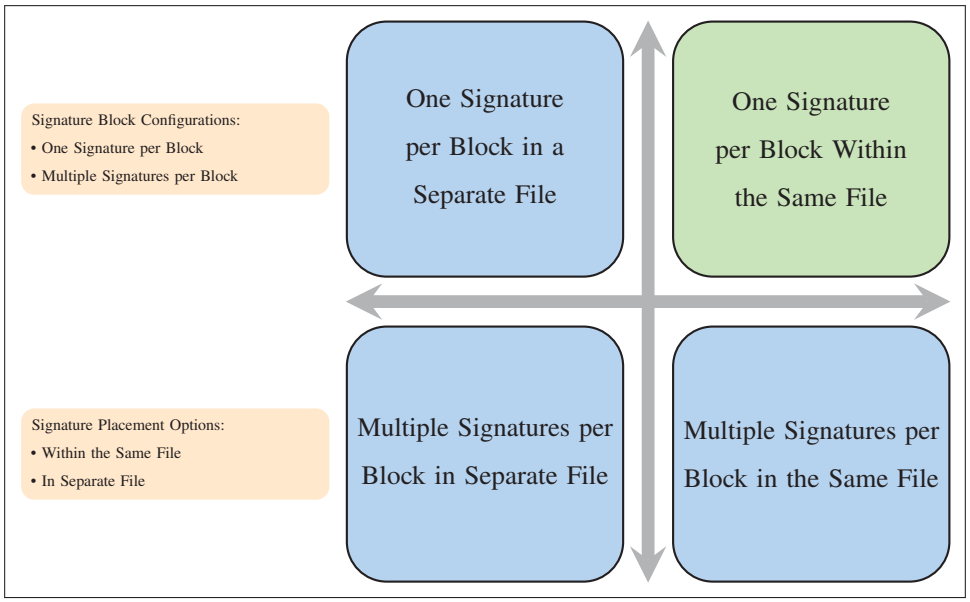

Figure 5.3 Potential solutions considering signature placement options and signature block configurations

5.6.2 Utilizing the ISO 10303-21 optional signature section for embedding digital signatures in IFC-Based BIMs

In research conducted within the manufacturing industry (Hedberg *et al.*, 2017; Hedberg,Jr., Krima & Camelio, 2019; Hedberg *et al.*, 2020) to enable effective and secure data communication,

the STEP file is used as an open data format for data exchange, and a signature block is suggested for "ensuring traceability and trustworthiness" (Hedberg *et al.*, 2020). The signature block is added to the STEP file in the optional section of ISO 10303-21:2016 (ISO10303-21, 2016) which is the standard that defines the data exchange structure. Although the proposed signature block structure supports the authentication of sub-models by adding a reference point in the model to define specific sections, this approach is not fully compatible with IFC-based BIMs, as it does not align with the IFC data schema. In (Fahdah, 2023), the same optional signature section is used to embed digital signature to the IFC-based BIMs at the file level. In the proposed framework designed, the concept of using the optional signature section of the STEP file is adopted, with the aim of developing a structure to authenticate BIMs at the object level.

Based on ISO 10303-21 (ISO10303-21, 2016), the file structure comprises five sections: one mandatory (the header) and four optional. The *header section* begins with "HEADER;" and ends with "ENDSEC;," containing meta information relevant to the entire exchange structure. The *anchor section* assigns external names to instances or values for reference in other structures. Following the header and anchor sections, the *reference section* holds entities and values from external sources. The *data section* contains the actual model instances, each corresponding to a specific schema specified in the header section. Finally, the *signature section* validates the data being transferred and authenticates its origin, beginning with "SIGNATURE;" and ending with "ENDSEC;." Multiple signature sections can be included.

The IFC exchange structure consists of the header section and the data section, both of which are mandatory. Figure 5.4 illustrates the data exchange file structure based on ISO 10303-21 and IFC exchange architecture, as well as the resulting IFC exchange structure with a signature.

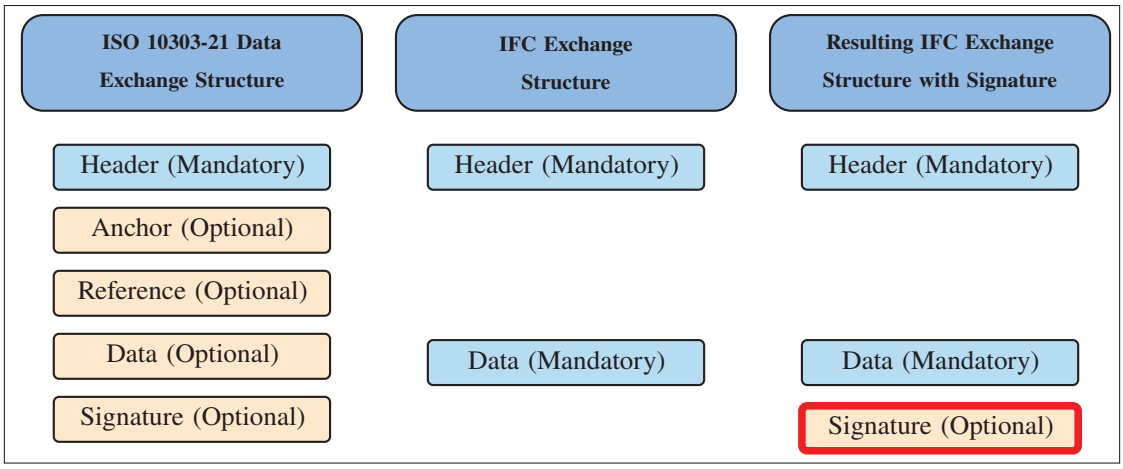

Figure 5.4 Comparison of ISO 10303-21 data exchange structure and IFC Exchange structure and resulting IFC exchange structure with signature

This research aims to create a structure for building a signature block for each individual who will take responsibility for a part of the BIM. These signature blocks are placed in the optional signature sections, which are located after the end of the data section in IFC-based BIMs. Since most BIM authoring and viewing software tools consider the end of the data section as the end of the file, these applications do not detect the signature blocks embedded beyond that point. This means the signature blocks do not interfere with current tools. Various IFC authoring tools, including ACCA's usBIM (ACCA, 2024), were examined by opening, exploring, and editing the model—typical functionalities—after embedding the signature blocks, and no issues were found with the software's functionality. However, the bSI IFC validation service (version validate 0.7.4 - #18837 ca) (bSI, 2025a) considers only the IFC data exchange structure as illustrated in Figure 5.4, flagging any additional sections, such as the optional signature section defined by ISO 10303-21, as errors. A workaround to address the bSI IFC validation service issue could be placing the added signature blocks within comments in the file, as suggested in (bSI, 2025b), using the EXPRESS syntax where comments begin with /* and end with */.

5.6.3 Structure of signature block

To effectively embed digital signatures into IFC-based BIMs files as attachments, a well-defined structure for the signature block is essential. The signature block serves as a container that encapsulates the digital signature information associated with specific list of objects, enabling object-level authentication without modifying the IFC data schema. This structure is compatible with existing BIM authoring and viewing tools. The structure of the embedded signature block in IFC files is illustrated in Figure 5.5.

Each signature block contains three parts: Header, Body, and Digital Signature. The Header includes 2 sections. First section is the signer metadata such as common name; surname; geographical attributes (e.g., country name, state or province name); organizational attributes (e.g., organization name, organizational unit name, title or role); certificate validity; and signing time (ETSI, 2010; ITU, 2019; X.520, 2019). Other optional data can also be added. It is recommended that the signer metadata align with common standards such as X.509 (ITU, 2019), XAdES (ETSI, 2010) , and X.520 (X.520, 2019). The second section in the Header part is the calculated hash of the previous signature block. In the case of the first signature block, this could be the calculated hash of the entire IFC data section. By including the hash of the previous signature block, the solution can chain all signature blocks together, which helps to detect missing or tampered signature blocks. Additionally, calculating the hash of the whole data section of the IFC file in the first signature block provides the ability to detect any changes in the entire file after the creation of the signature block, even if the changes occurred outside of the object list related to the signer of the signature block.

The Body of the signature block contains a list of triplets, each consisting of an ObjectID, the calculated hash of the object's definition, and a verification status. Each ObjectID corresponds to an object from the list of objects that is input to the Digital Signature Toolkit, as illustrated in Figure 5.2. The second element, the calculated hash of the objects' definition, guarantees the integrity of the data at the object level. If the definition of a specific object is changed after the creation of the signature block, the calculated hash will change, which will be detectable

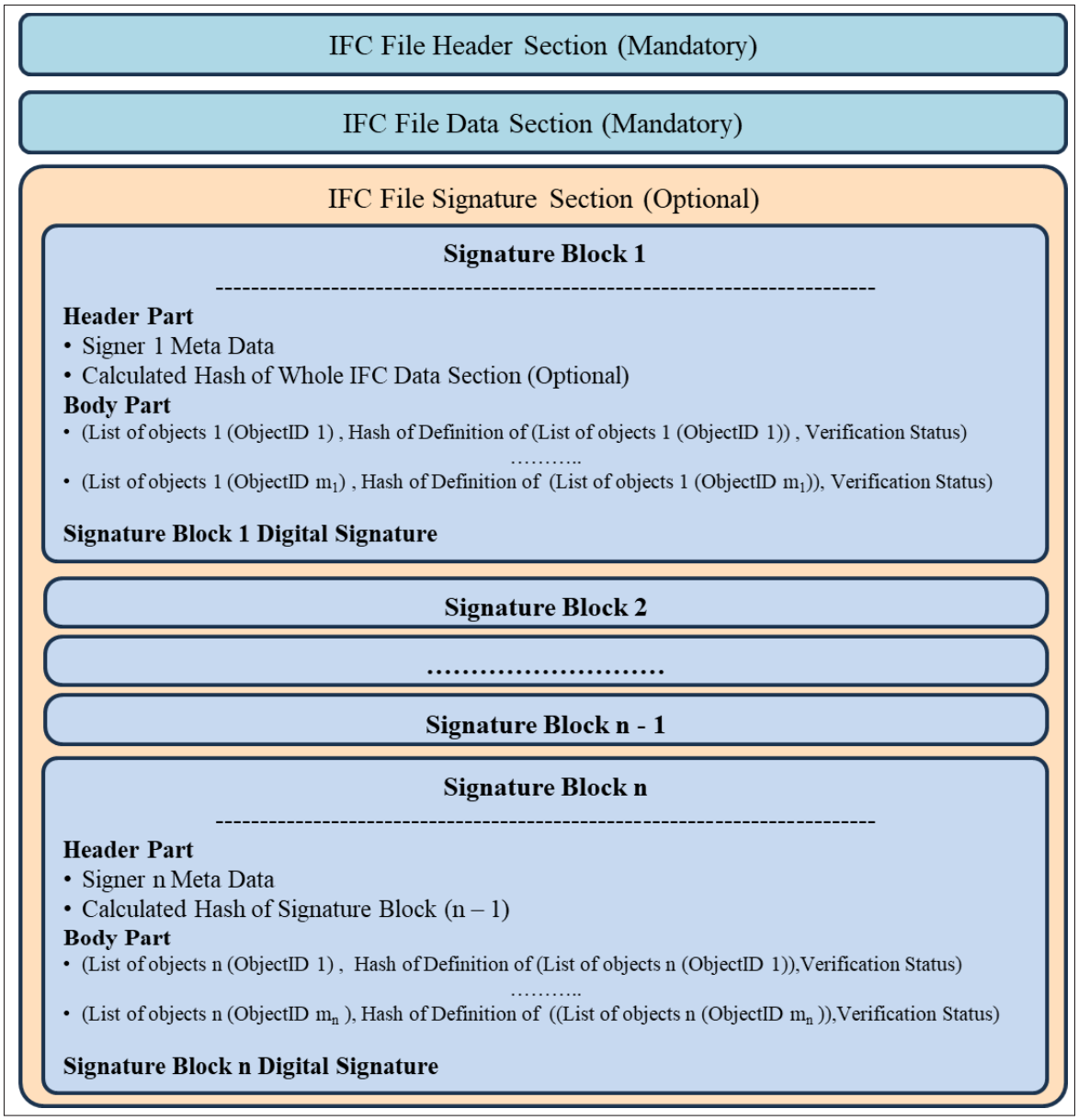

Figure 5.5 Structure of the signature block for embedding digital signatures into IFC-based BIMs at the object level

during the verification process. The last element in the triplet is the verification status, which is mainly used in the verification process to indicate whether the data remains intact or has been tampered with. It can have three possible values: "unverified," which means it has not been examined; "valid"; and "invalid." Its initial value during the signing process, before verification, is "unverified."

The last part of the signature block is the digital signature itself. The signer digitally signs the entire signature block to guarantee the integrity of the data within it. By doing so, any alteration to the signature block after signing can be detected during the verification process, ensuring that the data remains unmodified and trustworthy. In addition, the signer includes professional identity and responsibility within the signature block. This incorporation of professional credentials not only verifies the signer's identity but also associates them with specific parts of the BIM for which they are accountable. This adds a layer of authenticity and accountability, as stakeholders can confirm who signed the data and understand the extent of their responsibilities in the BIMs.

5.6.3.1 Creating the signature block

Creating a signature block involves several key steps that ensure the integrity and authenticity of the BIM data at the object level:

1. Assign UUID and Sequence Number to Signature Block: Generate a universally unique identifier (UUID) and assign a sequence number to the signature block. The UUID ensures that each signature block can be uniquely identified within the BIM, while the sequence number establishes the order of the signature blocks when multiple signatures are present. This is crucial for maintaining the integrity of the signature chain and for efficient management during the verification process.
2. Compile Signer Metadata: Gather the signer's metadata to include in the Header of the signature block. These metadata elements can be input directly into the system by the signer or extracted from the signer's digital certificate. This includes information such as common name, organization name, title or role, certificate validity period, and signing time. Aligning this metadata with common standards like X.509, XAdES, and X.520 is recommended (ITU, 2019; X.520, 2019; ETSI, 2010).
3. Input the List of ObjectIDs: The Digital Signature Toolkit receives, as input, a list of ObjectIDs representing the objects that the signer is responsible for and wishes to authenticate.

4. Extract Object Definitions: The toolkit extracts the definition of each ObjectID from the IFC file. This involves locating each object's definition line within the file to obtain the exact data that will be used for hash calculation.
5. Calculate Hashes of Object Definitions: For each extracted object definition, calculate the hash of its definition line. There are various hash functions available, each with different security properties and performance characteristics. Notable hashing algorithms include: Message Digest Algorithm 5 (MD5) (Rivest, 1992), RACE Integrity Primitives Evaluation Message Digest (RIPEMD) Family (Bosselaers & Preneel, 1995; Dobbertin, Bosselaers & Preneel, 1996), Secure Hash Algorithm (SHA) Family (of Standards and Technology, 2015) like SHA-1 , SHA-2 (SHA-224,SHA-256 ,SHA-384,SHA-512) and, SHA-3.

   For implementing the MVP, SHA-256 was used due to its relatively strong security properties, widespread acceptance, and balance between performance and security (Alamgir, Nejati & Bright, 2024). Additionally, it is possible to change the hashing algorithm in the future to adapt to evolving security requirements or specific performance needs, depending on project or system demands.
6. Create Body: Construct the list of triplets, each consisting of:
   - ObjectID: The identifier of the object.
   - Object Hash: The calculated hash of the object's definition.
   - Verification Status: Initially set to "unverified"; it will be updated during the verification process.
7. Compute Previous Signature Block Hash: Include the calculated hash of the previous signature block in the Header to chain all signatures together. For the first signature block, this could be the hash of the entire data section of the IFC file.
8. Generate Digital Signature: Digitally sign the entire signature block using the signer's private key. This creates the Digital Signature part, ensuring the integrity of the signature block itself.
9. Embed the Signature Block: Insert the signature block into the IFC file using the optional SIGNATURE section defined in ISO 10303-21 (ISO10303-21, 2016). Place the signature

block after the end of the data section (ENDSEC;) to avoid interference with BIM authoring tools.

To formally define the syntax of the signature block embedded in IFC files, the Wirth Syntax Notation (WSN) is utilized, which provides a clear and precise way to describe the grammar of structured data. Listing 5.1 specifies the structure of the signature block in accordance with the ISO 10303-21 (STEP file) exchange structure (ISO10303-21, 2016).

Listing 5.1: WSN Definition of the Signature Block

```
signature_block = "SIGNATURE;" header_section body_section
    digital_signature_section "ENDSEC;".

header_section = "HEADER" "(" header_content ")".

header_content = uuid_entry ";" sequence_number_entry ";"
    signer_metadata_entries ";" previous_signature_hash_entry.
uuid_entry = "UUID" ":=" string_value.
sequence_number_entry = "Sequence_Number" ":=" integer_value.
signer_metadata_entries = signer_metadata_entry { ";"
    signer_metadata_entry }.
signer_metadata_entry = metadata_key ":=" string_value.
metadata_key = "Signer_Name" | "Organization_Name" | "Title" |
    "Signing_Time" | "Certificate_Validity".
previous_signature_hash_entry = "Previous_Signature_Hash" ":="
    string_value.

body_section = "BODY" "(" object_entries ")".

object_entries = object_entry { "," object_entry }.
object_entry = "(" object_id_entry ";" object_hash_entry ";"
    verification_status_entry ")".
object_id_entry = "ObjectID" ":=" string_value.
object_hash_entry = "Object_Hash" ":=" string_value.
verification_status_entry = "Verification_Status" ":="
    string_value.
digital_signature_section = "DIGITAL_SIGNATURE" ":="
    string_value.
```

5.6.3.2 Implementation key points and considerations

Implementing digital signatures within IFC-based BIMs involves several critical factors that must be carefully addressed to ensure the solution's effectiveness. This section highlights key points and considerations in the implementation process, providing insights into the decisions made during the development of the signature embedding method.

Focus on the Data Section for Hash Calculation: In our solution, the hash calculation is performed exclusively on the data section of the IFC file. The primary reason for excluding the header section from the hash calculation is that the header can change each time the file is modified and saved or goes through import and export process in BIM software, even without any modifications to the actual BIM data. Such changes can occur due to software-specific metadata updates, timestamps, or other non-critical information that does not affect the integrity of the BIM model itself.

Including the header section in the hash calculation would lead to frequent invalidation of the hash during the verification process. Minor, non-substantive changes to the header would cause the computed hash to differ from the original, resulting in false indications of data tampering.

Canonicalization Techniques: To maintain consistency in hash calculations and ensure that the digital signatures are reliable across different systems and software, canonicalization techniques are applied to the data section before hash calculation:

- Elimination of Unnecessary White-spaces and Carriage Returns: White-spaces, tabs, and line breaks that do not affect the actual data are standardized or removed. This prevents discrepancies in hash values due to formatting differences that may occur when the file is handled by different software tools.
- In STEP files, the order of object definitions can vary without impacting the BIM model's content. The best way to guarantee that the calculated hash remains the same, regardless of the order of the lines, is to sort the file based on the ObjectIDs. However, doing so would have a negative effect on performance. Therefore, in this solution, we assume that the order of the lines remains the same, and any change in the order of the lines after the file has been

digitally signed indicates that the data has been tampered with. It is worth noting that line order affects the hash only when the first signature block includes, in its header, an optional hash of the entire IFC data section. If this overall hash is omitted, line order has no impact on hash computation during either the signing or the verification process.

- Comments within the IFC data section are ignored by the current solution; however, they can be included in the hash of the entire data section if that optional hash is added to the header of the first signature block.

Performance Considerations: Computing hashes for each object can be resource-intensive, especially for large BIM files with numerous objects. To mitigate performance impacts, optimizations such as parallel processing can be employed.

File Size Implications: Embedding signature blocks adds to the overall size of the IFC file. Particularly, in case of large BIMs When multiple stakeholders with long list of objects add signature blocks, the cumulative increase in file size may become significant.

5.6.3.3 Implementation summary and performance evaluation

This section presents the implementation details of the digital signature embedding solution, evaluates its performance, and discusses the challenges encountered during the process. The development was carried out using the C# programming language within the Microsoft Visual Studio 2022 integrated development environment (IDE). A significant aspect of the evaluation involved testing the solution on a sizable IFC-based model to simulate real-world scenarios and assess scalability. A sample .ifc file of 70 MB in size, containing 1,131,327 ObjectIDs, was utilized. This model provides a comprehensive dataset to test the performance and efficiency of the digital signature embedding process.

The test scenario involved creating three signature blocks for three engineers and the objects in the data section were divided into three distinct object lists, one for each engineer. The division was performed such that the union of all three lists equals the entire set of objects in the data section, and there was no common entries between any two object lists. The initial

signing process utilizing a laptop with Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz processor and 16 GB RAM, took approximately 12 seconds to complete, which was deemed sub-optimal for practical applications. By refining the code and optimizing algorithms and applied data structures, the signing time was reduced to less than 3 seconds. The tests revealed that hash calculation is a memory-intensive process, especially when dealing with large numbers of objects. Efficient memory management and optimization techniques are crucial to maintain acceptable performance levels.

After attaching the signature blocks, the size of the IFC file almost doubled, raising concerns regarding file transmission efficiency and the performance of BIM authoring software tools. To address the file size issue, common compression libraries were experimented with, including GZip (Microsoft, 2022) and CBOR (Concise Binary Object Representation) (Bormann & Hoffman, 2013). Despite implementing these compression algorithms, no considerable reduction in file size was achieved. In fact, hash strings exhibit high entropy to increase security, meaning they are already close to random and lack repetitive patterns (Magfirawaty, Suryadi & Ramli, 2017; Erbay & Ergïn, 2018; Loza & Matuszewski, 2014). This characteristic makes them inefficient to compress using standard algorithms, as compression relies on finding and encoding such patterns (Gupta & Agarwal, 2008).

Given the significant increase in file size and the negligible impact of compression, it was recognized that the current approach was not viable for practical use. The increased file size negatively affects file transmission and the performance of BIM tools, as BIM authoring and viewing softwares may experience degraded performance when handling excessively large files. To resolve these issues, an alternative solution was sought by restructuring the signature block to reduce its size. The details of this new solution are explained in the next section.

5.6.4 Restructuring signature blocks to optimize file size

In response to the significant file size increase resulting from the initial signature block structure, the signature blocks were restructured to effectively address this issue. The primary challenge

identified was the high number of hashed strings within each signature block, which directly contributed to the expansion of file size. To mitigate this, the research proposes reducing the number of hashed strings by grouping objects into sub-lists or collections. Instead of calculating the hash for each individual object definition, objects definitions within each collection are concatenated, and a single hash is computed for the resulting string. Additionally, the resulting hashes of all collections are compressed to further minimize the impact on file size. This approach not only addresses the file size concern but also maintains the integrity and authenticity of the BIM data. The new signature block structure is illustrated in Figure 5.6.

5.6.4.1 Implementation steps and test results

The implementation of the restructured signature blocks involves several key steps to ensure efficiency. The following list outlines the detailed process:

1. Assign UUID and Sequence Number.
2. Compile Signer Metadata.
3. Input the List of collections with objects in each collection: The Digital Signature Toolkit receives a list of collections with ObjectIDs in each collection representing the collections to be authenticated.
4. Extract and Concatenate Object Definitions: For each collection, the definitions of the objects within the collection are extracted from the file and concatenated into a single string.
5. Calculate Hash: A hash is calculated for the concatenated string of each collection. The resulting hash is then compressed to minimize its size.
6. Create Body: The body section of the signature block is constructed using the list of objectIDs in each collection plus Calculated Hash of concatenated strings of all Object definitions in the collection instead of individual object hashes. in addition to the list of objectIDs in the collection, each collection in the body has a triplet , each consisting of:
    - CollectionID: The identifier of the collection.
    - Calculated Hash of concatenated strings of all Object definitions in the collection
    - Verification Status

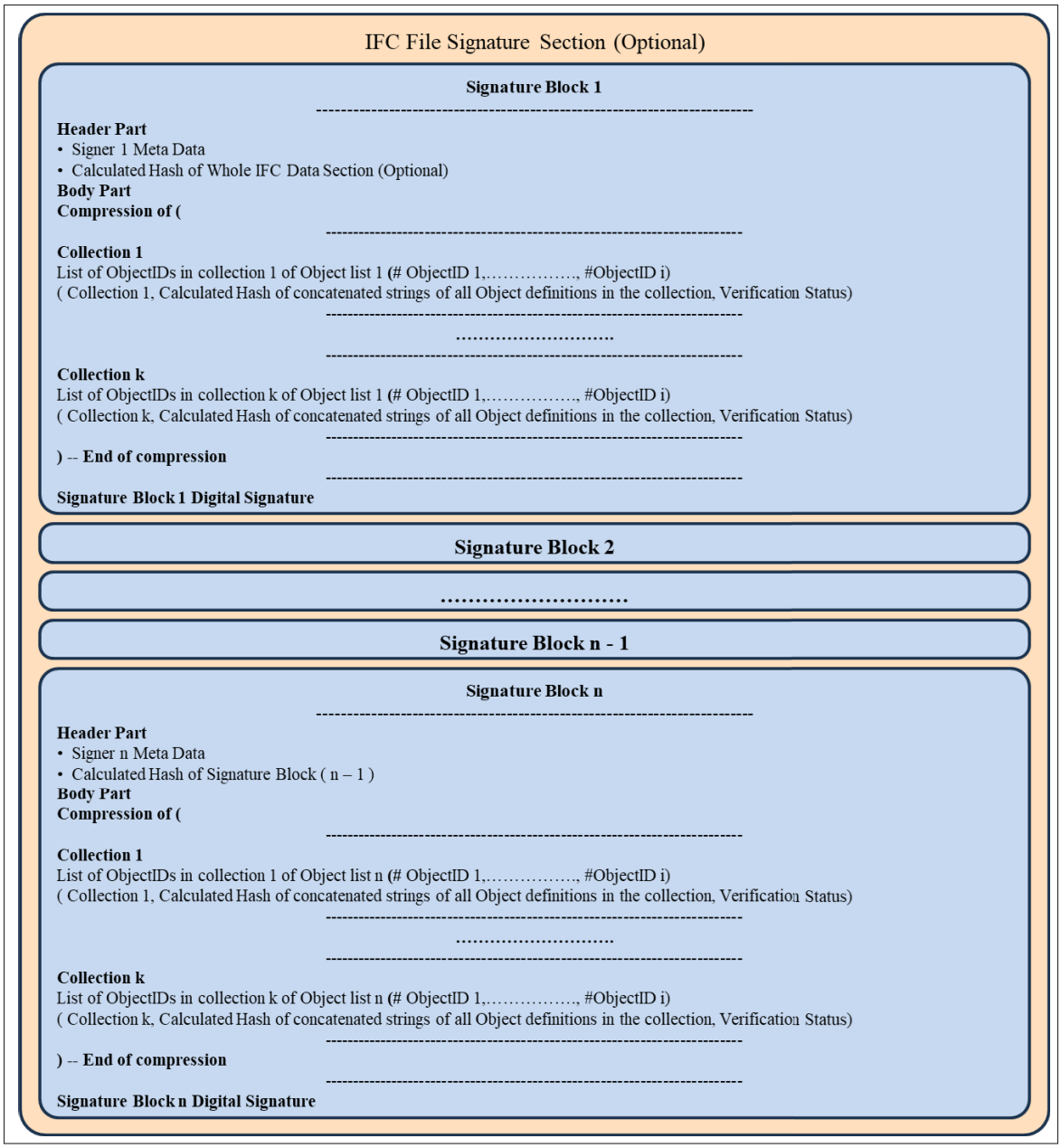

Figure 5.6 New structure of the signature block for embedding digital signatures into IFC-based BIMs at the object level

7. Compress the resulting Body
8. Compute Previous Signature Block Hash.
9. Generate Digital Signature.
10. Embed the Signature Block.

The restructured signature block implementation was tested using the same tools, IFC file, and scenario as the initial approach. The test involved creating three signature blocks for three engineers, each responsible for a distinct subset of objects within the data section and 3 collections in each signature block.

The restructuring resulted in the IFC file size increasing by less than 20 MB after hash calculation of collection and less than 3 MB after utilizing compression over the signature block, a significant improvement compared to the nearly doubled size observed with the initial signature block structure. Despite the structural changes, the signing process remained efficient, with signing times still under 3 seconds, similar to the optimized initial approach.

5.6.5 Discussion and comparison of proposed signature block structures

The implementation compared two signature block structures, each presenting distinct advantages and trade-offs. The comparative evaluation of the two signature block structures is summarized in Table 5.4. The initial structure employed object-level authentication, where each object within the IFC file was individually authenticated by calculating its specific hash. This approach, while providing fine-grained authentication, led to a considerable increase in the IFC file size, due to the high number of hashed strings. Consequently, the substantial file size increase rendered this approach impractical for real-world applications, adversely affecting file transmission efficiency and the performance of BIM tool software.

In contrast, the restructured signature block adopted a collection-level authentication strategy, wherein groups of objects were authenticated together by hashing their concatenated definitions. This method effectively addressed the file size issue. Additionally, the collection-based approach aligns with the anticipated module-based structure of IFC 5 (van Berlo *et al.*, 2021), allowing each collection to be mapped as a module. Furthermore, by authenticating collections rather than individual objects, the solution benefits from the ability to reuse calculated hashes for signing the same collection, reducing the need for repeated hash calculations and further optimizing performance.

However, this restructuring introduced a trade-off: while the file size issue was effectively mitigated, authentication was now performed at the collection level rather than the object level. This means that individual object tampering within a collection may not be directly detectable and makes hash of whole collection invalid. In summary, the restructured signature block offers a practical balance between maintaining data integrity and managing file size, making it a more viable solution for large-scale BIM projects. Although it compromises on the granularity of authentication, the benefits in file size reduction and compatibility with future IFC standards present a compelling case for its adoption. A final note is that if a collection in the restructured signature block is reduced to a single object, the restructured and initial signature-block structures become identical.

Table 5.4 Comparison of initial and restructured signature block structures

Aspect	**Initial Signature Block (Object-Level)**	**Restructured Signature Block (Collection-Level)**
Tampering Detection	Individual object changes can be identified	Can detect change in a collection but not the specific object
File Size Impact	Significant increase due to many hashes	Fewer hashes and compression significantly reduce file size
Equivalence Case	Always unique per object	Identical to object-level structure if a collection contains a single object

5.6.6 Verification process of the restructured signature block

The verification process validates that the signature block remains intact and that the BIM data has not been tampered with since the time of signing. It involves verifying signer's digital signature over the signature block, decompressing the stored hashes, recalculating hashes for the collections using the same methodology as in the signing process, and comparing them to the existing hashes. Additionally, the verification includes evaluating the hashes of previous signature blocks to maintain the integrity of the signature chain. Verification steps are:

1. Validate Digital Signature Integrity: Verify that the digital signature of the signature block is valid. This confirms that the signature block has not been altered and that it was signed by the purported signer.
2. Decompress the Signature Block: Decompress the signature block to access the collection hashes and the list of objects in each collection.
3. Extract Collections and Object Lists: From the decompressed signature block, retrieve the collections and their associated lists of ObjectIDs.
4. Recalculate Collection Hashes: For each collection:
    - Extract Object Definitions: Retrieve the definitions of all objects listed in the collection from the current IFC file.
    - Concatenate Object Definitions: Concatenate the extracted object definitions into a single string, maintaining the same order as in the collection list of objectIDs to ensure consistency.
    - Compute Hash: Calculate the hash of the concatenated string using the same hashing algorithm (e.g., SHA-256) employed during signing.
5. Compare Hashes: Compare the recalculated hashes with the existing hashes stored in the signature block for each collection.
    - Hashes Match: If the recalculated hash matches the existing hash for a collection, it indicates that all object definitions within that collection are intact and have not been altered since signing.
    - Hashes Do Not Match: If the recalculated hash does not match the existing hash, it suggests that at least one object definition within the collection has been modified after signing. This discrepancy flags potential tampering or unintended changes to the BIM data.
6. Evaluate Previous Signature Block Hashes: Verify the hash of the previous signature block included in the current signature block's header.
    - Hash Match: A matching hash confirms the integrity of the previous signature block and ensures the continuity of the signature chain.

- Hash Mismatch: A mismatch indicates that the previous signature block has been altered or is missing, compromising the integrity of the entire signature chain.

Based on the verification step, possible scenarios during verification process are:

1. Digital signature over signature block is valid and all hashes match and previous signature block hash match: The signature block is intact. The objects in each collection in the signature block have not been tampered with, and the integrity of the data since the time of signing is confirmed.
2. Digital Signature over signature block is Valid but Collection Hash Mismatch: it indicates that the signature block has not been altered, but the BIM data within the affected collections has been modified since signing. At least one object within the collection has been changed. However, it is not possible to recognize the modified objects.
3. Digital Signature over signature block is Invalid: it implies that the signature block itself has been altered or corrupted. This compromises the trustworthiness of the signature block and the BIM data integrity cannot be assured based on this signature block.
4. Previous Signature block Hash Mismatch: when The hash of the previous signature block does not match during evaluation, there is a disruption in the signature chain, indicating that a previous signature block has been altered or removed. In case of first signature block which can contain hash of whole data section, indicates that the data section is modified even if the hash of collections matches. This affects the overall integrity verification process and may signify tampering with the signature history.

   When the optional header of the first signature block contains a hash of the entire IFC data section, a mismatch during verification signals that the data section has been altered—potentially outside the signer's ObjectID list. The toolkit flags this discrepancy as a warning, leaving the ultimate validity decision to the professional reviewing the verification result.

In the verification process, several key considerations are essential to ensure accuracy and reliability. Maintaining the same order of object definitions during concatenation as used in the signing process is crucial; any change in this order can result in different hash values,

potentially leading to false indications of tampering. Consistency in the hashing algorithm is equally important; employing the same algorithm during verification as was used during signing guarantees accurate comparisons. When dealing with large collections, efficient memory management during hash recalculation is vital to prevent performance bottlenecks and ensure the process remains practical and timely.

The outcomes of the verification process carry significant implications. Successful verification assures stakeholders that the BIM data remains unaltered and reliable, which is essential for informed decision-making and smooth project progression. Furthermore, the verification process enables the detection of presence of unauthorized modifications.

5.7 Evaluation of the restructured signature block against requirements

The restructured signature block was developed to address the significant increase in IFC file size caused by the initial approach to embed digital signatures for each object. By grouping objects into collections and calculating a single hash for each collection, the restructured signature block optimizes file size while aiming to maintain data integrity and authentication capabilities. This evaluation assesses how the restructured signature block meets the characteristics and requirements of an ideal solution for object-level data integrity verification and authentication in BIM using digital signatures, as outlined in Section 5.5. This approach integrates seamlessly with existing BIM tools since it avoids changes to the IFC schema and relies on standard entities, ensuring that BIM software can handle the models without performance degradation or the need for an update of the implementations.

However, by authenticating at the collections level, rather than at the individual objects, modification within a collection is detected without identifying the specific object altered. Nevertheless, hierarchical signing is supported through the inclusion of previous signature block hashes, which allows signers to vouch for existing signatures and attach metadata to enhance traceability and accountability.

The solution is independent from engineering disciplines and regional regulations and aligns well with Maier's digital delivery framework (Maier, 2020) and ALCOA++ principles, ensuring data is attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available. It also meets functional requirements by supporting efficient batch signing, and satisfies non-functional requirements such as performance, scalability, usability, maintainability, and compatibility. Table 5.5 summarizes the evaluation of the restructured signature block against these requirements.

Table 5.5 Evaluation of the restructured signature block against requirements

Requirement	**Evaluation**
Integration with Existing Tools	Integrates seamlessly by avoiding changes to the IFC schema and using standard sections in ISO 10303-21, ensuring compatibility with existing implementations.
Object-Level Authentication	Provides authentication at the collection level; while it detects modifications, it cannot pinpoint individual object changes.
Hierarchical Signings and Metadata	Supports hierarchical signing through previous signature block hashes and allows metadata attachment, enhancing traceability and accountability.
Domain and Regulation Independence	Designed to be domain-agnostic and jurisdiction-independent, making it suitable for various disciplines and legal environments.
Alignment with Digital Delivery Framework & ALCOA++	Aligns well with Maier's digital delivery framework and meets ALCOA++ principles (attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available).
Functional Requirements	Supports efficient batch signing, comprehensive monitoring, and role-specific functionalities for diverse stakeholders.
Non-Functional Requirements	Achieves performance efficiency, scalability, usability, security, maintainability, and compatibility with minimal performance degradation.

5.8 Conclusion

This paper explores the possibilities to address the critical need for object-level data integrity verification and authentication in BIMs within the built asset industry. Current file-level security measures in BIM are insufficient for granular authentication and data integrity verification. To overcome these challenges, a practical solution utilizing digital signatures within the IFC-based BIMs file is proposed.

A Design Science Research methodology was employed to investigate the necessity of object-level authentication, define the requirements of an ideal solution, and develop a software toolkit that leverages digital signatures for authentication and data integrity verification. The initial approach of signing individual objects resulted in significant file size increases, hindering practical application. To address this issue, the signature blocks were restructured to authenticate collections of objects, significantly reducing file size while maintaining acceptable levels of data integrity and authentication. This finding confirms that collection-level hashing strikes a pragmatic balance between precision and performance, and that the framework integrates seamlessly with existing IFC-based workflows because it is independent of any particular IFC schema, thereby ensuring both backward and forward compatibility.

Building upon the findings of this research, several avenues for future work are proposed to enhance the solution and address its limitations. Firstly, investigating the possibility of utilizing multiple data sections within an IFC file, as allowed by the ISO 10303 standard, is suggested. By adopting this approach, authentication and exchange of each data section separately would be enabled. However, complexities such as managing dependencies between sections and potential duplication of data and definitions, instead of reusing them, would need to be addressed. Additionally, reaching out to buildingSMART International to propose the inclusion of digital signature optional sections in the IFC data exchange structure, and advocating for their acceptance as a valid part of the file within the bSI IFC validation service, is identified as a crucial step for broader industry adoption.

Engaging with domain experts to present the proposed solution, gather feedback, and make necessary adjustments is a crucial next step. Collaboration with practitioners in the built asset industry and cybersecurity domain would provide valuable insights into practical considerations, user acceptance, and potential barriers to adoption. By incorporating their feedback, the solution could be refined to better meet industry needs and enhance its applicability.

Finally, translating the solution into a commercial product would require further development, including user interface design, integration with popular BIM software, and robust testing.

Concurrent efforts to formalize the solution within industry standards should be made. Writing a standard based on existing standards and the proposed solution could increase acceptance in the market by providing clear guidelines and ensuring interoperability. Since the solution is based on ISO 10303, the same approach could potentially be applied to other open data formats that utilize this standard for data exchange, expanding its applicability beyond BIM. This expansion could benefit industries beyond built asset industry, such as manufacturing and aerospace, where data integrity and authentication are equally critical. By adapting the solution to different contexts, wider adoption could be promoted, contributing to improved data security practices across various sectors.

Acknowledgments

This work was supported through MITACS Grant IT31364 with the collaboration of Portage CyberTech.

CHAPTER 6

DISCUSSION

6.1 Introduction

This chapter discusses the overall research design and significant findings derived from the investigation of object-level authentication and data integrity verification in BIMs. It evaluates the implications and contributions to both theory and practice, highlights the originality of the developed framework, and identifies avenues for future work. Rather than summarizing discussions provided within each publication, this chapter offers a holistic evaluation of the entire research effort.

6.2 Discussion of the research design

The research employed a Design Science Research Methodology (DSRM), appropriate due to the prescriptive and exploratory objectives, focused explicitly on addressing a tangible industry challenge identified by practitioners. Grounding the problem in real-world relevance and verifying it through stakeholder engagement validated the practical urgency of the research. This methodology ensured rigorous alignment between theoretical gaps identified in existing literature and actual challenges encountered by industry partners. The iterative nature of DSRM allowed continuous refinement of artifacts through repeated cycles of design, development, demonstration, and evaluation, significantly enhancing the reliability and practical applicability of the research outcomes.

The evaluation of the research design aligns with the guidelines proposed by Hevner and Chatterjee (2010), specifically addressing their checklist:

1. Clearly articulated research questions defined the necessity (RQ1), ideal solution characteristics (RQ2), and the practical integration of object-level authentication (RQ3).
2. The developed artifact is a framework detailed extensively in Chapter 5, represented through digital signature blocks independent of the IFC data schema.

3. The iterative design process systematically explored schema-dependent methods, such as integrating signatures within existing IFC entities, before transitioning to a more viable schema-independent approach.
4. Theoretical grounding included comprehensive literature review on digital signatures, BIM adoption challenges, IFC schema structures, and existing authentication practices in construction, thereby supporting artifact development and design choices.
5. Internal evaluations involved iterative tests of software prototypes using realistic IFC models to refine and optimize signature block design and performance, resulting in practical, user-oriented enhancements.
6. Artifact demonstration validated utility through scenario-based testing involving intact and deliberately modified IFC files, confirming effectiveness in detecting data integrity breaches.
7. New knowledge, in the form of four publications (three conference papers and one journal article), has contributed to the scholarly and professional understanding of object-level authentication in BIM.
8. Collectively, the research questions were satisfactorily addressed, providing clear justification, identifying necessary characteristics, and demonstrating practical viability of the proposed solution.

Limitations of the research design included reliance on controlled environments rather than extensive field testing, necessitating future work to ensure broader practical validation and refinement.

6.3 Discussion of the findings

The principal findings from this research are categorized into conceptual justification, framework characteristics, and practical implementation:

- Conceptually, the necessity for object-level authentication was justified by identifying significant vulnerabilities and limitations in current file-based methods, thereby clearly articulating the industry demand for more granular authentication processes.

- Defining the essential characteristics of the ideal solution clarified functional requirements (object-level granularity, interoperability) and non-functional requirements (performance, scalability, regulatory compliance).
- Practically, the framework successfully integrated digital signatures independent of IFC schema constraints, optimizing the structure of signature blocks to balance granularity and performance considerations.

These findings align well with the guidelines established by DSRM, validating artifact viability through rigorous internal testing and iterative improvements. Stakeholder input further confirmed the solution's potential value and commercial relevance.

6.4 Originality of the work and contributions

This research provides several notable contributions:

- Compared to existing approaches that focus on file-level authentication or container-based solutions, the proposed framework introduces a novel semi object-level or collection of objects-level mechanism for embedding digital signatures within IFC-based BIMs. Current industry practices—such as the use of memorandum files, or wrapping IFC models in a container do not support per-object accountability or co-signing or vouching workflows. Blockchain-based approaches have also been investigated, offering tamper-evidence and traceability, yet they present significant limitations in implementation complexity, regulatory compatibility, and long-term validation.

  In contrast, this research proposes an IFC schema-independent method that operates without modifying the IFC data schema. By reusing existing IFC serialization and embedding signature blocks in the file as well as referencing IFC objects, this framework ensures interoperability, minimizes tool disruption, and supports scalable co-signing. Table 6.1 presents a comparative overview of the key characteristics of existing methods versus the proposed framework.

Table 6.1 Comparison of existing BIM authentication solutions and the proposed framework

Criteria	**Memorandum or wrapping-based Methods**	**Blockchain-based Methods**	**Proposed Framework**
Authentication Level	File-level only	File- or object-level	Collection of objects-level
Legal and Regulatory Acceptance	High	Low to moderate	High (uses standard digital signature infrastructure)
Co-signing and Vouching Capability	Not supported	Theoretically possible	Explicitly supported
Long-Term Validation (LTV)	Supported	Challenging to maintain	Supported
Implementation Complexity	Moderate	High	moderate

- Another significant contribution is the comprehensive evaluation of digital signatures against blockchain-based methods, establishing clear justification for selecting digital signatures based on practical and legal considerations.
- Methodologically, the application of DSRM within the BIM domain offers an exemplary case study, demonstrating its utility in addressing complex, multifaceted problems where iterative development and continuous stakeholder feedback are critical.
- Finally, practical insights from iterative testing significantly contribute to understanding performance trade-offs and practical considerations for implementing object-level authentication solutions in real-world BIM environments.

Collectively, these contributions advance both theoretical discourse and practical solutions, enabling more secure and reliable BIM practices.

6.5 Opportunities for future work

Several avenues for future research emerged from this investigation:

- First, full-scale field testing in diverse real-world BIM projects is essential for validating framework robustness and scalability. This would involve deploying the solution in live environments and rigorously assessing its impact on workflow efficiency and stakeholder acceptance.
- Future work could further optimize signature block structures and compression techniques to achieve truly individual object-level granularity without performance compromises.
- Integrating the framework into widely used commercial BIM platforms and developing user-friendly interfaces and tools would facilitate practical adoption. This effort should involve collaboration with software developers and end-users to ensure alignment with existing practices.
- Exploring additional regulatory, legal, and contractual implications arising from the widespread adoption of digital signatures in BIM workflows would be beneficial, enhancing the framework's comprehensive utility and facilitating broader acceptance.
- Lastly, longitudinal studies could assess long-term impacts of deploying such solutions on industry-wide practices, including the evolution of stakeholder responsibilities, changes in collaboration dynamics, and overall improvements in project quality and efficiency.

By addressing these opportunities, future research can significantly enhance the practical effectiveness and broader adoption of the proposed framework, ensuring its long-term relevance and utility in the rapidly evolving digital construction landscape.

CONCLUSION AND RECOMMENDATIONS

Built asset industry continually grapples with a paradox: trust, transparency, and traceability are essential for collaboration, yet achieving these through digital transformation introduces significant complexities. To overcome this challenge, the industry requires robust mechanisms to authenticate and verify data integrity at granular levels. The research conducted for this thesis represents a significant advancement toward addressing this duality.

The central objective of this thesis was to investigate and propose a solution for embedding digital signatures within Building Information Models (BIM) specifically at the object level. This goal was pursued through an extensive exploration into innovative methods for securing data authenticity and integrity, primarily via IFC schema and openBIM standards. The developed artifact—namely, the framework for embedding digital signatures in IFC-based BIMs—systematically addressed the critical research question: What is the potential impact of object-level digital signatures on trust, transparency, and traceability within BIM-based collaborative projects?

Practical experience from industry collaboration highlighted ongoing struggles related to validating data integrity and establishing reliable authentication mechanisms. Case analyses and stakeholder interactions underscored this challenge, reflecting the industry's need for more robust and precise security measures beyond traditional file-level approaches. Meanwhile, the existing theoretical discourse lacked specificity concerning digital authentication mechanisms tailored for BIM at the object level, often remaining confined to generalized discussions on cryptographic methods or generic digital security concepts. Thus, this research introduced practical clarity by defining new parameters for object-level verification, identifying explicit methods to secure BIM data, and improving collaborative processes through digital trust mechanisms.

The investigation was structured around two principal sub-questions: How can digital signatures be effectively integrated at the object level within IFC-based BIMs? And how does such

integration influence collaborative processes and data reliability? Answers derived from empirical analysis and the development of the proposed artifact provided a comprehensive understanding of object-level security, resulting in the formulation of a structured model for embedding and verifying digital signatures within BIM data exchanges. This model demonstrated that object-level authentication could significantly enhance the transparency and reliability of collaborative processes by systematically ensuring data integrity.

Prospectively, this research poses a crucial question to guide future work: Given the developed framework and its demonstrated potential, how can industry practices and software platforms further adapt to maximize the benefits of object-level digital authentication in BIM processes? Addressing this question will facilitate continued validation and refinement of the artifact, enabling broader adoption and practical implementation across diverse built asset projects and scenarios.

Throughout this thesis, the adopted stance has consciously avoided oversimplification or undue complexity. The developed artifact represents a balanced, scalable approach, accommodating both detailed analysis and high-level evaluations. Although the proposed framework offers significant benefits, its current application is primarily validated through specific research contexts and industry partnerships. Consequently, its generalizability requires further empirical validation in broader, varied industry settings.

In conclusion, this thesis contributes a valuable, structured method to address object-level data integrity and authentication in the built asset industry, providing practical tools to enhance digital collaboration. Recommendations for future research include further validation of the proposed artifact across diverse BIM platforms and project types, comprehensive testing of various cryptographic algorithms within the modular design of the framework, and exploration of the legal and regulatory implications of implementing object-level digital signatures within the broader built asset industry context.

BIBLIOGRAPHY

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.1943-7862.0001868.

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

Adepoju, O. (2022). Building Information Modelling. In Adepoju, O., Aigbavboa, C., Nwulu, N. & Onyia, M. (Eds.), *Re-skilling Human Resources for Construction 4.0: Implications for Industry, Academia and Government* (ch. 3, pp. 43–64). Cham: Springer International Publishing. doi: 10.1007/978-3-030-85973-2_3.

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.

Alketbi, A., Nasir, Q. & Abu Talib, M. (2020). Novel blockchain reference model for government services: Dubai government case study. *International Journal of System Assurance Engineering and Management*, 11(6), 1170–1191. doi: 10.1007/s13198-020-00971-2.

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.1943-4170.0000219.

Anghel, I. P., Rădulescu, D. & Marinescu, I. A. (2023). Effective Solutions to Prevent Digital Fraud by Introducing Electronic Signature of PDF Files. *2023 24th International Conference on Control Systems and Computer Science (CSCS)*, pp. 186–191. doi: 10.1109/CSCS59211.2023.00037.

Antunes, M., César,Júnior, K., Ribeiro, J., Oliveira, D. & Carvalho, J. (2024). Analysis of IFC interoperability data schema for project representation. *Automation in Construction*, 166. doi: 10.1016/j.autcon.2024.105650.

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/arinc827-1-827-1-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://aviation-ia.sae-itc.com/standards/arinc835-1-arinc-report-835-1-guidance-security-loadable-software-parts-using-digital-signatures.

Arshad, M. F., Thaheem, M. J., Nasir, A. R. & Malik, M. S. A. (2019). Contractual Risks of Building Information Modeling: Toward a Standardized Legal Framework for Design-Bid-Build Projects. *Journal of Construction Engineering and Management*, 145(4), 04019010. doi: 10.1061/(ASCE)CO.1943-7862.0001617.

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.

Azhar, S., Nadeem, A., Mok, j. & Leung, B. (2008). *Building Information Modeling (BIM): A New Paradigm for Visual Interactive Modeling and Simulation for Construction Projects*.

B. Rawat, D., Chaudhary, V. & Doku, R. (2021). Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems. *Journal of Cybersecurity and Privacy*, 1(1), 4–18. doi: 10.3390/jcp1010002.

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: 10.1007/3-540-33173-5.

Bhatt, G. & Bhushan, B. (2020). A Comprehensive Survey on various Security Authentication Schemes for Mobile Touch Screen. *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 248–253. doi: 10.1109/CSNT48778.2020.9115731.

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/rfc7049.

Borrmann, A., Beetz, J., Koch, C., Liebich, T. & Muhic, S. (2018). Industry Foundation Classes: A Standardized Data Model for the Vendor-Neutral Exchange of Digital Building Models. In *Building Information Modeling: Technology Foundations and Industry Practice* (pp. 81–126). Cham: Springer International Publishing. doi: 10.1007/978-3-319-92862-3_5.

Bosselaers, A. & Preneel, B. (1995). RIPEMD. In *Integrity Primitives for Secure Information Systems: Final Report of RACE Integrity Primitives Evaluation RIPE-RACE 1040* (pp. 69–111). Berlin, Heidelberg: Springer. Retrieved from: https://doi.org/10.1007/3-540-60640-8_5.

bSI. (2019a). BIM Collaboration Format (BCF) - buildingSMART International.

bSI. (2019b). bSI Standards - buildingSMART International.

bSI. (2020). openBIM Definition - buildingSMART International.

bSI. (2020). Industry Foundation Classes 4.0.2.1 Version 4.0 - Addendum 2 - Technical Corrigendum 1. Retrieved from: https://standards.buildingsmart.org/IFC/RELEASE/IFC4/ADD2_TC1/HTML/link/chapter-4.htm.

bSI. (2022). IfcObjectReferenceSelect - IFC 4.3.2 Documentation. Retrieved on 2024-05-21 from: https://ifc43-docs.standards.buildingsmart.org/IFC/RELEASE/IFC4x3/HTML/lexical/IfcObjectReferenceSelect.htm.

bSI. (2023a). buildingSMART International. Retrieved on 2024-05-06 from: https://www.buildingsmart.org/.

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

bSI. (2024a). buildingSMART Data Dictionary - buildingSMART International.

bSI. (2024b). buildingSMART/IDS. Retrieved on 2024-05-06 from: buildingSMART.

bSI. (2024c). IFC Validation Service. Retrieved on 2024-05-06 from: https://technical.buildingsmart.org/services/validation-service/.

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

bSI. (2024e). Information Delivery Manual (IDM). Retrieved on 2024-05-06 from: https://technical.buildingsmart.org/standards/information-delivery-manual/.

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

bSI. (2024g). Use Case Management. Retrieved on 2024-05-06 from: https://ucm.buildingsmart.org/?page=1&sort=language&direction=desc.

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

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.

buildingSMART. (2024). buildingSMART International. Retrieved on 2025-03-11 from: https://www.buildingsmart.org/.

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.

Chandurkar, S. N., Gotmare, A. R., Ramchaware, Y., Pawar, V., Mirajkar, R. & Sable, N. (2023). Case Study on Cryptography. *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, pp. 1–8. doi: 10.1109/ICBDS58040.2023.10346489.

Charitou, T., Lallas, E., Gerogiannis, V. & Karageorgos, A. (2024). A Network Modeling and Analysis Approach for Pharma Industry Regulatory Assessment. *IEEE Access*, 12, 46470–46483. doi: 10.1109/ACCESS.2024.3380317.

Chauhan, S. S., Jain, N. & Pandey, S. C. (2022). Digital Signature with Message Security Process. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 182–187. doi: 10.1109/ICACITE53722.2022.9823539.

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.

Chiu, J. & Koeppl, T. (2019). Incentive Compatibility on the Blockchain. In Trockel, W. (Ed.), *Social Design: Essays in Memory of Leonid Hurwicz* (pp. 323–335). Cham: Springer International Publishing. doi: 10.1007/978-3-319-93809-7_20.

Chong, H.-Y. & Cheng, M. (2023). Smart Contract Implementation in Building Information Modeling–Enabled Projects: Approach to Contract Administration. *Journal of Construction Engineering and Management*, 149(5), 05023004. doi: 10.1061/JCEMD4.COENG-13216. Publisher: American Society of Civil Engineers.

Ciccone, A., Di Stasio, S., Asprone, D., Salzano, A. & Nicolella, M. (2022). Application of openBIM for the Management of Existing Railway Infrastructure: Case Study of the Cancello–Benevento Railway Line. *Sustainability (Switzerland)*, 14(4). doi: 10.3390/su14042283.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Gün Sirer, E., Song, D. & Wattenhofer, R. (2016). On Scaling Decentralized Blockchains. *Financial Cryptography and Data Security*, pp. 106–125. doi: 10.1007/978-3-662-53357-4_8.

Decker, H. (2009). Modeling and monitoring the quality of data by integrity constraints and integrity checking. *ICSOFT 2009 - 4th International Conference on Software and Data Technologies, Proceedings*, 2, 207–214.

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.

Dobbertin, H., Bosselaers, A. & Preneel, B. (1996). RIPEMD-160: A strengthened version of RIPEMD. In *Fast Software Encryption* (vol. 1039, pp. 71–82). Berlin, Heidelberg: Springer Berlin Heidelberg.

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.

Dubey, R. & Thingom, C. (2017). An analysis on direct authentication of data. *2017 (ICIMIA)*, pp. 415–418. doi: 10.1109/ICIMIA.2017.7975648.

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,*. Retrieved from: 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.

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W. & Wang, G. (2020). Digital Signature Scheme for Information Non-Repudiation in Blockchain: A State of the Art Review. *EURASIP Journal on Wireless Communications and Networking*, 2020(1), 56. doi: 10.1186/s13638-020-01665-w.

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.

Gamalielsson, J., Jakobsson, F., Lundell, B., Feist, J., Gustavsson, T. & Landqvist, F. (2015). On the Availability and Effectiveness of Open Source Software for Digital Signing of PDF Documents. *11th International Conference on Open Source Systems (OSS)*, AICT-451, 71. doi: 10.1007/978-3-319-17837-0_7.

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.

Ghiro, L., Restuccia, F., D'Oro, S., Basagni, S., Melodia, T., Maccari, L. & Lo Cigno, R. (2021). A blockchain definition to clarify its role for the internet of things. *2021 19th Mediterranean Communication and Computer Networking Conference, MedComNet 2021*, pp. 1–8. doi: 10.1109/MEDCOMNET52149.2021.9501280.

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

Gomez, A. & Gomez, F. (2017). Open BIM Workflow in Project Processes. *Structures Congress 2017: Business, Professional Practice, Education, Research, and Disaster Management - Selected Papers from the Structures Congress 2017*, pp. 14–23. doi: 10.1061/9780784480427.002.

Goswami, P., Singh, M. & Rahman, K. (2021). Digital Signatures. *EAI/Springer Innovations in Communication and Computing*, 243–277. doi: 10.1007/978-3-030-60890-3_14.

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/TIC-STH.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.

Gupta, D. (2017). A new approach of authentication in graphical systems using ASCII submission of values. *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1362–1369. doi: 10.1109/IWCMC.2017.7986483.

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., Krima, S. & Camelio, J. A. (2017). 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.

Hevner, A. & Chatterjee, S. (2010). Introduction to Design Science Research. In Hevner, A. & Chatterjee, S. (Eds.), *Design Research in Information Systems: Theory and Practice* (pp. 1–8). Boston, MA: Springer US. doi: 10.1007/978-1-4419-5653-8_1.

Hevner, A., March, S., Park, J. & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly: Management Information Systems*, 28(1), 75–105. doi: 10.2307/25148625.

Hijazi, A. A., Perera, S., Al-Ashwal, A. M. & Neves Calheiros, R. (2019). Enabling a single source of truth through BIM and blockchain integration. *Proceedings of the 2019 International Conference on Innovation, Technology, Enterprise and Entrepreneurship (ICITEE 2019), 24-25 November 2019, Kingdom of Bahrain*, pp. 385–393. Retrieved from: https://researchdirect.westernsydney.edu.au/islandora/object/uws%3A54569/.

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.1943-7862.0002142.

Hileman, G. & Rauchs, M. (2017). *SSRN Scholarly Paper n°3040224*. Global Blockchain Benchmarking Study. Rochester, NY.

Holland, M., Stjepandić, J. & Nigischer, C. (2018). Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology. *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, pp. 1–8. doi: 10.1109/ICE.2018.8436315.

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.

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.

Ibrahim, F., Shariff, N., Esa, M. & Rahman, R. (2019). The barriers factors and driving forces forbimimplementationin Malaysian AEC Companies. *Journal of Advanced Research in Dynamical and Control Systems*, 11(8 Special Issue), 275–281.

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

ISO29481-1. (2016). ISO 29481-1:2016.

ISO32000-1:2008. (2008). ISO 32000-1:2008. Retrieved on 2024-01-25 from: https://www.iso.org/standard/51502.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.

Iswari, D. A. I. D. & Rudy, D. G. (2023). EXAMINING THE LEGAL STANDING OF DIGITAL SIGNATURES UNDER CIVIL AND ITE LAWS. *POLICY, LAW, NOTARY AND REGULATORY ISSUES*, 2(2), 142–154. doi: 10.55047/polri.v2i2.603.

ITU. (2019). X.509 : Information Technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate Frameworks.

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.

Jaiswal, H., Muddukrishna, B. & Kulyadi, G. (2020). Data integrity violations: A challenge to the pharmaceutical industry. *International Journal of Pharmaceutical Quality Assurance*, 11(1), 196–198. doi: 10.25258/ijpqa.11.1.30.

Jallow, A., Demian, P., Baldwin, A. & Anumba, C. (2014). An Empirical Study of the Complexity of Requirements Management in Construction Projects. *Engineering*, 21. doi: 10.1108/ECAM-09-2013-0084.

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-W5-2024-203-2024.

Jayawardhana, A. & Colombage, S. (2020). Does blockchain technology drive sustainability? An exploratory review. *Developments in Corporate Governance and Responsibility*, 15, 17–42. doi: 10.1108/S2043-052320200000015002.

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.

Kaewunruen, S., Baniotopoulos, C., Guo, Y., Sengsri, P., Teuffel, P. & Bajare, D. (2024). 6D-BIM Applications to Enrich Circular Value Chains and Stakeholder Engagement Within Built Environments. *4th International Conference "Coordinating Engineering for Sustainability and Resilience" & Midterm Conference of CircularB "Implementation of Circular Economy in the Built Environment"*, pp. 346–356. doi: 10.1007/978-3-031-57800-7_32.

Kamara, J., Augenbroe, G., Anumba, C. & Carrillo, P. (2002). Knowledge Management in the Architecture, Engineering and Construction Industry. *Construction Innovation*, 2(1), 53–67. doi: 10.1108/14714170210814685.

Kassim, N., Yusof, Y. & Awang, M. (2016). Reviewing ISO 14649 through iso10303. *ARPN Journal of Engineering and Applied Sciences*, 11(10), 6599–6603.

Kavasidis, I., Lallas, E., Leligkou, H., Oikonomidis, G., Karydas, D., Gerogiannis, V. & Karageorgos, A. (2023). Deep Transformers for Computing and Predicting ALCOA+Data Integrity Compliance in the Pharmaceutical Industry. *Applied Sciences (Switzerland)*, 13(13). doi: 10.3390/app13137616.

Khan, G., Gupta, B. & Gola, K. (2017). MDS3C: Modified digital signature scheme for secure communication. *Advances in Intelligent Systems and Computing*, 479, 309–315. doi: 10.1007/978-981-10-1708-7_36.

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.

Kim, J.-W. (2020). Blockchain technology and its applications: Case studies. *Journal of System and Management Sciences*, 10(1), 83–93.

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.

Kotula, Y. (2023). BIM vs Digital Twin: When and How to Use Them. Retrieved on 2024-01-24 from: https://intelvision.pro/blog/bim-vs-digital-twin-when-and-how-to-use-them/.

Laakso, M. (2009). Developing a multidiscciplinary process view on IFC standardization. In *Managing it in Construction/Managing Construction for Tomorrow* (pp. 487–492). CRC Press. doi: 10.1201/9781482266665-69.

Lakshmanan, M. & Anandha Mala, G. (2024). Merkle tree-blockchain-assisted privacy preservation of electronic medical records on offering medical data protection through hybrid heuristic algorithm. *Knowledge and Information Systems*, 66(1), 481–509. doi: 10.1007/s10115-023-01937-z.

Lakshmi Triveni, K., Balamuralidhara, V. & Pramod Kumar, T. (2017). Data integrity in clinical trials: An overview. *Pharma Times*, 49(6), 14–18.

Lax, G., Buccafurri, F. & Caminiti, G. (2015). Digital Document Signing: Vulnerabilities and Solutions. *Information Security Journal: A Global Perspective*, 24(1-3), 1–14. doi: 10.1080/19393555.2014.998843.

Lee, Y.-C., Eastman, C., Solihin, W. & See, R. (2016a). 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., Eastman, C. M. & Solihin, W. (2016b). An ontology-based approach for developing data exchange requirements and model views of building information modeling. *Advanced Engineering Informatics*, 30(3), 354–367. doi: 10.1016/j.aei.2016.04.008.

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.

legisquebec. (2024). Act to Establish a Legal Framework for Information Technology. Retrieved on 2023-12-07 from: https://www.legisquebec.gouv.qc.ca/en/document/cs/C-1.1.

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.

Li, J., Greenwood, D. & Kassem, M. (2019). Blockchain in the Built Environment and Construction Industry: A Systematic Review, Conceptual Models and Practical Use Cases. *Automation in Construction*, 102, 288–307. doi: 10.1016/j.autcon.2019.02.005.

Lin, W. (2023). Digital Signature. In *Trends in Data Protection and Encryption Technologies* (pp. 77–81). Cham: Springer Nature Switzerland. doi: 10.1007/978-3-031-33386-6_15.

Liu, X. & Xie, H. (2014). Research on the anticipation and development of building information modeling. *Applied Mechanics and Materials*, 584-586, 1881–1884. doi: 10.4028/www.scientific.net/AMM.584-586.1881.

Longhurst, S. (2010). Data integrity - The core of a successful data warehouse. *EngineerIT*, 18.

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*.

McNamara, A. J. & Sepasgozar, S. M. E. (2021). Intelligent Contract Adoption in the Construction Industry: Concept Development. *Automation in Construction*, 122, 103452. doi: 10.1016/j.autcon.2020.103452.

Microsoft. (2022). GZipStream Class (System.IO.Compression). Retrieved on 2024-10-03 from: learn.microsoft.com/en-us/dotnet/api/system.io.compression.gzipstream.

Mogos, G. (2008). Security of QImage file. *Proceedings of the 2008 International Conference on Computer Design, CDES 2008*, pp. 53–56.

Mohammad, W., Abdullah, M., Ismail, S. & Takim, R. (2019). Technology-Organisation-Environment Framework for Building Information Modelling (BIM) Adoption Challenges for Contractor's Organisations in Malaysia. *Journal of Computational and Theoretical Nanoscience*, 16(5-6), 2282–2288. doi: 10.1166/jctn.2019.7885.

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.

Mulder, V., Mermoud, A., Lenders, V. & Tellenbach, B. (Eds.). (2023). *Trends in Data Protection and Encryption Technologies*. Cham: Springer Nature Switzerland. doi: 10.1007/978-3-031-33386-6.

Nawari, N. O. & Ravindran, S. (2019). Blockchain and the built environment: Potentials and limitations. *Journal of Building Engineering*, 25, 100832. doi: 10.1016/j.jobe.2019.100832.

NBIMS-USTM. (2023). NBIMS-USTM COBie v3 Standard.

Nieles, M., Dempsey, K. & Pillitteri, V. (2017). *NIST SP 800-12 Rev. 1 An Introduction to Information Security* (Report n°NIST Special Publication (SP) 800-12 Rev. 1). Retrieved on 2025-02-03 from: https://csrc.nist.gov/pubs/sp/800/12/r1/final.

of Standards and Technology, N. I. (2015). *Secure Hash Standard (SHS)* (Report n°Federal Information Processing Standard (FIPS) 180-4). Retrieved on 2024-10-02 from: https://csrc.nist.gov/pubs/fips/180-4/upd1/final.

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.

Oluwole Alfred,OLATUNJI, O. (2011). A PRELIMINARY REVIEW ON THE LEGAL IMPLICATIONS OF BIM AND MODEL OWNERSHIP. *Electronic Journal of Information Technology in Construction*, 16, 687–696.

openBIM-bSI. (2025). openBIM - buildingSMART International. Retrieved on 2025-03-11 from: https://www.buildingsmart.org/about/openbim/.

Park, J. (2024). Framework for Managing Multiple Common Data Environments. *Construction Research Congress 2024, CRC 2024*, 1, 1117–1127. doi: 10.1061/9780784485262.114.

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. (2022). "Patiyoot" Cryptography Authentication Protocol for Computer Network. *2022 International Electrical Engineering Congress (iEECON)*, pp. 1–3. doi: 10.1109/iEECON53204.2022.9741669.

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.

PDF/A-3. (2020). PDF/A-3, PDF for Long-term Preservation, Use of ISO 32000-1, With Embedded Files [web page]. Retrieved on 2024-07-21 from: https://www.loc.gov/preservation/digital/formats/fdd/fdd000360.shtml.

Peffers, K., Tuunanen, T., Rothenberger, M. & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), 45–77. doi: 10.2753/MIS0742-1222240302.

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.

Phansalkar, S., Mishra, D., Chaube, N. & Sonkamble, R. (2023). Towards Adoption of Green Blockchain with Emphasis on Blockchain Type, Consensus Protocols, Data Sharding and Smart Contracts. *2023 IEEE International Conference on Blockchain and Distributed Systems Security, ICBDS 2023*, pp. 1–8. doi: 10.1109/ICBDS58040.2023.10346419.

Poirier, E. A., Forgues, D. & Staub-French, S. (2014). Dimensions of Interoperability in the AEC Industry. 1987–1996. doi: 10.1061/9780784413517.203.

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 . *Construction Research Congress 2020: Computer Applications*, 1174–1183. doi: 10.1061/9780784482865.124.

Preidel, C., Borrmann, A., Mattern, H., König, M. & Schapke, S.-E. (2018). Common data environment. In *Building Information Modeling: Technology Foundations and Industry Practice* (pp. 279–291). Springer International Publishing. doi: 10.1007/978-3-319-92862-3_15.

R. Alagheband, M. & Mashatan, A. (2022). Advanced Digital Signatures for Preserving Privacy and Trust Management in Hierarchical Heterogeneous IoT: Taxonomy, Capabilities, and Objectives. *Internet of Things (Netherlands)*, 18. doi: 10.1016/j.iot.2021.100492.

Raglin, A. & Moraffah, R. (2023). Data Integrity and Artificial Reasoning. *Proceedings - 2023 IEEE 5th International Conference on Cognitive Machine Intelligence, CogMI 2023*, pp. 93–96. doi: 10.1109/CogMI58952.2023.00022.

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.

RAIC. (2020/2022). Part 6 : Phases of the Design Project. In *The Canadian Handbook of Practice for Architects*. Royal Architectural Institute of Canada.

Ramadhan, M., Mandala, S. & Yulianto, F. (2023). Analysis and Implementation of Digital Signature Algorithm in PDF Document. *2023 11th International Conference on Information and Communication Technology, ICoICT 2023*, 2023-August, 11–16. doi: 10.1109/ICoICT58202.2023.10262708.

Rivest, R. L. (1992). *The MD5 Message-Digest Algorithm* (Report n°RFC 1321).

Roddis, W., Matamoros, A. & Graham, P. (2006). Interoperability in building construction using exchange standards. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4200 LNAI, 576–596. doi: 10.1007/11888598_52.

Roy, D. A. & Karforma, S. (2012). A Survey on Digital Signatures and Its Applications. *JCIT*, 3, 45–69.

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: 10.52711/0974-360X.2024.00381.

Sabeena, S. & Vijila, S. (2024). Blockchain-based Solution for Securing Job Card Data Integrity and Payment System using Bi-Quad Merkle Tree. *International Journal of Intelligent Systems and Applications in Engineering*, 12(12s), 314–328.

Sadkhan, S. B. & Sadkhan, R. S. B. (2022). Analysis of Different Types of Digital Signature. *2022 8th International Engineering Conference on Sustainable Technology and Development (IEC)*, pp. 241–246. doi: 10.1109/IEC54822.2022.9807502.

Sagar Hossen, M., Tabassum, T., Ashiqul Islam, M., Karim, R., Rumi, L. & Kobita, A. (2021). Digital signature authentication using asymmetric key cryptography with different byte number. *Lecture Notes on Data Engineering and Communications Technologies*, 53, 845–851. doi: 10.1007/978-981-15-5258-8_78.

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.

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.

Saurabh Bhausaheb Gawali. (2023). A Comprehensive Study on Digital Signatures. *International Journal of Advanced Research in Science, Communication and Technology*, 37–39. doi: 10.48175/IJARSCT-11608.

Secretariat Treasury Board of Canada. (2021). Government of Canada Guidance on Using Electronic Signatures. Retrieved on 2023-03-27 from: https://www.canada.ca/en/government/system/digital-government/online-security-privacy/government-canada-guidance-using-electronic-signatures.html.

See, R., Karlshoej, J. & Davis, D. (2012). An Integrated Process for Delivering IFC Based Data Exchange. buildingSMART International, BLIS Consortium.

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.

Shehzad, H. M. F., Ibrahim, R. B., Yusof, A. F., Khaidzir, K. A. M., Iqbal, M. & Razzaq, S. (2021). The Role of Interoperability Dimensions in Building Information Modelling. *Computers in Industry*, 129, 103444. doi: 10.1016/j.compind.2021.103444.

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.

Sridhar, A. & Mamatha, H. R. (2021). Keystroke Dynamics for User Verification. *Evolutionary Computing and Mobile Sustainable Networks*, pp. 127–136. doi: 10.1007/978-981-15-5258-8_14.

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

Sultana, R. (2021). A Survey on Digital Signatures.

Sumukha Krishna, P., Hemanth Kumar, S. & Gangadharappa, H. (2020). A review and analysis of data integrity: Pharmaceutical industry perspective. *International Journal of Pharmaceutical Research*, 12(1), 940–948. doi: 10.31838/ijpr/2020.12.01.068.

Sun, C., Jiang, S., Skibniewski, M., Man, Q. & Shen, L. (2017). A literature review of the factors limiting the application of BIM in the construction industry. *Technological and Economic Development of Economy*, 23(5), 764–779. doi: 10.3846/20294913.2015.1087071.

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.

Tanwar, S. & Kumar, A. (2019). An efficient and secure identity based multiple signatures scheme based on RSA. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(6), 953–971. doi: 10.1080/09720529.2019.1632024.

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.

Tribelsky, E. & Sacks, R. (2011). An Empirical Study of Information Flows in Multidisciplinary Civil Engineering Design Teams Using Lean Measures. *Architectural Engineering and Design Management*, 7(2), 85–101. doi: 10.1080/17452007.2011.582332.

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

Vadgama, N. (2019). Distributed Ledger Technology in the Supply Chain. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3921895.

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.

Velásquez, I., Caro, A. & Rodríguez, 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.

Venugopal, M., Eastman, C., Sacks, R. & Teizer, J. (2012). Semantics of model views for information exchanges using the industry foundation class schema. *Advanced Engineering Informatics*, 26(2), 411–428. doi: 10.1016/j.aei.2012.01.005.

Vitiello, U., Ciotta, V., Salzano, A., Asprone, D., Manfredi, G. & Cosenza, E. (2019). BIM-based approach for the cost-optimization of seismic retrofit strategies on existing buildings. *Automation in Construction*, 98, 90–101. doi: 10.1016/j.autcon.2018.10.023.

Volker, L. & Chao-Duivis,M.A.B. (2010). Potential Conflicts with Procurement Law during Architect Selection. *W113-Special Track 18th CIB World Building Congress*, pp. P 346.

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

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.

X.520, I. (2019). X.520 : Information Technology - Open Systems Interconnection - The Directory: Selected Attribute Types.

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.

Xu, M., Guo, Y., Liu, C., Hu, Q., Yu, D., Xiong, Z., Niyato, D. & Cheng, X. (2024). Exploring Blockchain Technology through a Modular Lens: A Survey. *ACM Computing Surveys*, 56(9). doi: 10.1145/3657288.

Xu, Y., Tao, X., Das, M., Kwok, H. H. L., Liu, H., Wang, G. & Cheng, J. C. P. (2023). Suitability Analysis of Consensus Protocols for Blockchain-Based Applications in the Construction Industry. *Automation in Construction*, 145, 104638. doi: 10.1016/j.autcon.2022.104638.

Xue, F. & Lu, W. (2020). A Semantic Differential Transaction Approach to Minimizing Information Redundancy for BIM and Blockchain Integration. *Automation in Construction*, 118, 103270. doi: 10.1016/j.autcon.2020.103270.

Yemm, S. (2019). Maintaining Data Integrity in the Lab With ELNs. *Informatics from Technology Networks*.

Yu, J., Zhong, H. & Bolpagni, M. (2023a). Integrating blockchain with building information modelling (BIM): a systematic review based on a sociotechnical system perspective. *Construction Innovation*, 24(1), 280–316. doi: 10.1108/CI-04-2023-0082. Publisher: Emerald Publishing Limited.

Yu, Y., Zhang, Y., Yu, J. & He, X. (2023b). 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. (2023c). 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.

Yushasman, Y., Rizal, A., Lee, Y. & Rahman, R. (2024). Trust Issues in BIM-Based Construction Projects: A Systematic Literature Review. *Lecture Notes in Civil Engineering*, 381, 559–566. doi: 10.1007/978-3-031-39663-2_46.

Zhang, J. & Chen, H. (2010). Secuirty storage in the cloud computing: A RSA-based assumption data integrity check without original data. *ICEIT 2010 - 2010 International Conference on Educational and Information Technology, Proceedings*, 2, V2143–V2147. doi: 10.1109/ICEIT.2010.5607505.

Zhang, L., Pan, Y., Wu, X. & Skibniewski, M. J. (2021). Process Mining. In Zhang, L., Pan, Y., Wu, X. & Skibniewski, M. J. (Eds.), *Artificial Intelligence in Construction Engineering and Management* (pp. 147–172). Singapore: Springer. doi: 10.1007/978-981-16-2842-9_7.

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.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X. & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 14(4), 352–375. doi: 10.1504/IJWGS.2018.095647.

Zhu, W.-T. & Lin, J. (2016). Generating Correlated Digital Certificates: Framework and Applications. *IEEE Transactions on Information Forensics and Security*, 11(6), 1117–1127. doi: 10.1109/TIFS.2016.2516818.