Optimal Construction Management & Production Control

D1.6 – Ethics & Privacy, Information Security

WP1 – Digital Building Twin Process

Issue date:	08/04/2022
Author(s):	Mikel Borràs, Jorge Leao (IDP)
Editor:	Mikel Borràs (IDP)
Lead Beneficiary:	16 - IDP
Dissemination level:	Public
Type	Report
Reviewers:	Carla Tortelli (ACCIONA), Tomi Pitkäranta (FIRA)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 958398

BIM2TWIN KEY FACTS

Project title	BIM2TWIN: Optimal Construction Management & Production Control
Starting date	01/11/2020
Duration in months	42
Call (part) identifier	H2020-NMBP-ST-IND-2020-singlestage
Topic	LC-EEB-08-2020 Digital Building Twins (RIA)
Fixed EC Keywords	-
Free keywords	Digital Twin; Graph database; BIM; IA; Machine Learning; Image recognition; process optimization; safety improvement
Consortium	17 organizations

BIM2TWIN CONSORTIUM PARTNERS

	Partner	Country
1	CSTB: CENTRE SCIENTIFIQUE ET TECHNIQUE DU BATIMENT	FR
2	TECHNION: ISRAEL INSTITUTE OF TECHNOLOGY	IL
3	UNIVERSITY OF CAMBRIDGE	UK
4	TUM: TECHNISCHE UNIVERSITAET MUENCHEN	DE
5	INRIA: INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE	FR
6	FIRA GROUP OY	FI
7	INTSITE LTD	IL
8	FUNDACION TECNALIA RESEARCH & INNOVATION	ES
9	ACCIONA CONSTRUCCTION SA	ES
10	RUHR-UNIVERSITAET BOCHUM	DE
11	SPADA CONSTRUCTION	FR
12	UNIVERSITA POLITECNICA DELLE MARCHE	IT
13	UNISMART – FONDAZIONE UNIVERSITÀ DEGLI STUDI DI PADOVA	IT
14	ORANGE SA	FR
15	SIEMENS AKTIENGESELLSCHAFT	DE
16	IDP INGENIERIA Y ARQUITECTURA IBERIA SL	ES
17	AARHUS UNIVERSITET	DK

DISCLAIMER

EXECUTIVE SUMMARY

The ultimate goal of the BIM2TWIN project is the reduction of all kinds of operational waste, schedule shortenings, cost reductions, quality and safety improvement, and carbon footprint reduction. Furthermore, it consists of a Digital Building Twin (DBT) platform for construction management that provides full simulation awareness and extensive sets for construction management applications.

BIM2TWIN is an EU special innovation project that will create a Digital Building Twin (DBT) platform for construction site management with artificial intelligence (AI) and semantically linked data techniques. The Digital Building Twin (DBT) will offer a programming interface application allowing construction management applications to interoperate with its data, information, and knowledge bases. The platform will provide a complete situational insight on the as-built product and as-performed processes, which will be used and compared to the as-designed applications to implement a close-loop plan-do-check-act process. This entire process will rely on multiple onsite sensors for data acquisition, cross-domain analysis, and complex AI-based event processing.

The Digital Building Twin platform will support decentralized data storage, related services, and APPs located in various locations. This deliverable has been written in work package one to develop, implement, and test the platform usages in a platform-as-a-service (PaaS) to be applied in the BIM2TWIN project. Underlining interoperability, the utilized and developed services communicate through agreed APIs and prevailing data formats.

The primary purpose of this deliverable is the introduction of concepts adopted by the Digital Building Twin platform concerning security and privacy issues by first looking at the data security aspects to follow a cybersecurity paradigm representing confidentiality, integrity, and availability of the BIM2TWIN data while also taking a closer look at the legal roles involved in data handling established in the GDPR (General Data Protection Regulation) focusing primarily on the main concern of the BIM2TWIN project "real-time" monitoring and personal data protection of the on-site personnel through a video anonymization process; nevertheless, a GDPR consent form is also introduced to inform all the participant on what will be done, how the extracted data from hardware/sensors previously installed on the job-site will be handled, stored, and discarded. Next, this document deep dives into the cybersecurity aspects to consider protecting the BIM2TWIN platform from cybercrimes by establishing a high-level architecture for cybersecurity as well as establishing the knowledge required by anyone with access to the BIM2TWIN platform stored data about cybercrimes, cybercrimes techniques, famous cyber-attacks, and cyber security prevention. Furthermore, besides only educating any party that can gain access to the BIM2TWIN stored data there are security audits and tastings (e., penetration testing and vulnerability or security scans) that the BIM2TWIN partners can use to test the overall cybersecurity integrity of the platform. Lastly, this document describes the cybersecurity technologies implemented in the BIM2TWIN project like cryptography, identity verification, user authentication, digital certificates and chain of trust, connection level of security, and web application firewall in other to further protect the integrity of the data stored in the BIM2TWIN platform.

The primarily targeted audience of this report is the BIM2TWIN's partners for guidance towards concrete development and implementation actions for the platform, tools, and validated pilots. The secondary audience is the professional parties interested in privacy efficiency and security practices in implementing the Digital Building Twin concept. This text requires a baseline contextual understanding of the project and technology; moreover, it's written in a technical style that could limit the knowledge of some interested groups.

TABLE OF CONTENTS

BIM2TWIN KEY FACTS **2**
BIM2TWIN CONSORTIUM PARTNERS **2**
EXECUTIVE SUMMARY **3**
TABLE OF CONTENTS **4**
LIST OF FIGURES **6**
ABBREVIATIONS **6**
1 INTRODUCTION **8**
1.1 Purpose and target groups 8
1.2 Contributions of partners 8
1.3 Relations to other activities 9
2 DATA PRIVACY, ETHICS, AND POLICIES **10**
2.1 Data privacy and ethics 10
2.2 Data policies 12
2.3 Data security 12
2.4 GDPR 13
3 ETHICS AND PRIVACY MEASURES IN BIM2TWIN **14**
3.1 GDPR on video surveillance and other hardware/sensors monitoring 14
3.2 BIM2TWIN on video surveillance and other hardware/sensors monitoring 15
4 CYBERSECURITY **17**
4.1 High-level architecture for cybersecurity 18
4.2 Cybercrimes 20
4.3 Cybercrime techniques 21
4.4 Famous cyber attacks 23
4.5 Cyber security prevention 24
4.6 Security audits 26
4.7 Penetration testing 28
4.8 Vulnerability or security scans 31
5 CYBERSECURITY TECHNOLOGIES IN THE BIM2TWIN PROJECT **33**
5.1 Cryptography 33
5.2 Identity verification 33
5.3 User authentication 33
5.4 Digital certificates and chain of trust 34
5.5 Connection levels of security 35

5.6 Web application firewall 36
6 **CONCLUSION..... 40**
6.1 Summary of achievements..... 40
6.2 Relation to continued developments..... 40
REFERENCES..... 42
ANNEX-1 – CONSENT FORM..... 43

LIST OF FIGURES

Figure 1. BIM2TWIN cybersecurity architecture 18
Figure 2. BIM2TWIN high-level security architecture 19
Figure 3. Authentication and authorization feature 20
Figure 4. How a WAF works ..... **Erreur ! Signet non défini.**
Figure 5. IPS and WAF overview ..... **Erreur ! Signet non défini.**
Figure 6. Chain of Trust process 34

ABBREVIATIONS

B2T	BIM2TWIN
DBT	Digital Building Twin
DBTP	Digital Building Twin Platform
AI	Artificial Intelligence
EEB	Energy Efficient Building
PaaS	Platform-as-a-service
GDPR	General Data Protection Regulation
EU	European Union
BIM	Building Information Model
R&D	Research and Development
AES	Advanced Encryption Standard
API	Application Programming Interface
CDN	Content Distribution Network
DES	Data Encryption Algorithm
DNS	Domain Name System
DDoS	Distributed Denial of Service
DoS	Denial-of-Service
EEB	Energy Efficient Building
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HMAC	Hash Message Authentication Codes
HTTPS	Hypertext Transfer Protocol Secure
ICA	Intermediate Certificate Authorities
IPS	Intrusion Prevention System
ISSAF	Information System Security Assessment Framework
MFA	Multi-Factor Authentication
NGFW	Next Generation Fire Wall
NIST	National Institute of Standards and Technology
OSSTMM	Open-Source Security Testing Methodology Manual
PEP	Policy Enforcement Point
PIA	Privacy Impact Assessment
PTES	Penetration Testing Execution Standard
RCA	Root Certificate Authority
RDP	Remote Desktop Protocol

SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TELNET	Teletype Network
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WAF	Web Application Firewall

1 INTRODUCTION

1.1 Purpose and target groups

The primary purpose of this deliverable is to summarize the privacy and security risk to find suitable general approaches and standards to prevent them. The principal targeted audience of this deliverable is the BIM2TWIN partners, to use as guidance towards concrete actions in the development implementation of the Digital Building Twin platform and tools used in this and subsequent work packages.

Professional parties interested in Digital Twins for construction site management with artificial intelligence (AI) and semantically linked data techniques and utilizing BIM technologies more efficiently in the future are the secondary target group for this deliverable. Since this is a technical document, it will demand a baseline technical understanding of the privacy and security topics, creating difficulties and limitations in understanding certain interested groups such as end-users.

The targeted groups for this deliverable include the following professional parties expressly:

- Transversal Professionals involved in the construction business
- Construction and engineering companies
- Municipalities and policymakers
- Information managers in the architectural, engineering, and construction industry
- Construction management consulting firms
- End-users
- Industry and associations
- Scientific community

1.2 Contributions of partners

This deliverable has been written as an outcome of a collaborative effort between all consortium partners. The contributions of the involved partners to the various sections are explained in the following table:

Tasks Carried Out	Chapters	Involved Partners(s)
Preparation and writing of general parts	All	IDP
Preparation and content writing	All	IDP
General parts and structure development	All	IDP
Technical additions, especially for single sign-on	All	IDP
Conclusions	All	IDP
List of Acronyms and Glossary	All	IDP
References	All	IDP
Review with comments	All	IDP

1.3 Relations to other activities

This deliverable is related to the entire BIM2TWIN project and the activities underwent within every work package. However, it affects above all the activities, tasks, and deliverables to be carried out under WPs 2, 3, 4, 5, 6, and 7 as these are the technical work packages that will address the development of the platform as well as other tools to optimize the construction stage, process, and planning of the different demo sites', this meaning they will require the provision and sharing of data.

2 DATA PRIVACY, ETHICS, AND POLICIES

This chapter looks at data privacy, its importance, and data privacy controls to help preserve the integrity of exploited personal information in the BIM2TWIN project. This chapter also explains the importance of having security policies to ensure the continued successful security of operations, managing various topics concerning data flows in and out of the web service, and handling data inside a system. Also, this chapter also the data security aspects to follow a cybersecurity paradigm representing confidentiality, integrity, and availability of the BIM2TWIN data. Lastly, this chapter has a closer look at the two legal roles involved in handling data in a system established in the GDPR (General Data Protection Regulation).

2.1 Data privacy and ethics

Data privacy generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. This personal information can be one's name, location, contact information, or online or real-world behavior. Just as someone may wish to exclude people from a private conversation, many online users want to control or prevent certain types of personal data collection.

As Internet usage has increased over the years, so has the importance of data privacy. Websites, applications, and social media platforms often need to collect and store personal data about users to provide services. However, some applications and platforms may exceed users' expectations for data collection and usage, leaving users with less privacy than they realized. Other apps and platforms may not place adequate safeguards around the data they collect, resulting in a data breach that compromises user privacy.

Data privacy controls help maintain confidentiality because it guarantees that only users of the BIM2TWIN platform will have access to the respective data originally written (sometimes with different software like the one reading the data on the second step) or users with access to the data given by either the data originators or with a user group concept.

- **The Least Privilege Principle**, strong guidance for maintaining confidentiality, ensuring only the bare minimum access permission required to complete a task is guaranteed for the user; moreover, if users are granted access permits, exploitation opportunities should be minimized.
- **Regular Rotation of Security Keys and Certificates**, as security keys are the root of the security infrastructure, a handling procedure should be in place to ensure that a single actor won't compromise the system.
- **Compartmentalization**, as a security engineering concept, means that the person or application requesting data will only be able to access the one needed to complete their task. As a result, exposure potential will be limited, or even in the case of a data breach, the damage could be minimized.
- **Data Distortion** will ensure that an untrusted party releases company data (or pattern extracted from data); this party won't learn any of the company's sensitive information or re-identify company users. It is achieved through controlled data distortion/modification preserving specific characteristics (defined as utilities) of the data, e.g., statical properties.
- **Monitoring** will allow individual actions to be traced with user IDs to sensitive changes.
- **Only Saving Necessary Data**, temporary information needed to execute requests that are not important for further use, shouldn't be saved in the Cloud Storage.
- **Video anonymization**. Whenever placing video cameras at a construction site, collecting data regarding the workers on site, video footage should be treated so that workers are anonymized and cannot be identified by others. If no video anonymization is applied, BIM2TWIN organizations should tackle construction site onboarding, asking workers' consent to use their data. All workers participating in Demo Sites must sign this data consent if Video footage is to

be used within the BIM2TWIN project. In the related Privacy Policy, it must be clear that the data will be used to "ensure safe, efficient and quality execution on-site and to perform production management activities and to follow worker presence at the site". The BIM2TWIN project will implement a video anonymization method programmed on the local PC installed on the building pilot demosite which will process all the data exploited from the site in which all videos and photos in which persons faces are detected will be overridden to blur their faces. This video anonymization method consists of a pre-trained neural network to detect persons on pictures (open source from TensorFlow) from which the BIM2TWIN partner TUM will code to program the local PC to blur all sections in the photos and videos where persons are detected.

- **Oblige to inform**. Workers should be previously notified or representatives about the user system and its result. Any worker or personnel participating in the BIM2TWIN project will be required to sign a consent form through which they are informed the purpose of the research project, what's expected from them during the duration of the project, their rights to withdraw from the research at any time, their rights to confidentiality and privacy, the benefits of the BIM2TWIN project, possible risks of the BIM2TWIN project, and data dissemination and sharing intend of the exploited data from the building pilot site. See annex for the first draft of the consent form.
- **Data responsibility**. The captured images are personal data, implying that those affected must be informed about personal processing data. The related company must be responsible for the data and has the obligation of keeping updated records or treatment activities of the data. Furthermore, the processing data company must answer for any exercise of rights that might come their way.
- **Data treatment system**. If they are Acciona's cameras and systems, an evaluation of the technical requirements of the cameras and systems must be made. Suppose they are cameras from an external supplier. In that case, a data processing contract must be signed with this supplier and evaluate the technical requirements of the resources used.
    - Images may only be used for the purpose for which they are reported and for which they are intended.
    - It is necessary to assess whether converting images into data is done in real-time or requires someone's intervention.
    - Another assessed aspect is the location and number of cameras to be installed to comply as far as possible with the principle of data minimization.
- **Security measures**. Security and cybersecurity measures must be adopted for the system, not only for data protection but also for information security.

In the context of responsible sharing of construction-related data, these rights translate into the principle that information sharing coming from design, models, and other potential intellectual property, is an ethical contract that the involved parties have signed, and they lead to the core elements for responsible data sharing, which include:

- transparency
- accountability
- data quality and security
- privacy, data protection, and confidentiality
- risk-benefit analysis
- recognition and attribution
- education and training
- accessibility and dissemination

2.2 Data policies

Data policies should ensure the continuous successful security of operations, managing various topics concerning data flows in and out of the web service, and handling data inside a system. Furthermore, these policies should consist of automated validations, parameters monitoring, or work instructions.

Strong password policies should be in place for authentication. Whenever possible, multifactor authentication (MFA) should be in place; adding a physical token to the already strong password will increase the complexity of log copy. Additionally, a certain complexity should be required on the passwords to ensure users are using non-common or not-easy-to-crack passwords. Also, a regular password change should be necessary, as the risk of password compromise increases exponentially over time.

Password databases should be stored using a one-way hash to ensure that passwords won't be reverse-engineered to prevent the usage of common lookups tables and stand-out duplicate passwords in the database. Each password must include a random character to protect the database against brute force attacks. Furthermore, the hash function used for password protection should be implemented many times, as this hardening of the authentication system will increase the protection against brute force attacks.

Other examples of data policy topics are:

- Policies considering which sources could be accepted as trustworthy.
- Policies monitoring methodology changes impacting security.
- Policies ensuring that routine maintenances are being performed.
- Policies containing response plans to handle security incidents.

2.3 Data security

CIA Triad is a cybersecurity paradigm representing Confidentiality (preventing the extraction of information), Integrity (avoiding the modification of data), and Availability (ensuring access to the desired data and related services).

Data confidentiality

The principal meaning of data confidentiality is the restrictive information accessibility for non-authorized parties. Furthermore, to ensure that data could not be read during network communications, extracted from secure data repositories, or read by a non-authorized user.

Data confidentiality has a close-knit relationship with privacy. Privacy relates to controlling access to information to one's personal information; additional actors could violate privacy by sharing the information they have been granted access to. A confidentiality breach will quickly lead to privacy violation, but not necessarily a violation of the confidentiality principle (it could be rather a social or legal issue).

Data confidentiality includes data transportation layers security. For example, attackers could gain access to communications sent over the internet and attend to retrieve its content. E.g., to gain knowledge of competitors' secrets or obtain information about subsequent attacks.

Data integrity

Data integrity is the overall completeness, accuracy, and consistency of data. Ensuring that information couldn't be modified, altered, or deleted, because this could impact BIM2TWIN and its client's data, injecting doubt in data quality or resulting in vital business data loss.

For example, attackers could create their own communication network to create false records, edit existing records, or delete records.

Data availability

Data availability is the process of ensuring that data is available to end-users and applications when and where they need it. Data availability relates to data insurance because attackers could attempt a Denial-of-Service (DoS) attack—eliminating or slowing down data services by a capacity overburdening, the most common attack to generate massive financial losses for the targeted company.

For example, attackers could generate massive network traffic to occupy the targeted computer resources and consume enough resources that won't allow the necessary number of resources to handle legitimate communications correctly. Additionally, attackers could shut down the compromised computer resources and hardware to the complete cessation of operations.

All the presented above issues regarding privacy, ethics, and policies, among other things, is why the General Data Protection Regulation, in short GDPR, exists.

2.4 GDPR

The GDPR, General Data Protection Regulation differentiates between two roles of legal persons involved in handling data in a system. Namely, these persons are the Data Controller defined as "the natural or legal person, public authority, agency or other body which, alone, or jointly with others, determines the purposes and means of processing personal data"(Information Commissioner's office, 2016). The other legal role is the Data Processor, defined as "the natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller"(Information Commissioner's office, 2016).

Who is the data controller, and who is the only data processor?

The Data Controller decides on the "purposes" and "means" of the personal data processing. In other words, the "why" and "how" of the processing identifying the party fulfilling this role, the following questions can be investigated:

- In which specific context does the data processing take place?
- Who decides on the purpose of personal data processing? Does the party process data on its behalf, or were other parties asked to do so? To answer this, an analysis should determine which actors are involved in the processing of the data and what role they fulfill.
- Who decides on the technical ways and organizational elements of data processing? The controller gives guidelines for questions like:
    - Which data should be processed?
    - For how long is the data stored?
    - Who shall have access to the data?
- What are the contractual relations between the different parties involved in the processing? The answer to this question is particularly useful in complex environments where other actors tend to see themselves as "facilitators" and have no responsibility for the data, which can be determined.
- If a contract between parties is vague about who the controller is, are there elements from which the conclusion may be extracted?

Partners and tasks from WP2 oversee capturing and the pre-processing of data and data integration and development of the platform. These partners address the data controlling and processing issues found in the BIM2TWIN project.

3 ETHICS AND PRIVACY MEASURES IN BIM2TWIN

This chapter has a closer look at the GDPR concerning video monitorization and the different points that the BIM2TWIN partners have to tackle to install video surveillance equipment, as well as various monitoring hardware/sensors in the job site allowing the BIM2TWIN partners to monitor the work and activities being performed by the workers on the job site.

Furthermore, this chapter also provides the BIM2TWIN solutions established by the partners to solve the video surveillance and monitorization by using various hardware/sensors installed in the BIM2TWIN pilot sites.

Lastly, this chapter includes the consent form template required to be signed by on-site personnel participating in the project. This may be updated under Task 8.2 with any further requests by B2T Demo Site Owners and/or partners.

3.1 GDPR on video surveillance and other hardware/sensors monitoring

Video surveillance and additional hardware/sensors monitoring are points to tackle before implementing this technology on the construction site because exploiting this technology without informing the parties/persons to be "monitored" goes against The General Data Protection Regulation (GDPR).

The law states that the whole purposes of the processing have to be specified in detail in Article 5 - Principles relating to the processing of personal data(1-b) of the General Data Protection Regulations, stating that:

> *Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').* (European Parliament and Council of the European Union, 2016a)

Additionally, the monitoring purposes should be documented in writing and need to be specified for every surveillance camera in use; cameras used for the same objective by a single controller can be documented together, as long as every camera in use has a documented purpose this is stated in Article Principles relating to the processing of personal data (section 2) of the General Data Protection Regulations, stating that:

> *The controller shall be responsible for and demonstrate compliance with paragraph 1 ('accountability').* (European Parliament and Council of the European Union, 2016a)

Furthermore, data subjects must be informed of the purpose(s) of the processing following Article 13 - Information to be provided where personal data are collected from the data subject (Recital 60 – Information Obligation) of the General Data Protection Regulations, stating that:

> *The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed.* (European Parliament and Council of the European Union, 2016c)

Lastly, personal data shall be processed lawfully, fairly, and transparently concerning the data subject in accordance with Article 5 - Principles relating to the processing of personal data (1-a) of the General Data Protection Regulations, stating that:

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, and transparency). (European Parliament and Council of the European Union, 2016a)

All these regulations for video surveillance were considered at the time of writing this document.

3.2 BIM2TWIN on video surveillance and other hardware/sensors monitoring

The main purpose of the use of video surveillance and implementation of other hardware/sensors used for monitoring on the BIM2TWIN project are:

- Enable **real-time response to critical conditions on-site**, primarily of two kinds: a) safety hazards, such as when a worker mistakenly enters the zone of operation of a bulldozer, or b) quality control, such as when a precast component is being placed accurately in position using laser scan control.
- Support **evaluation of the current state compared to the intended state** at any point in time. These are value judgments that must answer questions relating to the product (such as "Is the wall in the right place and of the right size?"; "Is the wall built of the right materials and is it's surface planar?") and relating to process (such as "Is the wall masons' productivity too low or as expected?" "Is the project ahead of, on, or behind schedule?"; "Is the project on budget?"). To do this, one must be able to compare an as-designed/as-planned version for any point in time with the as-built/as performed model of the same point in time. PSM information is compared to BIM information.
- Support **simulation of future states** based on the current as-built/as-performed state and any alternative future state as-designed/as-planned. Simulations are essential for predicting possible outcomes, which informs managers' decision-making, allowing them to select some optimal future design/plan for delivery to the construction team for execution from any given time forward.
- Store the building's product and process information well beyond the construction phase of any given building so that it can support **learning from experience**. Collections of 'historical digital building twins' provide the information for automated learning of various kinds, enabling continuous improvement of design and construction practices on a wide scale.

As shown, the overall purpose of the video surveillance and implementation of other hardware/sensors implemented on the BIM2TWIN building pilot sites doesn't require any personal data from the on-site personnel. Due to this, any data exploited from the BIM2TWIN building pilot sites in which faces of the on-site participants might appear will be overwritten by the local PC through a video anonymization method coded by the BIM2TWIN partner TUM. This video anonymization method will identified any image or video in which a person's face might me recognized and blurred before they are sent to the FTP server and made accessible to the BIM2TWIN partners.

As mentioned before, personal data from the on-site personnel are not required to be exploited by the BIM2TWIN partners; the relevant data to be exploited as stated in WP2 - Digital Building Twin Platform from the hardware/sensors installed on the BIM2TWIN pilots are:

- As-designed building information models and execution-related data (equipment, labor, schedule, performance, etc.) to encompass design information.
- Real-time data to mirror the construction processes on-site.
- Operational data.

The usages for this data to be exploited from the different pilots in the BIM2TWIN are defined as follows in the different WP's:

- WP3 – Progress Monitoring & Quality Control for Volumetric Building will develop procedures and software for automating:

  - The detection of meaningful point clusters and assignment of the most likely object labels to them probabilistically.
  - The detection of expected-but-missing objects and updating the related activities' progress status.
  - Object spatial measurement properties (length, width, flatness, etc.) on their corresponding point clusters and their comparison against their corresponding as-designed values and specification tolerance limits.
- WP4 - Progress and quality monitoring of surface/textural work will develop procedures and software for monitoring and evaluating:
  - conformance of as-built product to as-designed product.
  - Conformance of as-performed process to as-planned process, specifically focusing on building elements and products applied on surfaces, having texture.
- WP5 - Digital Twins for Occupational Safety and Health (OHS) of Workers will use the generated Digital Twins fed by all the raw data extracted from the hardware/sensors installed on the job site for:
  - Smart computational rule-checking algorithms for safe workspace planning.
  - Automated remote sensing and artificial intelligence for proactive risk detection and prevention.
  - Advanced data reporting and visualization techniques for enhanced hazard awareness.
- WP6 - Equipment optimization will develop an efficient equipment method to optimize the usage of equipment on the job site for:
  - Optimal and quality-assured construction.
  - Short- and medium-term operational planning and control of the equipment.
- WP7 - Production Planning will develop procedures and a software prototype for:
  - Optimization of construction planning subject to lean principles.
  - Transform production management from reactive to proactive by providing a user-friendly tool for people on-site (site managers, crew leaders, construction engineers) to evaluate, in real-time, the possible outcomes of design/plan decisions they consider.

As it is clearly stated in full detail in the above text, the BIM2TWIN overall usage of data purpose is to provide a Digital Building Twin platform that compiles all the information extracted in "real-time" to:

- Enhance progress monitoring and quality control.
- Enhance safety.
- Optimize work planning and use of equipment.

When writing this document, the video recording sensors to be utilized are not fully defined. An initial preselection of the hardware/sensors to be used on the BIM2TWIN project is provided in D1.5 - Data Capture Hardware Review and Selection specifying the usage of all the hardware/sensors, and this list of hardware/sensors will be fully defined in WP8 – Task 8.2 Install Monitoring Equipment, providing the full selection of the equipment to be used and its purpose. These purposes and the equipment to be used on the job site will be explained to the on-field personnel in detail as the GDPR stipulates on their norms through the consent form.

Also, in this consent form, the BIM2TWIN partners will describe how the data collected through the cameras will be handled, how it will be processed, stored, and discarded, and the responsible data controllers and processor partners in the BIM2TWIN project.

The template that will be used for the consent for of the BIM2TWIN project can be found in the annex-1 of this document.

4 CYBERSECURITY

The growth of digitization and digitalization processes in industry and the proliferation of shared data environments in different human activities can consider additional data privacy and ethical use of information issues. Nowadays, digital algorithms using artificial intelligence pre-process enormous amounts of data before getting to the researchers, end-users, or other stakeholders. While this may make large data sets more amenable to human analysis and understanding, it raises the possibility that there will be a time when "sentient" processors might distort data for various reasons. Similarly, in the age of IoT, traffic coming from smart devices is projected to increase by a factor of 30 in the next 20 years, which means most communication will be between machines. Humanity is now in a crucial transition moment of "digitizing everything." Within the AECO sector, this means a paradigm change that must face data management processes to guarantee a transparent use of information in a wide range of services. This chapter discusses how the BIM2TWIN project can meet this paradigm change.

This chapter deepens how security and privacy are considered in the BIM2TWIN project, a highly relevant topic on a European scale to GDPR. The work aims to guarantee that only users granted have access to the content and data in the BIM2TWIN project. The presented not approach in this deliverable is holistic, explaining the importance of data and communication security and ensuring confidentiality by user privacy control.

The BIM2TWIN project is developing a Digital Building Twin (DBT) platform enabling the interaction of various applications, establishing building collection assessment services for both building projects lifecycles, newbuilt or maintenance through their life cycle from the construction stage. By enabling the collaboration of a wide variety of actors from the AECO (Architecture, Engineering, Construction, and Operations) sector to collaborate in diverse forms like management, data acquisition, cross-domain analysis, and complex AI-based events processing. Simply put, BIM2TWIN will act as a binder for many services in the ecosystem, having core functionalities arranged through an API. Furthermore, this approach will enable a sign-on to provide access to assets static data with management configuration in the Building Information Model (BIM) and dynamic contents from different services related to the simulations and monitoring's by taking advantage of the shared information.

Account privacy and security features will be critical for integrating this diverse number of applications and data sharing to ensure a trustworthy interaction and safe information sharing. For perspective usability, developers aim to provide login services, enabling the use of same-user credentials for multiple services; this single-sign-on feature in the authentication service end-users greatly value it.

The BIM2TWIN ecosystem approach, as an applications federation, will bring new challenges and technical issues, requiring an effective security architecture. The proposed cybersecurity architecture connects entities across applications, enabling advanced threat prevention, detection, and mitigation. Besides federated identity assurance, the BIM2TWIN holistic architecture needs to address conventional cloud-based security and privacy controls, authentication and non-repudiation, risk management, and privacy and security policy management.

Significant features from the BIM2TWIN platform cybersecurity architecture revolve around data security and security communication, as shown in Figure 1.

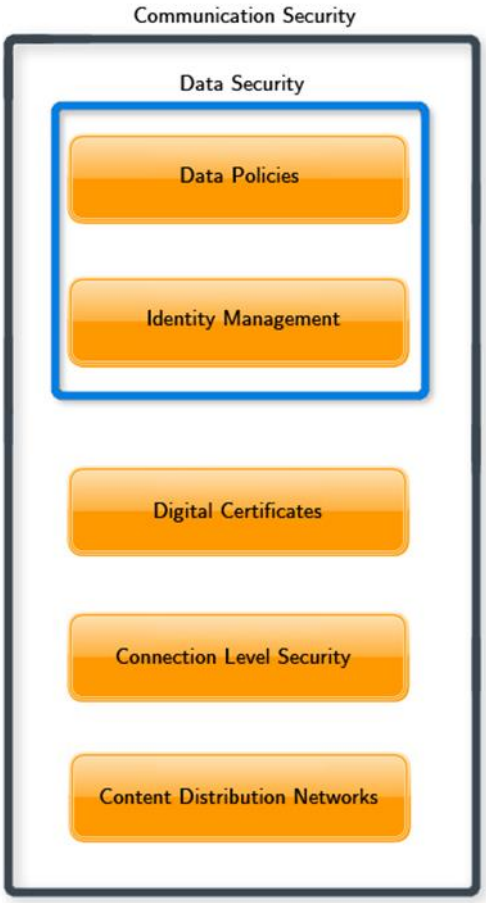

Figure 1. BIM2TWIN cybersecurity architecture

BIM2TWIN cybersecurity architecture:

- The main goal of Data Security is to protect data from unwelcome access, unauthorized modification, and insurance that confidential data is being shared.
- The main goal of Communication Security is the security (authentication, authorization, and accounting, AAA) of data transfers between contributors of the BIM2TWIN project from third-party access.

4.1 High-level architecture for cybersecurity

The BIM2TWIN high-level security architecture is illustrated in figure 2: BIM2TWIN high-level security architecture. The interplay was shown in Figure 2 by critical components from the BIM2TWIN services (partner applications), external services, BIM2TWIN API, and BIM2TWIN core services, including geometry, asset, data, and sensor data management; moreover, users management is handled through an authentication service.

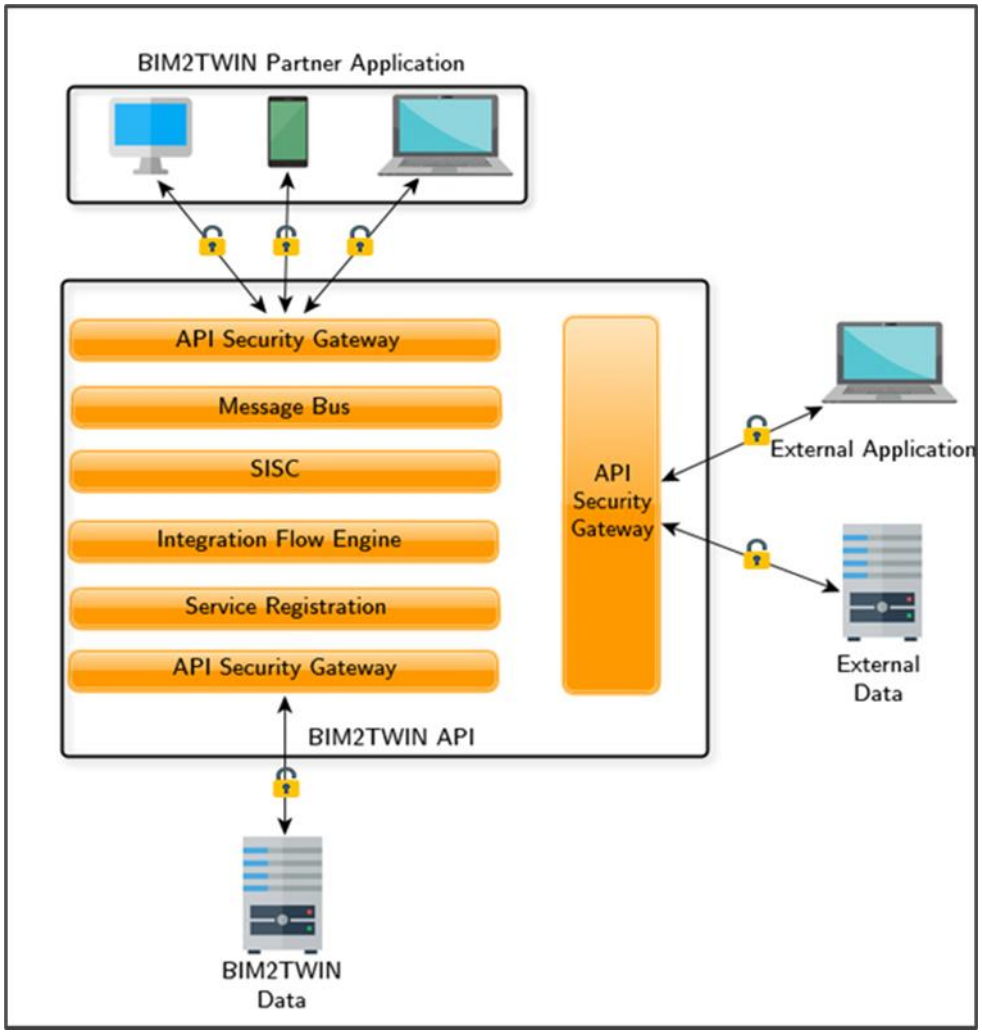

Figure 2. BIM2TWIN high-level security architecture

BIM2TWIN high-level security architecture components are described thoroughly in the following list:

- **Integration Flow Engine** is a component from the BIM2TWIN API that provides a platform for system integrators to create integrative flows for the interconnection of different APIs and services.
- **Service Registry** allows the registration of services by their providers in the BIM2TWIN API. It provides an easier way for the service consumers or system integrators to discover the different services offered on the BIM2TWIN API and allow them to retrieve the metadata information required for the creation of flow integrations.
- **Message Bus** is used to mediate messaging or data transfers between the asynchronous services communicated through the BIM2TWIN API.
- **BIM2TWIN integrity and security component SISC** is a BIM2TWIN component responsible for providing a single sign-on (SSO) capability across the BIM2TWIN ecosystem (see API Security Gateway). Additionally, the SISC component enables data integrity, security analytics, trust and reputation mechanisms, policies definitions, and governance enforcement.
- **API Security Gateway** is a component of the BIM2TWIN API and sub-functionality of SISC, acting as a policy enforcement point (PEP) for the BIM2TWIN API and platforms communicating through it. Furthermore, it intercepts all traffic on the BIM2TWIN API and implements security services for authentication and authorization decisions.

- **Federal Identity Assurance** enables federated identity management on the BIM2TWIN API, access controls, and authentication and authorization management. Also, one of the major requirements of the BIM2TWIN platform is to establish a digital application federation and enable interoperations between applications joining the federation.

Authentication and authorization features on the following activity diagram clarify the level of integration in the BIM2TWIN application. For data accessed through multiple applications in the ecosystem, with a single set credential, several management controls must be in place based on attributes and/or contextual information. For example, policy management, event management, authentication, top-level command execution for password management, and user's password configuration.

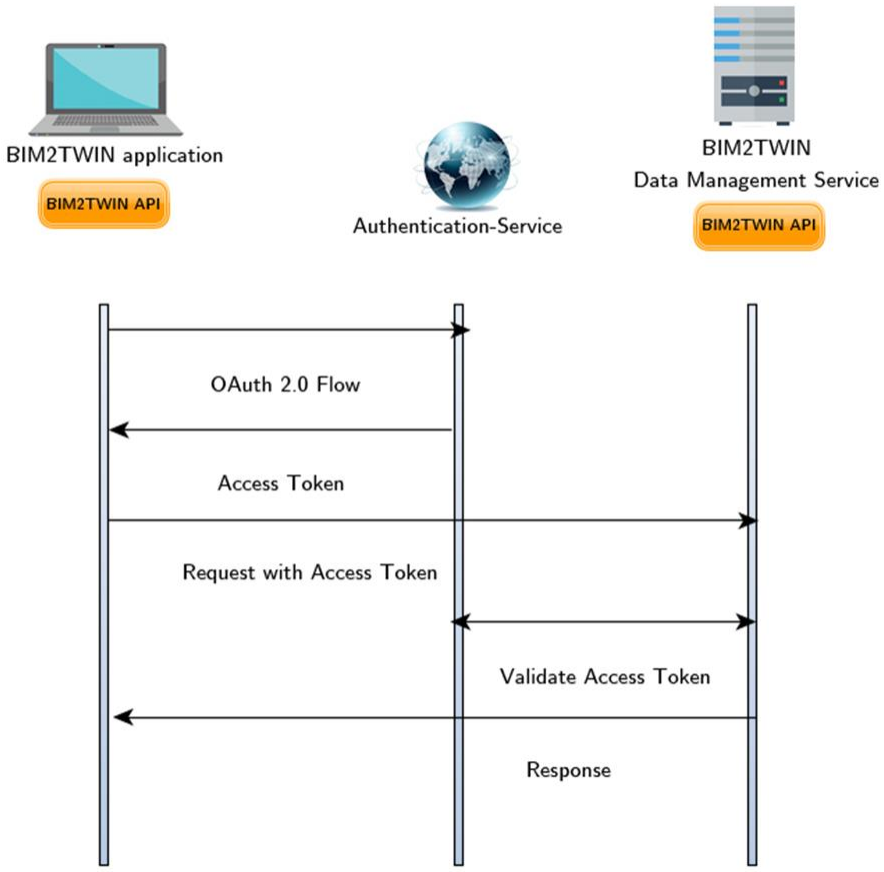

Figure 3. Authentication and authorization feature

In the BIM2TWIN federation, all data is consolidated in the Data Management Service; every application wanting to access or update data will have to receive an Access Token from the authentication service, to access and change data from the Data Management Service.

4.2 Cybercrimes

The GDPR checklist requires the BIM2TWIN partners to build awareness about data protection and possible cybercrimes attempts that the project may face to further protect the BIM2TWIN data stored in the platform and restrict any unwanted access to the platform. The BIM2TWIN partners had to look at the most common cybercrimes techniques to educate the platform users on identifying these attend to access the BIM2TWIN private data by hackers or unwanted entities.

Cybercrime consists of online criminals accessing electronic communications networks and information systems(European Commission, 2020). Social engineering it's the most common technique used to access private online information or gain access to private locations. In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems(CISA, 2020). These social engineering attacks are built around people's actions and thoughts; moreover, these types of attacks are helpful for user behavior manipulation. One example of social engineering attacks is email phishing; spam emails are masked to look like authentic emails from trusted websites by clicking on the containing links. Additionally, you will be asked to log in with your user and password or secret information that hackers will use to reset your password or gain account access.

Hackers exploit the speedy technology progress and the lack of understanding of their users, making users unaware of specific threats to their sensitive information. Likewise, users are unaware of their data value, like a phone number or email address.

Social engineering is more than simple hacking, a psychological technique around people's stimulus and motivations, making humans prone to perpetrators' manipulations to incite specific actions and responses.

- **Emotional Manipulation:** Users are prone to make irrational or risky decisions in the heat of the moment, and attackers try to provoke these responses by implanting fear, anger, or excitement on their victims to get the upper hand.
- **Reciprocity:** People feel obliged to return the favor to those who once helped them.
- **Shortage:** Nothing motivates us more than exclusivity.
- **Authority:** Authority radiating people find their demands and needs usually fulfilled.
- **Urgency:** People may urge to compromise themselves under serious problems requiring immediate attention.

4.3 Cybercrime techniques

Social engineering techniques can take many forms, and the most used are described in the following list:

- **Baiting:** Involves luring the victim into performing a specific task by providing easy access to something the victim wants(European Union Agency for Cybersecurity, 2021b). This technique uses false promises to pique the victim's greed or curiosity to lure them into a trap that steals their personal information or inflicts their system with malware.
  The most used form of baiting uses physical media to disperse malware. For example, attackers leave a bait, typically a malware-infected flash drive, in a conspicuous area where potential victims are prone to see them (e.g., bathrooms, elevators, parking lot of targeted company). The bait has an authentic look, such a label presenting it as from one of the companies on the payroll list.
  The curious victim picks up the bait and inserts it into their work or home computer, resulting in an automatic malware installation on the system, moreover, giving them access to sensitive documents or information from the company's victim's server or their own personal and financial information from their home system.
  Baiting Scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead victims to malicious sites or encourage them to download malware-infected applications.
- **Scareware:** Contraction of "Malicious software." A program injected in a computer system, generally surreptitiously, intending to compromise privacy, integrity, or the availability of data, of the applications or the operative systems of the target(Presidency of the Council of Ministers, 2013). This technique happens when victims are bombarded with false alarms and fictitious threats, making users think that their system has been affected by malware,

persuading them to install unnecessary software for the user (but necessary for the perpetrator), or installing malware itself without the user knowledge. Scareware is also referred to as deception software, rogue scanner software, and fraud.

A typical scareware example is the legitimate-looking pop-up banners appearing in your browser while surfing the web, displaying a text saying something like "Your computer may be infected with harmful spyware programs." Furthermore, it will either offer you to install a tool for you (often malware-infected), or it will redirect you to a malicious site where your system will become infected.

Scareware can also be distributed via a spam email that will dole out numerous bogus warnings or offer users to buy worthless/harmful services.

- **Pretexting:** This technique uses a pretext - a false justification for a specific course of action - to gain trust and trick the victim(European Union Agency for Cybersecurity, 2021b). This scam will often be initiated by the perpetrator pretending to need sensitive information from the victim to perform a critical task. With this technique, the attacker will learn sensible details through a series of cleverly crafted lies.

  The attacker will initially establish a trust link with the victim by impersonating a co-worker, police, bank or tax officials, or another person who will have the right and proper authority to know the requested sensitive information. Furthermore, the perpetrator will ask a series of questions to confirm the victim's identity while gathering the victim's personal information.

  By using these scams, all sorts of information and records are gathered, such as tax ID numbers, personal addresses, phone numbers, phone records, staff vacation dates, bank records, and even security information related to a physical plant.
- **Tailgating:** Tailgating is the act of following an authorized person into a restricted area or system(European Union Agency for Cybersecurity, 2021b). Also known as "piggybacking," these types of attacks happen when somebody without proper authentication follows and authenticates an employee into a restricted area. The attacker might impersonate a delivery driver and wait outside a building to get things started. When an employee gains security's approval and opens the door, the attacker asks the employee to hold the door, thereby gaining access to the building.

  Tailgating does not work in all corporate settings, such as large companies whose entrances require the use of a keycard. However, in mid-size enterprises, attackers can strike up conversations with employees and use this show of familiarity to get past the front desk.

  Colin Greenless, a security consultant at Siemens Enterprise Communications, used these tactics to access multiple floors and the data room at an FTSE-listed financial firm. He could even set up shop in a third-floor meeting room and work there for several days.
- **Phishing:** Phishing attacks are a means to persuade potential victims into divulging sensitive information such as credentials or bank and credit card details(European Union Agency for Cybersecurity, 2021a). This attack is the most popular among social engineering attack types, phishing scams can be seen in the form of emails and text messages campaign aimed to create a false sense of urgency, curiosity, or fear on the victims, making them prone to reveal sensitive information, clicking on links to malicious websites, or opening attachments containing malware.

  For example, an email is sent to an online service user, alerting them of a policy violation requiring immediate action, such as a password change. Additionally, it includes a link to an illegitimate website, looking just like the official website, prompting the unaware user to login with his credentials; moreover, after the victim has completed the malicious form, this form is automatically sent to the perpetrator.

  Given that similar or near-identical messages are sent to all users, detecting and blocking them is much simpler than email servers having access to threat-sharing platforms.

4.4 Famous cyber attacks

To get a good sense of the social engineering tactics and dangers, we should take a step back and look at attackers' past techniques to understand how these social engineering techniques work and how they could affect the BIM2TWIN project.

Nigerian 419: Nigerian letter frauds combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter mailed, or e-mailed, from Nigeria offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author—a self-proclaimed government official—is trying to transfer illegally out of Nigeria. The scheme relies on convincing a willing victim, who has demonstrated a "propensity for larceny" by responding to the invitation, to send money to the author of the letter in Nigeria in several installments of increasing amounts for various reasons. The recipient is encouraged to send information to the author, such as blank letterhead stationery, bank name, and account numbers, and other identifying information using a fax number given in the letter or return the e-mail address provided in the message.

Payment of taxes, bribes to government officials, and legal fees are often described in detail with the promise that all expenses will be reimbursed as soon as the funds are spirited out of Nigeria. In actuality, the millions of dollars do not exist, and the victim eventually ends up with nothing but loss. Once the victim stops sending money, the perpetrators have been known to use the personal information and checks that they received to impersonate the victim, draining bank accounts and credit card balances. While such an invitation impresses most law-abiding citizens as a laughable hoax, millions of dollars in losses are caused by these schemes annually. Some victims have been lured to Nigeria, where they have been imprisoned against their will and lost large sums of money. The Nigerian government is not sympathetic to victims of these schemes since the victim conspires to remove funds from Nigeria in a manner contrary to Nigerian law. The schemes themselves violate section 419 of the Nigerian criminal code, hence the label "419 fraud".

Fake employee: Impersonation is one of several social engineering tools used to gain access to a system or network to commit fraud, industrial espionage, or identity theft. Impersonation differs from other forms of social engineering because it occurs in person rather than over the phone or through email.

The social engineer "impersonates" or plays the role of someone you are likely to trust or obey convincingly enough to fool you into allowing access to your office, to information, or your information systems. This type of social engineering influences our natural tendencies to believe that people are who they say they are and to follow instructions when asked by an authority figure. It involves the conscious manipulation to obtain information without the individual realizing that a security breach is occurring.

Impersonation requires a lot of preparation, so it occurs less often than other forms of social engineering. Social engineers prefer the more anonymous phone or email approach over appearing in person. Done well; however, nobody ever knows that the impersonator was ever there. The people they spoke to were just another individual in a non-stop stream, although perhaps just a bit nicer than the run-of-the-mill grump.

Act like you're in charge: Most people are primed to respect authority, or as it turns out, to respect people who act like they have the power to do what they are doing. By knowing these, attackers can exploit varying degrees of knowledge of a company's internal processes to convince people that they have the right to be in places and see things that they shouldn't, or that any communication from them is coming from somebody the victim respects. For instance, in 2015, finance employees at Ubiquiti Networks wired millions of dollars in company

money to scam artists who were impersonating company executives, probably using a lookalike URL in their address. On the lower-tech side, investigators working for British tabloids in the late '00s and early '10s often found ways to get access to victims' voicemails accounts by pretending to be other employees of the phone company via sheer bluffing; for instance, one PI convinced Vodafone to reset the actress Sienna Miller's voicemail PIN by calling ad claiming to be "John from credit control."

Sometimes it's external authorities whose demands we comply without giving it so much thought. For example, Hillary Clinton, former white house chief of staff John Podesta, had his email hacked by Russian spies in 2016 when they sent him a phishing disguised email from google asking him to reset his password. Furthermore, he gave his login credentials away by doing what he thought he had to do to secure his account.

4.5 Cyber security prevention

As seen in the previous famous cybercrimes, social engineers thrive on human feelings manipulation, such as curiosity and fear, to carry out schemes by drawing their victims into traps. Therefore, people should be worried whenever they feel alarmed, either by an alarming email, any offer displayed on a website, or whenever they encounter a stray of digital media lying around. Because by being alert to scams, people will be able to protect themselves or at least be less prone to be victims of a social engineering cyberattack.

Here are some general approaches to minimize or make people less vulnerable to social engineering attacks:

- **Safe Communication:** Online communication is where people are the most vulnerable because social media accounts, emails, and text messages are the most common targets of cyber social engineers, but also considering in-person interactions as well.
- **Slow down:** Spammers want their victims to act first and think later. If the message in question conveys a sense of urgency or uses a high-pressure sales tactic, be skeptical; users should never let their urgency influence their careful review.
- **Never Click on Links in Emails or Messages:** First, we would want to cross-check the authenticity of the sender user and the URL by manually inserting the URL in our address bar. However, taking the extra step of investigating an official version of the URL in question will give us a different pace of mind. Never engage with any URL without previously verifying it as authentic or legitimate.
- **Use Multi-Factor Authentication:** Online accounts are safer when more than just a password is used to protect them. Multi-factor authentication add-up an extra layer of security that verifies the user identity after they log in with their password. These "factors" could include a temporary passcode sent to the user's mobile to biometrics, like fingerprints or facial recognition.
- **Use Strong Passwords:** Each user's passwords should be unique and complex; they should aim to use diverse character types, including uppercase, numbers, and symbols. Additionally, users should opt for longer passwords when possible.
- **Avoid Sharing Names of your Schools, Pets, Places of Birth, or Other Personal Details:** By doing so, users could be unknowingly exposing answers to their security questions or parts of their secret password. Also, if users consider using memorable questions but inaccurate ones, it will make it harder for attackers to crack their accounts. For example, if the user's first car was a "Toyota," but instead of writing Toyota, the user opts for using a lie like "Clown Car," the user will completely throw off any prying hacker.
- **Beware of any Downloads:** If users don't personally know the sender or are expecting a file from them, downloading anything will be a mistake.

- **Be Very Cautious of Building Online-Only Friendships:** While the internet is a great place to connect with people worldwide, this is also a common method for social engineer attacks. Be alerted to tells and red flags that indicate manipulation or clear abuse of trust.
- **Foreign Offers are Fake:** receiving an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the funds are guaranteed to be scams.
- **Safe Network Use:** Compromised online networks could be another vulnerability point that social engineers' hackers could exploit for background research. To avoid using your data against you, taking protective measures for any connected network is heavily suggested.
- **Use a VPN:** If someone on the user's main network, wired, wireless, or even cellular, finds a way to intercept traffic, a Virtual Private Network (VPN) can keep them out. VPNs give their users privacy, an encrypted "tunnel" on any internet connection they use. Additionally, their connection is guarded against unwanted eyes, but their data is anonymized, so it cannot be traced back to them via cookies or other means.
- **Keep all Networks-Connected Devices and Services Secure:** Many people know internet security practices for mobile and traditional computing devices. However, securing a network itself and all their smart devices and cloud services is just as important. Users should be sure to protect commonly overlooked devices like car infotainment systems and home network routers because data breaches on these devices could fuel personalization for a social engineering scam.
- **Never let Strangers Connect to your Primary Wi-Fi Network:** At home or in their workplace, access to a guess Wi-Fi connection should be made available. Doing so allows the user's primary encrypted, password-secured connection to remain secure and interception-free. Because if someone decides to "eavesdrop" for information, they won't be able to access the user's activity and others using this network safe.
- **Set Spam filters to High:** All email programs have a spam filter. To find it, users should look at their settings options and set their spam filters to high to avoid any suspicious email or any fake tenting offer reaching their eyes.
- **Delete any Request for Financial Information or Password:** If users are asked to reply to a message or email with a personal email, this is more likely to be a scam.
- **Secure Your Computing Devices:** Users should install anti-virus software, firewalls, email filters and keep these up to date. Additionally, users should set their operating systems to update automatically, and if their smartphone doesn't update automatically, they should manually update it whenever they receive a notice. Furthermore, using an anti-phishing tool offered by their web browser or third party will alert them of possible risks.
- **Safe Device Use:** Users keeping their devices to themselves is just as important as all the previously discussed methods.
- **Internet Security Software:** If social engineering tactics succeed to breach the user's carefulness, malware infections are an expected outcome. For combating rootkits, trojans, and other bots, it is critical to employ a high-quality Internet security solution that can eliminate infections and help track down their source.
- **Secure devices in public:** Users should always keep their computers and mobile devices locked, especially at work. Whenever users use their devices in public spaces like airports or coffee shops, they should always have them under their possession.
- **Update Software:** Immediate updates give essential security fixes; whenever users skip or delay updates of their operating systems or apps, they leave known security loopholes exposed for hackers to target. Additionally, since hackers know this is a common behaviour of many computer and mobile users, these users become highly potential targets for socially engineered malware attacks.

4.6 Security audits

Besides only educating the responsible parties of accessing personal data or any other party that may be vulnerable to grant access to the BIM2TWIN stored data there are security a high-level description of the many ways an organization can test and assess its overall security posture, including cybersecurity. Through these security audits the BIM2TWIN project can test the overall security of the platform when need

Companies might employ more than one type of security audit to achieve their desired results and meet their business objectives. Regular audits can catch new vulnerabilities and unintended consequences of organizational change.

Following are some specific benefits of running security audits:

- Verify that the current in-place security strategy is the most efficient.
- Check if the new security pieces of training are improving the system security from one audit to the next.
- It reduces cost by shutting down or repurposing extraneous hardware and software that might be uncovered during the audits.
- Uncover vulnerabilities introduced into the organization by new technologies or processes.
- Prove that the organization is compliant with regulations like HIPAA, SHILED, CCPA, GDPR, etc.

The different use cases for a security audit are:

- One-time assessments are security audits performed for ad-hoc or particular circumstances and triggers in the company's operations. For example, suppose the company will introduce a new software platform. In that case, they have a battery of tests and audits that they have to run to discover any potential unknown risks that they might be introducing into their shop.
- Tollgate assessments are security audits with a binary outcome. It's a go or no-go audit to determine if a new process or procedure can be introduced into the company's environment. Companies aren't determining risk as much as looking for showstoppers to prevent them from moving forward.
- Portfolio assessment security audits are annual, bi-annual, or regularly scheduled audits. These audits are used to verify that the company's security processes and procedures are being followed and adequate for the current business climate and needs.

Security audit executions are usually separated into 4 different stages.

Defining the scope of the audit: The first task on the checklist is to establish the scope of the audit. Whether the company wants to check their general state of security or do a specific network security audit, third-party security audit, or any other, the company or person responsible for performing the audit needs to know what to look for and what to skip during the audit.

The company will need to draw a security perimeter, a boundary around all their valuable assets for this to happen. This boundary should be as small as possible and include every valuable asset that the company has and requires protection. The person responsible for the audit will need to audit everything inside this boundary and not touch anything outside the already established perimeter.

The best way to define a security perimeter is by creating a list of all valuables assets that the company has; this can be reasonably tricky because companies often omit things like purely internal documentation detailing. For example, various corporate policies and procedures appear to have no value for the potential perpetrator. However, such information is valuable for the company itself because if those documents are ever lost or destroyed (e.g., because of some hardware failure or employee mistake), it will take time and money to recover or recreate them. Therefore, they should also be included in the master list of all assets requiring protection.

Defining data threats: Once a security perimeter is specified, the company should create a list of potential threats that their data could face. For example, if a natural disaster, such as a hurricane, is relatively rare, but if it happens, it could be devastating in financial terms; because of this, it will be included in the list. Striking the right balance between how likely threats are and how much impact they have is the hardest part of the audit.

All the most common threats that should be considered are the following:

- **Natural disasters and physical breaches:** As mentioned, while this is something that rarely happens, the consequences of such a threat could be devastating; therefore, it's something that the company should have control of just in case.
- **Malware and Hacking Attacks:** External hacking attacks are one of the biggest threats to data security out there and should always be considered.
- **Ransomware:** This malware type gained popularity in recent years. If the company being audited is working in healthcare, education, or finances, they should probably watch out for this type of attack.
- **Denial of Service Attacks:** The rise of IoT devices saw a dramatic increase in botnets. Denial of service attacks is now more widespread and more dangerous than ever. If the company or software depends on uninterrupted network service, they should include these.
- **Malicious Insider:** This threat most of the companies don't take into consideration, but many faces. Both the company's employees and third-party vendors with access to its data can easily leak or misuse it, and the company won't detect it. Therefore, it's best to be ready and include it on the threat list.
- **Inadvertent Insider:** Not all insider attacks are made out of malicious intent. The employee is making an honest mistake and accidentally leaking the company's data, which is very common in this connected world. Furthermore, this should be a threat to be considered.
- **Phishing and Social Engineering:** More often than not, a kicker will try to get access to the company's network by targeting their employees with social engineering techniques, practically making them give up their credentials voluntarily; moreover, this is something definitely to be taken into consideration.

Risk calculation: Once the company has established a potential list of threats that their data may face, the person responsible for the audit needs to assess each potential threat's risk. Such risk assessment will help the audit responsible person put a price tag on each threat and prioritize when it comes to implementing new security controls. To do so, the person responsible for the audit should look at the following things:

- **Company Past experiences:** Whenever the company has encountered a specific threat may impact the probability of them encountering it in the future. If the company was a target of hacking or denial of service attack, it is good to happen again.
- **General Cyber Security Landscape:** Looking at the current trends in cyber security. What threats are becoming increasingly popular and frequent? What are new and emerging threats? What security solutions are becoming more popular?
- **State of the Industry:** Looking at the experience or the company's direct competition and common threats that the industry faces. For example, if the company works in healthcare or education, face insider attacks will be more frequent, phishing attacks and ransomware. In contrast, retail may face denial of service attacks and other malware more frequently.

Devising the Necessary Controls: Once the potential risks associated with each threat are established, there is one last stop, creating an IT security checklist of controls that need to be implemented. Examine controls in place and devise a way to improve them or enforce the missing processes.

The most common security measures to be considered are:

- **Physical Server Security:** if the company owns its servers, it should secure physical access. Of course, this is not a problem if they rent server space from a data center. At the same time, any IoT devices in the company should have all their default passwords changed, and physical access to them thoroughly secured to prevent any hacking attempts.
- **Regular Data Backup:** Data backup is very effective in the case of natural disasters or malware attacks that corrupt or lock the company from its data (ransomware). Ensure all backups are made as frequently as possible and establish a proper procedure for resting their data.
- **Firewall and Anti-virus:** This is cybersecurity 101, but companies need to protect their networks with correctly configurated firewalls and computer anti-viruses.
- **Anti-Spam Filter:** Correctly configurated anti-spam filters can be a great boon in fighting phishing attacks and malware sent via email.
- **Access control:** There are several ways to control access, and the company would be better off putting all of them in place. First of all, they will need to ensure that they control the level of privilege users have and use the principle of least privilege when creating new accounts. Apart from that, two-factor authentication is a must. It dramatically increases the security of the login procedure and allows the company to know who accessed their data and when.
- **User Action Monitoring:** Software makes a video recording of everything the user does during the session, allowing the company to review every incident in its proper context; this is very effective when it comes to detecting insider threats, but its also an excellent tool for investigating any breaches and leaks, as well as a great answer to a question of how to do IT security compliance audit, as it allows the company to produce the necessary data for such an audit.
- **Employee Security Awareness:** To protect employees from phishing and social engineering attacks, reduce the frequency of unintentional mistakes, and ensure that all security procedures are followed. It is best to educate them on the best cyber security procedures security. The company should invest in teaching their employees about threats that both they and the company face and the company's measures to combat those threats. Raising employee awareness is a great way to transform them from liability to a helpful asset in cyber security.

4.7 Penetration testing

Penetration testing (pen-testing or pen-testing) is a method of testing, measuring, and enhancing established security measures on information systems and support areas. Social engineering penetration testing focuses on people and processes and the vulnerabilities associated with them. These pen tests typically consist of an ethical hacker conducting different social engineering attacks such as phishing, USB drops, or impersonation that a person could face during their work. This test aims to identify weaknesses in a person, group of people, or process and identify vulnerabilities with a clear path to remediation.

Users are commonly referred to as the “weakest link” regarding security, yet users still have more than the necessary permissions to perform their jobs.

So, it would only make sense to pen tests those users. These pen tests can show who is susceptible to the attacks previously discussed and more.

Social engineering pen tests are typically done in a hybrid fashion combining on-site and off-site tests.

On-Site Test

On-site tests are used to test the physical security and policies in place, like a clean workstation policy.

The typical methods of attack you would use for an on-site test are:

- Impersonation
- Dumpster Diving
- USB drops
- Tailgating

Off-Site Test

Off-site tests test users' security awareness during a typical day. During this type of test, the pen tester will research the company and use publicly available information to test the company.

These tests are conducted remotely and commonly consist of the following attacks:

- Vishing
- Phishing
- Smishing

Methods Used to Perform Social Engineering Attacks

Three main methods are used to perform a social engineering attack, including information gathering, victim selection, and engagement with victims.

- **Information Gathering.** Before testing a target, the person responsible for testing needs to become familiar with them. To do this, they will need to collect as all publicly available information about the target as possible. They can gain information about a target in numerous ways, but the most common social engineering methods are active and passive reconnaissance and open-source intelligence (OSINT). It doesn't make sense to test a target with medical phishing attacks when it is a financial company.
- **Active Reconnaissance** is an attempt to gain information about a target while engaging with the target. It could be by calling the target and impersonating someone else to gain knowledge or could be more subtle by conducting port scans.
- **Passive Reconnaissance** is a great way to quickly gain general information about the target searching for a threat vector. When an attacker is conducting passive reconnaissance, they often turn to popular social media sites like Facebook or LinkedIn. For example, an attacker could use the information of a planned vacation posted on Facebook to know when their victim will be out of town. Once gone, they could search their home for ways to access the company's network. Next to being free, one of the main advantages of passive reconnaissance is that the attacker does not have to interact with the target to collect information, thereby reducing the risk of being detected.

Open-Source Intelligence (OSINT) refers to the type of data that has been collected from publicly available sources and is deemed "open." Thinking back to Passive reconnaissance, passive is the method in which the data was collected, and OSINT would be the type of data collected.

Victim Selection

To perform a successful test, you must select your "victims" carefully. You will want to choose victims, or groups of victims, that are easily tricked.

These typically consist of:

- Employees who are less aware
- Mistreated employees
- Recently fired employees

Glassdoor is an excellent source for this type of information. Since Glassdoor allows current and former employees to review the company and comment about their experience, pay, and benefits.

From these reviews, attackers can quickly identify people who may be less aware and more willing to share information about the company.

Companies would be surprised how money can influence an employee's loyalty, especially if they feel underpaid or undervalued.

Engagement with Victims

This step is where the attacker will begin engaging with his victims. Once he has identified his victims, he will start planning out the methods of attack that will work best against each person or group of people. He may need to do more targeted active and passive reconnaissance to plan accordingly. Again, the goal is to collect as much data about people without triggering any alarms. He does not want to tip his victim hat and reveal to the person that an attack or test might be looming.

Steps to Performing a Social Engineering Penetration Test

There are four main steps to performing a social engineering penetration test: test planning and scoping, attack vector identification, penetration attempts, and reporting.

Step 1: Test Planning and Scoping

This step is the most crucial step during the penetration test. During this step, companies will identify what is in scope and how the test will be performed. It typically requires a meeting between management and the personnel performing the test. To keep in mind, the company will want to keep the number of people involved in this meeting to a minimum to prevent several people from knowing about the test.

The company will want the test to be as accurate as possible and to do so. They will need to minimize the test awareness. While scoping out the test, the company performing it will want to include all the methods and attacks to be implemented. For example, if a tailgate, impersonate employees, or delivery personnel social engineering attacks, it needs to be addressed in the scope. From the scope, the company should write up a clear contract that all the involved parties agree on; a contract is a key to a successful penetration test.

Step 2: Attack Vector Identification

After scoping out and the pen test is completed. This step of the pen test will involve the tester identifying all the methods they will use during the test. A transparent contract is defined for what and who is included in the test.

These methods should also be linked to specific users and groups. For example:

- **Security guards will be tested using impersonation tests.** This test will include impersonating an Amazon delivery person making a delivery to an employee in IT.
- **Security guards will be tested using a tailgating test.** This test will involve the tester closely monitoring employees as they enter the building and enter the building, or secure area, while a high volume of people is entering.
- **Personnel in accounting will be tested using a phishing test.** This test will involve sending an accountant a phishing email that spoofs the Chief Executive Officer and request last month's expense report for review.
- **An employee in IT will be tested using an impersonation test.** This test will involve a member of the pen test requesting a password reset for an employee in the account receivable department.

Listing out the attack vectors like above helps steer the pen test and gives management a clear understanding of the steps taken to test the company. Each test can be scored based on how well the users respond and will help with the overall final score of the penetration test.

Step 3: Penetration Attempts

During this step of the pen test, the tester will take all the listed attack vectors from the previous step and execute those tests.

Documentation is vital in this step as these tests will later become supporting evidence for the report. The type of evidence that should be collected is:

- **Recorded Phone Calls.** These phone calls are essential as there is no other method to document that this attack occurred and show its outcome.
- **Emails from Phishing Attacks.** These emails are important because they can show how far a user has allowed the attack before catching it. In some cases, users don't catch on until after giving up sensitive information.
- **Documentation found while dumpster diving.** This type of documentation should include scans of the documents found and even pictures of where the documents were found if appropriate.

Along with the evidence, the tester should include the start and end time for each test, the name of the person conducting the test, and the employee(s) being tested.

Step 4: Reporting

The reporting step of a pen test is where the tester will bring all the results together by writing a report.

Most of the time, this report is to be read by senior management, and it should make sure to address all the initial concerns discussed at the inception of the test and all the vulnerabilities found during the test.

In the report, the tester should mention the vulnerabilities found and provide recommendations on how to address say vulnerabilities.

A typical pen testing report should consist of:

1. An executive report
2. A walkthrough of technical risks found
3. The potential impact of the vulnerabilities found
4. The remediation options available for each vulnerability found
5. The concluding thoughts of the pen test
6. Vulnerability elimination

4.8 Vulnerability or security scans

Vulnerability scans are performed by automated software designed to assess other software, network operations, or applications. This software will scan potential weaknesses in code or structure which could be exploited in later attacks.

There are two kinds of scans; authenticated and authenticated. Authenticated vulnerability scans allow remote protocols to access the network directly. Such protocols can be a secure shell (SSH) or remote desktop protocol (RDP). The difference is that unauthenticated scans can just check publicly visible information.

The scan results are a vulnerability assessment report containing vulnerabilities classified as a priority. Critical vulnerabilities indicate a high likelihood that an attacker could exploit weaknesses and enact damage. Lower-priority threats may help intruders gather information but do not directly allow breaches. It is essential to consider that the data in such a report is not backed by an attempt to exploit them; some may be false positives. For example, such a report may indicate a service endpoint as vulnerable as it uses HTTP and not HTTPS. This endpoint is only used to relay legacy clients to the new HTTPS and doesn't give access to any other data.

Differences between vulnerability scans and penetration tests:

Vulnerability scans

- It can be performed automatically.
- Scans for potential vulnerabilities in a particular system.
- It should be performed regularly.
- It can be performed relatively quickly in the background.

Penetration test

- Requires various levels of expertise.
- Attempting to exploit vulnerabilities to penetrate a particular system.
- It should be performed after significant changes or introducing new components into the environment.
- Depending on the test strategy and size of the system. It can take days, weeks, or even months to finish.

In contrast to a vulnerability scan, penetration testing involves identifying vulnerabilities in a particular network and attempting to exploit them to penetrate the system. Another critical difference between the two is that vulnerability scanning can be automated, where a penetration test requires various levels of expertise and usually manual work.

5 CYBERSECURITY TECHNOLOGIES IN THE BIM2TWIN PROJECT

This chapter will briefly introduce suitable cyber technologies related to the BIM2TWIN project.

5.1 Cryptography

There are two types of encryptions. Symmetric, where a single key is used for encryption and decryption of information, and Asymmetric, where a public/private keypair exists; moreover, one key can decrypt data encrypted by another user key.

The cryptography method to be chosen should be carefully selected. For example, NIST offers guidelines for Block Ciphers (Barker, 2020), emphasizing the procedures for both applying for cryptographic protection (e.g., Encryption) and removing or verifying this information (e.g., Decryption): Advanced Encryption Standard (AES) and Triple Data Encryption Algorithm (Triple DES).

Quantum Safety is described as the possibility of a great technical leap soon. A computer power leap might mean that the current safety encryption algorithms could be easily cracked whenever quantum computers are created with this use. Furthermore, more complex encryption is advised to prepare for this case scenario.

Hash functions are a standard method for data protection, especially passwords. A hash function takes a group of characters (called a key) and maps it to a value of a certain length (called a hash value or hash). The hash value is representative of the original string of characters but usually is smaller than the original. Hash functions turn data into data stamps which could be repeatable but not invertible, so it is infeasible to infer the original data and small changes in the input data results.

Algorithms should be carefully selected. For example, NIST offers guidelines on hash functions (Barker, 2020). It's important to consider that some commonly used hash functions like MD5 are not secure, as input data can be inferred from the output data.

5.2 Identity verification

Public / Private cryptography creates an exciting opportunity because it's possible to perform mathematical operations for knowledge demonstration of the secret private key value, but without revealing any information about its secret. If the secrets of the private key remain confidential, this ability could be used as a mechanism for authentication verification of remote parties.

Beyond a simple remote entity authentication, this remote entity could also endorse data through a digital signature. The data is specified, and the entity encrypts the hash function of the selected data. Additionally, for data endorsement verification, other parties could calculate their hash functions and decrypt their final hash function output with the first entity public key.

If both values are the same, the integrity of the message could be verified. The digital signature algorithms should be chosen carefully. For example, NIST offers guidelines on digital signatures (Barker et al., 2009).

5.3 User authentication

OAuth and OpenID are vital applications for identity verification within the BIM2TWIN platform, which will handle the authentication delegation to a centralized server, allowing for system distribution (such as BIM2TWIN) to have a consistent identity system. OAuth uses a Keyed-Hash Message Authentication Codes (HMAC) for token signings. If HMAC's are signed with a private key, all the entities on the ecosystem could use the public key to verify the message's authenticity. If an asymmetric key is being used, the OAuth server will have to confirm the message, resulting in additional communication.

NIST provides details for HMAC's (Gutierrez & Turner, 2008). Authentication distribution to a single server allows better control of security practices within the critical infrastructure, where great care could be applied to this essential service on the BIM2TWIN platform.

OAuth and OpenID also offer user group creation, a valuable feature for shared access to components, APIs, GUIs, and data items or database collections. Currently, the BIM2TWIN project uses an open-source identity and access system known as Key cloak to design single-sign-on services (Keycloak, 2022).

5.4 Digital certificates and chain of trust

The authentication ability of a remote entity through a private key knowledge is powerful. Still, without the help of additional support, this ability will be found limited in terms of identity. Furthermore, it could verify that the remote entity has not changed, but the initial identity binding to a private key requires some trust level; moreover, cryptographic certificates and trust chains are used to solve this issue. A digital certificate, a digital statement about identity, expresses the subject entity's identity, specifies their public key, the entity identity confirmation, and later digitally signed by the confirming entity. As such, the confirming entity can vouch for the identity of the subject entity. Additionally, trust is extended to a small group of entities to vouch for the identity of other entities, which later will be trusted to some degree to do the same.

For the chain of trust process to start(WolfSSL, 2020) in Figure 4, the system end-users will trust their software provider to provide a list of verified certificates for Root Certificate Authorities (RCAs). In turn, the RCAs will verify other entities, some of which are assigned intermediate Certificate Authorities (ICA), which will authorize the designated entity to authorize other entities. In addition, to identity verification of a remote entity, this could provide a digital certificate, and upon obtaining all the digital certificates used in the process, a chain of trust can be followed up from the RCAs through and ICAs to the final remote entity, to be sure of the identity of the previous unknown party.

However, a slight risk of private critical leakages over time exists, either through accidents or due to cyber-attack. Furthermore, as this risk accumulates over time, an expiration date on digital certificates is used, and compromised keys could not be used forever.

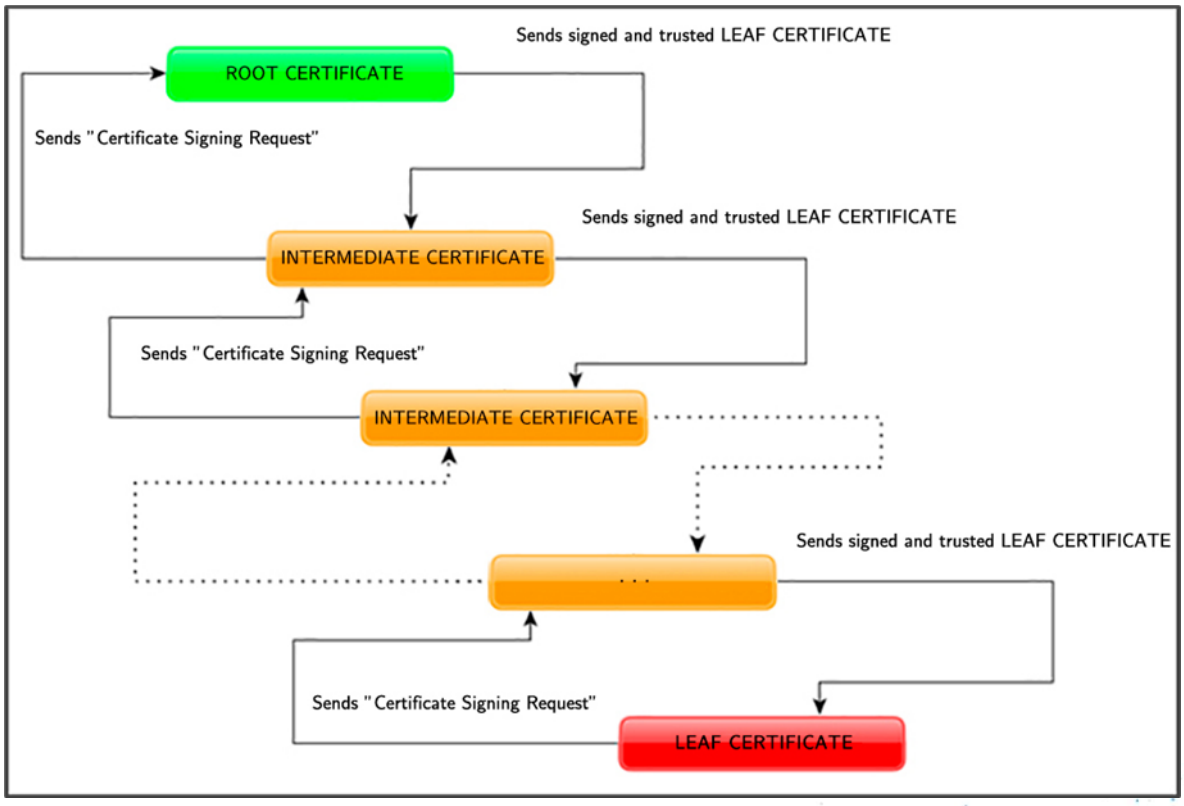

Figure 4. Chain of Trust process

The process for creating a chain of trust works as follows:

1. The **ROOT PRIVATE KEY** is made in a cleanroom on a disconnected computer.
2. With the **ROOT PRIVATE KEY**, the **ROOT CERTIFICATE** is created.
3. Only the **ROOT CERTIFICATE** is transferred to a connected system, from which it be spread to all manufactures browsers.
4. An **INTERMEDIATE PRIVATE KEY** is made similarly to the **ROOT PRIVATE KEY**.
5. With the **INTERMEDIATE PRIVATE KEY**, the **INTERMEDIATE CERTIFICATE** is created.
6. The **ROOT CERTIFICATE** owner will receive a certificate signing request with the **INTERMEDIATE CERTIFICATE**.
7. The **ROOT PRIVATE KEY** signs the **INTERMEDIATE CERTIFICATE**.
8. The previously created **INTERMEDIATE PRIVATE KEY** could create other **INTERMEDIATE CERTIFICATES**.
9. A **LEAF PRIVATE KEY** is created.
10. The **LEAF PRIVATE KEY** makes the **LEAF CERTIFICATE**.
11. The **INTERMEDIATE CERTIFICATE** owner will receive a certificate signing request with the **LEAF CERTIFICATE**.
12. The **INTERMEDIATE PRIVATE KEY** signs the **LEAF CERTIFICATE**.

- Note that during this process, only certificates and certificates signings are transferred, not the private keys.
- The browser internally can check if the LEAF CERTIFICATE is trusted by the following chain of signings.

5.5 Connection levels of security

Connection level security handles data transit. It must assume that data will be sent across the internet (or any wide or local network) in general, and traffic will be visible to hostile actors. It's difficult to hide the connection evidence, and some information about the nature of the information could be inferred by network traffic monitoring. Still, the date within the connection (messages) can be protected.

Hypertext transfer protocol secure (HTTPS)

Hypertext Transfer Protocol Secure (HTTPS) uses its protocol in cooperation with Transport Layer Security (TLS). Transport Layer Security (TLS) is a cryptographic protocol that forms the bulk security Internet communication foundation.

HTTPS provides several significant advantages over plain HTTP because digital certificates are used to authenticate identities of remote parties, and communications are encrypted to ensure the confidentiality and integrity of messages.

HTTPS is commonly used with modern browsers, with trends marking sites without HTTPS specifically as insecure by the browser.

Digital certificates management is imperative to ensure proper uninterrupted service. For the BIM2TWIN platform, this means that further considerations are required to handle certificate management for web servers. One option would be to purchase certificates, valid for a certain period, typically between 1 – 3 years. On the other hand, another option would be to use a free service like "Let's Encrypt," which offers domain certificate signings but a limited 90 – days expiration window. Furthermore, both options will require certificates rotation handling procedures.

Content distribution networks (CDNs)

While HTTPS guarantees confidentiality and integrity, it doesn't apply to availabilities concerns. Protection from Distributed Denial of Service (DDoS) takes a lot of resources, more than small and

medium businesses could have at their disposal, primarily as these resources can only be used during an attack.

Specialized companies provide Content Distribution Networks (CDNs), which operate global networks with great capacities. By routing HTTPS traffic through these CDNs, the CDN can be used as a filter for the cyber-attack traffic, allowing the proper allocation of resources to increase the availability aspect of the BIM2TWIN platform and providing an extra layer of security against DDoS attacks.

Using CDNs has its pros and cons. Utilizing a CDN like Cloudflare, the Domain Name Service (DNS), the name is set on the CDNs and DNS servers, where CDNs can redirect incoming HTTPS requests to proxy servers on the domain's behalf. Because CDNs are proxy servers, they need to decrypt incoming connections to check their end-destination. Furthermore, the connection content will be read, with the possibility of connection modification, creating a loop-whole for attacks that violate the confidentiality and integrity of the information. On the other hand, an advantage of this service is that CDNs manage the HTTP certificates, reducing administrative overhead needs.

Alternatives to CDNs providing resistance against DDoS attacks will require more active administration of communication traffic, capacity to scale resources (such as Cloud Computing solutions) against DDoS attacks, and additional funding for more resources.

5.6 Web application firewall

A web application firewall (WAF) protects web application servers and infrastructure from attacks and breaches originating from the Internet and external networks. It helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site request forgery, cross-site-scripting (XSS), file inclusion, and SQL injection. A WAF is a protocol layer 7 defense (in the OSI model) and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools that together create a holistic defense against a range of attack vectors

A shield is placed between the web application and the Internet by deploying a WAF in front of a web application. While a proxy server protects a client machine’s identity by using an intermediary, a WAF is a reverse proxy that protects the server from exposure by having clients pass through the WAF before reaching the server.

A WAF operates through a set of rules, often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies.

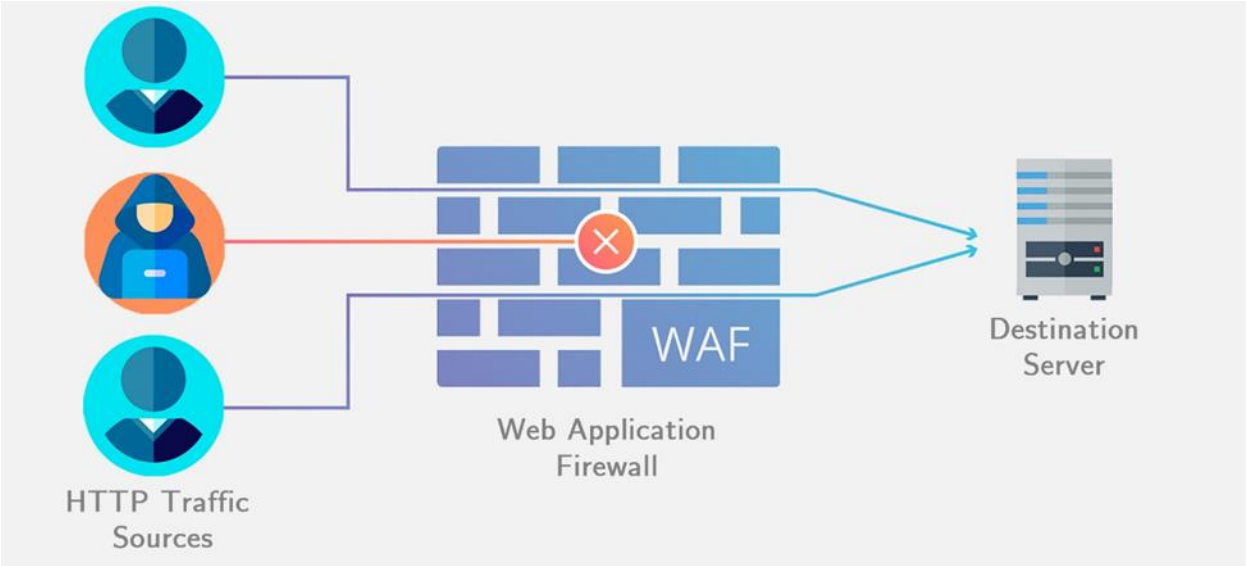

Figure 5. How a WAF works

Cross-Site Request Forgery: Cross-site request forgery (CSRF) is a type of website exploit carried out by issuing unauthorized commands from a trusted website user. It forces an end user to execute unwanted actions on a web application that is currently authenticated. With a bit of help from social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is an average user, a successful CSRF attack can force the user to perform state-changing requests like transferring funds, changing their email address, and so forth. CSRF can compromise the entire web application if the victim is an administrative account.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser cannot know that the script should not be trusted and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

File Inclusion: The File Inclusion vulnerability allows an attacker to include a file, usually exploiting a "dynamic file inclusion" mechanisms implemented in the target application. The exposure occurs due to the use of user-supplied input without proper validation.

File inclusion can lead to something as outputting the contents of the file, but depending on the severity, it can also lead to:

- Code execution on the webserver
- Code execution on the client-side such as JavaScript which can lead to other attacks such as cross-scripting (XSS)
- Denial of Service (DoS)
- Sensitive Information Disclosure

Local file inclusion (also known as LFI) is the process of including files that are already locally present on the server by exploiting vulnerable inclusion procedures implemented in the application. This vulnerability occurs, for example, when a page receives, as input, the path to the file that has to be included, and this input is not properly sanitized, allowing directory traversal characters (such as dot-dot-slash) to be injected. Although most examples point to vulnerable PHP scripts, we should remember that it is also common in other technologies such as JSP, ASP, and others.

SQL injection: A SQL injection attack consists of the insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack in which SQL commands are injected into data-plane input to execute predefined SQL commands.

OSI Model: The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements to support interoperability between different products and software. In the OSI reference model, the communications between a computing system are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

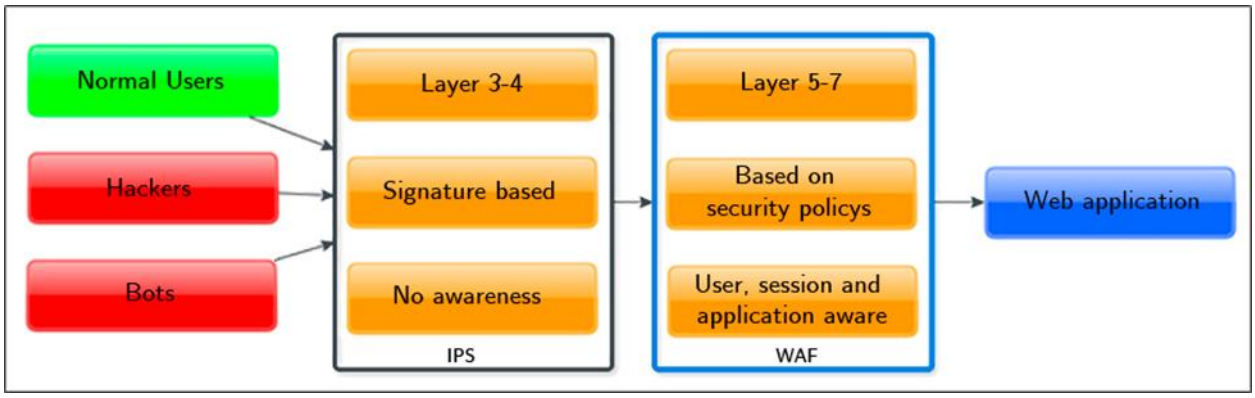

Figure 6. IPS and WAF overview

A WAF can be implemented one of three different ways, each with its benefits and shortcomings:

- **A network-based WAF** is generally hardware-based. Since they are installed locally, they minimize latency, but network-based WAFs are the most expensive option and require physical equipment storage and maintenance.
- **A host-based WAF** may be fully integrated into an application's software. This solution is less expensive than a network-based WAF and offers more customizability. The downside of a host-based WAF is the consumption of local server resources, implementation complexity, and maintenance costs. These components typically require engineering time and may be costly.
- **Cloud-based WAFs** offer an affordable, straightforward option; they usually provide a turnkey installation as simple as a change in DNS to redirect traffic. Cloud-based WAFs also have a minimal upfront cost, as users pay monthly or annually for security as a service. Cloud-based WAFs can also offer a consistently updated solution to protect against the newest threats without any additional work or cost on the user's end. The drawback of a cloud-based WAF is that users hand over the responsibility to a third party. Therefore some features of the WAF may be a black box to them. Learn about Cloudflare's cloud-based WAF solution.

A traditional firewall provides stateful inspection of network traffic. It allows or blocks traffic based on state, port, and protocol and filters traffic based on administrator-defined rules.

A next-generation firewall (NGFW) does this and so much more. In addition to access control, NGFWs can block modern threats such as advanced malware and application-layer attacks. According to Gartner's definition, a next-generation firewall must include:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention

- Application awareness and control to see and block risky apps
- Threat intelligence sources
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

6 CONCLUSION

6.1 Summary of achievements

This document provided a closer look into the data privacy, ethics, and policies and their importance for privacy control to preserve the integrity of the exploited personal information in the BIM2TWIN project. It explains the importance of security policies to ensure continuous successful security operations, manage the web service's data flows, and handle data in the system. It provides data security aspects to handle the BIM2TWIN data with proper confidentiality, integrity, and availability and the responsible legal roles involved in handling the in-system data established in the GDPR (General Data Protection Regulation).

Also, this report tackled the GDPR guidelines regarding video monitoring and data processing regarding the video recording and monitoring aspects of the BIM2TWIN project through the different hardware/sensors installed on the job site. These hardware/sensors monitor the activities and work performed by the on-site personnel; therefore, video anonymization was proposed by the different BIM2TWIN partners to tackle this issue. Likewise, a consent form is proposed to be signed in this report by the on-site personnel informing them of the full scope of the project, about all the hardware/sensors that will be installed on the job site, and how the data exploited by these sensors will be used, stored, and discarded. However, the consent form present in this deliverable is only a first draft of the official consent form that will be included in WP8 - D8.2 Selection, description, and installation of monitoring/acquisition systems in each demo case study due to the reason that the pilot sides are not fully defined at the moment and tasks 8.2 - Install Monitoring Equipment, Task 2.2 - Integration of BIM and project management data, Task 2.3 - Capturing and pre-processing on-site collected data, and Task 2.4 - Capturing and pre-processing data of the operational phase must be completed to provide a fully detailed consent form.

Similarly, this document provides the security and privacy aspects taken into consideration in the BIM2TWIN project to guarantee that only users with proper access to the BIM2TWIN content and data. To ensure this security and privacy, the BIM2TWIN partners had to look at the possible new challenges and technical issues that the whole BIM2TWIN ecosystem approach could face. For this reason, a cybersecurity architecture that connects entities across applications, enabling advanced threat prevention, detection, and mitigation. The proposed holistic architecture proposed in this document also addresses the conventional cloud-based security and privacy controls, authentication and non-repudiation, risk management, and privacy and security policy management. To reach the proposed holistic cybersecurity architecture, the BIM2TWIN partners had a look at the different social engineering techniques used by hackers to gain private information like access tokens, passwords, or valuables. For this reason, some famous cyber-attacks were studied to understand the social engineering tactics and dangers that they present to the BIM2TWIN project data.

Furthermore, this document describes how the security and privacy solutions proposed for the BIM2TWIN are considered in practice, considering the security procedures required for cybercrime prevention like implementing a web application firewall, security audits to assess companies' measures against cyberattacks. These security audits include penetration tests with simulations of cyberattacks and performing vulnerability or security scans to find potential weak points against cyber-attacks.

Lastly, this document provides a closer look at the cybersecurity technologies implemented in the BIM2TWIN project like cryptography, identity verification, user authentication, digital certificates and chain of trust, and connection levels of security.

6.2 Relation to continued developments

The consent form draft template created on this deliverable will be the base for the official one included in WP8 – D8.2 Selection, description, and installation of monitoring/acquisition systems in each demo case study.

Furthermore, the material discussed inside this document are also relevant in the correct development of tasks 8.2 - Install Monitoring Equipment, Task 2.2 - Integration of BIM and project management data, Task 2.3 - Capturing and pre-processing on-site collected data, and Task 2.4 - Capturing and pre-processing data of the operational phase.

REFERENCES

Barker, E. (2020). *NIST Special Publication 800-175B Revision 1 Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*. https://doi.org/10.6028/NIST.SP.800-175Br1

Barker, E., Locke, G., & Gallagher, P. D. (2009). *NIST Special Publication 800-102 Recommendation for Digital Signature Timeliness*. https://doi.org/10.6028/NIST.SP.800-102

CISA. (2020, August 25). *Avoiding Social Engineering and Phishing Attacks | CISA*. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas/tips/ST04-014

European Commission. (2020). *Cybercrime*. https://ec.europa.eu/home-affairs/cybercrime_en

European Parliament and Council of the European Union. (2016a). Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR). *General Data Protection Regulation*, 1–88. https://gdpr-info.eu/art-5-gdpr/

European Parliament and Council of the European Union. (2016b, April 14). *Recital 32 - Conditions for Consent - General Data Protection Regulation (GDPR)*. European Union Regulation. https://gdpr-info.eu/recitals/no-32/

European Parliament and Council of the European Union. (2016c). Recital 60 - Information Obligation - General Data Protection Regulation (GDPR). *European Union Regulation*, 1–88. https://gdpr-info.eu/recitals/no-60/

European Union Agency for Cybersecurity. (2021a, August 26). *Phishing/Spear phishing*. https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing

European Union Agency for Cybersecurity. (2021b, August 26). *What is "Social Engineering"?* https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering

Gutierrez, C. M., & Turner, J. M. (2008). *FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC) CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY*.

Information Commissioner's office. (2016). *What are 'controllers' and 'processors'? | ICO*. Regulation (EU) 2016/679 of the European Parliament and of the Council. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/

Keycloak. (2022, February 24). *Keycloak*. https://www.keycloak.org/

Presidency of the Council of Ministers. (2013). *NATIONAL STRATEGIC FRAMEWORK FOR CYBERSPACE SECURITY*.

WolfSSL. (2020, February 18). *What is a Certificate Chain and the Chain of Trust? - wolfSSL*. https://www.wolfssl.com/certificate-chain-chain-trust/

ANNEX-1 – CONSENT FORM

CONSENT FORM

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 958398.
Call identifier: LC-EEB-08-2020.

INFORMATION NOTICE

PROJECT TITLE

BIM2TWIN

FULL RESEARCHER WITH SCIENTIFIC RESPONSIBILITY FOR THE PROJECT

Name:
Email:
Telephone:
Address:

Information of the responsible researcher with scientific responsibility for the project.

OTHER RESEARCHERS INVOLVED IN THE PROJECT

- *University/Laboratory/Company: Name of the researcher, Responsibility.*
- *University/Laboratory/Company: Name of the researcher, Responsibility.*
- *University/Laboratory/Company: Name of the researcher, Responsibility.*
- *University/Laboratory/Company: Name of the researcher, Responsibility.*

RESEARCH LOCATIONS

Pilot location description.

PURPOSE OF THE RESEARCH PROJECT

The goal of the BIM2TWIN project is to reduce all kinds of operational waste, schedule shortenings, cost reductions, quality, safety improvement, and carbon footprint reduction. It comprises a Digital Building Twin (DBT) platform for construction management that provides full simulation awareness and extensive construction management applications. BIM2TWIN is an EU extraordinary innovation project that creates a Digital Building Twin (DBT) platform for construction site management with artificial intelligence (AI) and semantically linked data techniques. The platform provides a complete situational insight into the as-built and as-performed processes, which uses and compares to the as-designed applications to implement a close-loop plan-do-check-act process. This entire process relies on multiple onsite sensors for data acquisition, cross-domain analysis, and complex AI-based event processing. The Digital Building Twin (DBT) offers a programming interface application that allows construction management applications to cooperate with its data, information, and knowledge bases.

WHAT IS EXPECTED OF YOU

If you agree to participate in the BIM2TWIN project, you will have to agree to be monitored while performing your daily activities at the building pilot project. The duration of your participation will be until the end of the project on April 30th, 2024, at most.
The project partners will implement the usage of sensors and hardware for data collection during the development of the pilot building.

- *Fixed cameras (e.g., on tower cranes) capturing images in regular intervals.*
- *Cameras on drones for photogrammetric reconstruction (as-built geometry).*
- *Laser scanner to capture point clouds (as-built geometry).*

YOUR RIGHTS TO WITHDRAW FROM THE RESEARCH AT ANY TIME

You may discontinue your participation by contacting the study's scientific leader. Your decision to participate, refuse to participate, or discontinue participation will have no repercussions. Following the withdrawal of consent to participate in the study, which may occur at any time, the records will not be deleted since the data exploitation performed on the building pilot site doesn't include any personal data and any image or video recording in which a person can be recognized will use a video anonymization method programmed on the local PC before this information it's sent to the FTP server. This video anonymization method is a pre-trained neural network to detect persons on the pictures (open

source from TensorFlow). TUM will code to program the local PC to blur all sections in the photos and videos where persons are detected. Furthermore, all the data exploited not relevant to the building will be discarded at the end of the project on April 30th, 2024.

YOUR RIGHTS TO CONFIDENTIALITY AND PRIVACY

The data extracted from the hardware and sensors installed in the building pilot project will be treated with the strictest confidentiality. No personal data will be required nor stored into the Building Digital Twin Platform. As mentioned in "your rights to withdraw from the research at any time" any photo or video captured from the job site will use a video anonymization method coded by TUM to blur images and videos on the local PC before they are sent to the FTP server and accessible by the BIM2TWIN partners. Thus, it will not be possible to recognise your face and/or any other personal physical features through the video/pictures taken. Furthermore, all the pictures and videos with no relevance to the building will be discarded at the end of the project on April 30th, 2024.

BENEFITS

The objectives of the BIM2TWIN project are:

- *Enable **real-time response to critical conditions on-site**, primarily of two kinds: a) safety hazards, such as when a worker mistakenly enters the zone of operation of a bulldozer, or b) quality control, such as when a precast component is being placed accurately in position using laser scan control.*
- *Support **evaluation of the current state compared to the intended state** at any point in time. These are value judgments that must answer questions relating to the product (such as "Is the wall in the right place and of the right size?"; "Is the wall built of the right materials and is it's surface planar?") and relating to process (such as "Is the wall masons' productivity too low or as expected?" "Is the project ahead of, on, or behind schedule?"; "Is the project on budget?"). To do this, one must be able to compare an as-designed/as-planned version for any point in time with the as-built/as performed model of the same point in time. PSM information is compared to BIM information.*
- *Support **simulation of future states** based on the current as-built/as-performed state and any alternative future state as-designed/as-planned. Simulations are essential for predicting possible outcomes, which informs managers' decision-making, allowing them to select some optimal future design/plan for delivery to the construction team for execution from any given time forward.*
- *Store the building's product and process information well beyond the construction phase of any given building so that it can support **learning from experience**. Collections of 'historical digital building twins' provide the information for automated learning of various kinds, enabling continuous improvement of design and construction practices on a wide scale.*

POSSIBLE RISKS

The BIM2TWIN project does not involve any significant risk for your personal data since the project doesn't require any personal information and any video or photograph in which the personal identity of any person on the job-site will be blurred before they are sent to the FTP server.

DATA DISSEMINATION AND SHARING

The BIM2TWIN project will not publish any personal data since it will only be reporting on the implementation of sensors and hardware in the construction site and the overall application of the digital building twin platform as a service and its performance on progress monitoring and quality control for volumetric building (WP3), progress and quality monitoring of surface/textural work (WP4), occupational safety and health of workers (WP5), Equipment optimization (WP6), and production planning (WP7).

The only authorized parties to store, process, and discard the data extracted from the installed sensors and hardware on the project pilot site are the BIM2TWIN partners.

You have the right to ask questions about the research at any time by contacting the scientific leader of the project by e-mail or by phone at the following address:

Name:

Email:

Telephone:

INFORMED CONSENT

Project: **BIM2TWIN**

I _____

Born on _____/_____/_____

Residing at (full address) _____

_____

_____

Declare that I have understood the purpose and procedures of this study, which were fully explained to me by _____

_____.

The information about the principle of the study and its interest was communicated to me in the information notice. I had the opportunity to study it carefully. All my questions were answered. I have had sufficient time to consider my decision. I agree to voluntarily participate in the study. The principal investigator is _____.

It was made clear to me that I could refuse to participate in this study and that if I did participate, I could change my mind at any time. I am therefore free to refuse to participate in the study, to stop the study without having to justify myself, or to withdraw my consent during the experiment without incurring any prejudice. Following the withdrawal of consent to participate in the study, which may occur at any time, the records will not be deleted since the data exploitation performed on the building pilot site doesn't include any personal data and any image or video recording in which a person can be recognized will use a video anonymization method programmed on the local PC before this information it's sent to the FTP server. This video anonymization method is a pre-trained neural network to detect persons on the pictures (open source from TensorFlow). TUM will code to program the local PC to blur all sections in the photos and videos where persons are detected. Furthermore, all the data exploited not relevant to the building will be discarded at the end of the project on April 30th, 2024.

It was also explained to me that I can contact the scientific director of the study to ask questions at any time before and during the study at ( ) _____.

I have been informed:

- The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework concerning data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
- Following the law of August 9, 2004, at the end of the study, I can ask the investigator for a summary of the overall results of the research.
- That this study respects the Data Protection Act.

_____ _____

Signature of the person concerned Signature of the investigator