BIMy Project:
D2.3 User/Authorization Model

Document metadata

Date	2021-03-24
Status	Final
Version	2.01
Authors	Alper Kanak, PHD, ERARGE Osman Kumaş, NETAŞ Stijn Goedertier – GIM Steven Smolders – GIM Gözdenur Yeşilyurt- GY
Coordinator	Alper Kanak – ERARGE
Reviewed by	

Version history

Version	Date	Author	Change
0.01	2019-04-14	AKA	Introduction and scope
0.02	2019-05-28	AKA	Role-based access control
0.03	2019-05-29	SGO	User authentication and technical roles
0.04	2019-06-17	SGO	OAuth2 security scopes
0.05	2019-06-18	AKA	Conclusion added and finalized
2.0	2021-03-04 2021-03-23	GN /SGO/SS	Role-Based Authentication / Authorization / Access Control
2.01		GY	Section 5.1 updated

1 Table of Contents

2 Glossary

AEC	Architecture Engineering Construction
AES	Advanced Encryption Standard
BIM	Building Information Model Building Information Modelling Building Information Management
CDE	Common Data Environment
CPS	Cyber-Physical System
DES – 3DES	Data Encryption Standard – Triple DES
ECDSA	Elliptic Curve Digital Signature Algorithm
FM	Facilities Management
GIS	Geographical Information Systems
HSM	Hardware Security Module
IoT	Internet of Things
PC	Personal Computer
PCIeX	Peripheral Component Interconnect Express
RBAC	Role-Based Access Control
RSA	Rivest–Shamir–Adleman cryptosystem
SHA	Secure Hash Algorithm

3 Introduction

This document defines the required mapping rules to convert between the BIM and GIS data standards that are used in the BIMy platform. This chapter introduces the context, objective, scope, and methodology applied to write this document.

3.1 Context: Security Needs of BIMy – GDPR Alignment

The BIMy project, as stated in the Full Project Proposal [1], aims at providing an **open collaborative platform for sharing, storing and filtering BIMs among different BIM owners/users and integrating and visualizing them in their built and natural environment**. BIMy can be seen as an open and generic intermediary that enables interactions between existing and new applications through a unique standardized open API platform. Such a platform will provide a secure collaborative working environment where different stakeholders can benefit and/or utilize BIM models not only at single building level but also at larger levels that can be scaled up to wider-area smart city applications.

BIMy will overcome the limitations of current BIM exchange platforms, providing the following features: **BIM with scale and time** (supporting different levels of details and different stages of the building lifecycle), **BIM/GIS semantic and dynamic integration** and **cloud storage** (integrating BIM in their built and natural environment), BIM filtering (providing relevant information according to stakeholders and applications), cooperation (supporting stakeholder interactions), simulation and 3D visualization (mixed and augmented reality through different devices).

BIMy is bringing into the consortium all the actors necessary to the successful completion of the platform. There are **large companies** that can provide a **Cloud infrastructure** for hosting the BIMy platform and contribute with bigger resources when needed. The **smaller companies** offer more focused know-how to specified tasks as collaboration or BIM sharing and visualization. The **research partners** will support companies with more complicated problems such as creating simple API and modelling and integrating BIM and GIS at different scales and times. **BIM owners/users** have an important role in definition of the requirements, modelling, in offering their expertise for different applications and business models as well as the evaluation of demonstrators. The demonstrators in two different countries improve the chances to make BIMy more replicable to new countries and environments. This enhances remarkably the market potential of BIMy.

3.2 Objective

As stated in the Full Project Proposal [1], the goal of this deliverable is to formally model the semantics and geometric representation of time and scale for BIM models. This modelling will be based on the needs of the domain (stakeholders). T2.1 will then **extend the existing standard IFC with time and scale**. The goal is to **support querying/filtering BIMS in different levels of details** and/or at different stages of the life cycle of a building.

3.3 Scope – Role-based Security-by-Design

In any IT system role-based access control (RBAC) or role-based security is a common approach to restricting system access to unauthorized users. RBAC is a policy-neutral access control mechanism where different roles and privileges are defined. RBAC is mandatory especially in large-scale collaborative WEB platforms where many stakeholders meet in the same virtual environment.

RBAC-by-design is the method adopted in BIMy as well. There are three primary rules in BIMy's RBAC- or Security-by-design strategy:

1. Role assignment
2. Role Authorization
3. Permission Authorization

In role assignment, a BIMy user can exercise a permission only if the user has selected or been assigned a role. Role authorization is related to the user's active role that must be authorized for the subject. Together with the role assignment, role authorization enables and ensures users have the permission on roles for which they are authorized. Finally, permission authorization becomes meaningful with the first two rules which ensures that BIMy users can exercise only permission for which they are authorized.

Secure-by-design or in general secure-by-default is planned to be realized by applying two models incorporating with each other:

- Permission management
- User management.

Such a modular and divided model assures that the BIMy platform has decoupling between user management and permissions. This is a widely accepted concept that allows separate users to create and assign permission sets from the users allowed to create users or user groups.

The permission management is based on a hierarchical model which allows different stakeholders to access to BIM models at different levels of authority. Here, a tree structure is applied which has an implication that architects, engineers, BIM owners, contractors, and other assistive stakeholders can be given specific inheritance of permissions. Such an approach facilitates the user management experience.

3.4 Methodology: Encapsulating Security

In recent distributed cloud applications, there is a need to identify the issues and approaches in addressing security of distributed networks. Along with the wide deployments of distributed IoT networks and mobile devices, the types of attacks are likely to change and evolve from physical domain to cyber-physical domain. Security and privacy have been encountered at a holistic level through an assurance policy regarding the confidentiality, identity, integrity, authentication, access control, non-repudiation of the data that are transmitted in the network, trust and governance, and anonymity.

For instance, a report [2] discusses how the hacking of an IoT device potentially enables the theft and fraudulent exploitation of a large amount of private and confidential data. Moreover, mobile devices can continuously collect and store private and sensitive information (e.g., geographical location, financial data, and consumption habits)[3]. All such studies show that the new IoT era brings the big threat of cyber-

physical attacks in any distributed or heterogeneous system, including the BIM-based collaborative platforms.

CPSs (Cyber Physical Systems) have become a de facto in smart cities, i.e. in the context of power grids [4] and industrial systems[5]. Examples like the Stuxnet, WannaCry ransomware cryptoworms, or Toyota throttle bug extend the cyber-physical attack surfaces that result with life losses, reputation and trust degradation and of course huge money at billion € levels. So, in principle the recent cyber-physical security concept has come forward rather than cyber-only security, and this notion is applicable in any field of smart city public space protection.

3.4.1 BIM Security

BIM is not limited to the planning, design and construction phases of a building or structure. It is intended that information models will be used throughout the asset's lifecycle for asset management, performance monitoring and change management [6]. Since BIM aims to facilitate collaborative working, BIMy envisages the uses of a Common Data Environment (CDE), which should be secured at all levels.

The concept of CDE is very important because it provides a single repository of the infrastructure and the process data related to information generation and exchange between all project stakeholders. Since all buildings can be assumed as critical infrastructures, the following security objectives are also sound for the BIMy platform:

- Confidentiality, including control and authorization of access to information or data
- Integrity, which includes trustworthy operation of electronic and computer-based systems
- Availability of data, information, systems and processes required for the safe, secure and reliable design, delivery and operation of the building or facility

Such a cyber BIM environment, dealing with critical building data (i.e gas pipelines) or private data (bedrooms or financial process data within the construction or planning stages), require a holistic cyber-physical protection strengthened with hardware-based security components and effective cyber-preparedness software or network tools. Such a holistic approach, as already planned to be applied in BIMy, is expected to reduce the attacks surfaces that may be originated from external or internal threat agents and systems or business failures.

4 Role-Based Authentication/Authorization/Access Control

4.1 User authentication

Every user should be able to authenticate with the BIMy platform using an approved identity provider. This means that users could log in to the BIMy platform using for example a Google account, a Gitlab.com account, etc. In a later phase, the BIMy platform could also support authentication via governmental identity providers, such as the national eID schemes, as enabled by the European eIDAS Regulation [7]. The latter is not a priority of the BIMy platform, as eIDAS is only required for *public services*, and we currently do not foresee the BMy platform to be operated by a public authority.

To enable users to authenticate via various platforms, a standard protocol is needed that caters for *federated* authentication. The OAuth 2.0 standard [8] defines a protocol that is nowadays commonly implemented by various identity providers. As part of WP3, we have implemented the "BIMy API" that uses OAuth 2.0 with Gitlab.com as an identity provider.

4.2 Technical Roles

The roles defined below are defined by considering the OAUTH2.0 specifications which mainly describe the simplest use of BIMy platform. Thus, the platform has one or more administrators who have full access rights to the platform whereas the project owners are the coordinators of each BIMy project having full access right to the project. Project editors are also crucial as they create or update BIM data. Finally, users are associated with each project having limited access to BIM model(s) and regarding resources or tools.

The BIMy platform must support a limited set of *technical* roles:

- **Platform Administrator**: has all rights to the platform. The administrator of the platform who able to create projects, give users roles, access all databases. He/she has control of the platform.
- **Project owner**: has the right to create a construction project and grant access to users and editors in that project. After creating a project, he/she will get this role by the platform and can count other users in project.
- **Project editor**: has the right to create or update data in the context of a specific construction project.
- **Project user**: has the right to consult data in the context of a specific construction project.
- **Guest**: can access any information that is made available.

The business roles should be mapped to the above technical roles.

The API of the BIMy platform (see deliverable D1.3) [9, p. 3] reflects these technical roles as OAuth2 security scopes:

- **read:project**: Allows read-only access to your projects on the BIMy platform (project user role).
- **write:project**: Allows read/write access to your projects on the BIMy platform (project editor role).

- **own:project**: Allows to create projects on the BIMy platform (project owner role).
- **admin:platform**: Allows every operation on the BIMy platform.

4.3 Other Roles/Stakeholders and Authorization levels in BIMy

This section defines the roles and stakeholders that can be derived from the requirements identified in deliverable D1.2 Platform applications and requirements [10]. Since BIMy will be organized in terms of BIMy projects which are composed of one or more BIMs and many related stakeholders who various access rights to the projects. There also exist concept roles in BIMy which are described below.

4.3.1 Concept Roles related to the exploitation of BIMy platform within projects

Concept roles are the main actors who will benefit from BIMy directly or indirectly. Direct roles can be the main users of the BIMy outputs at first hand, like firemen or urban planners. Indirect roles on the other hand are the main beneficiaries who can benefit from BIMy outputs indirectly, like seeing or interpreting any BIM assessment result. According to this definition the concept roles, but not limited to, are as follow:

- Clients
- Architects
- Other designers (engineers)
- External advisers
- Contractors
- Facility manager
- Governments:
    - Urban planning
    - Fire department
    - Other First responders
    - Crisis management authorities
    - Tax authorities
- Municipalities
- Insurance companies
- Utility companies
- Marketeers
- Environmental protection administrations

4.3.2 Stakeholders in Construction

A deeper classification of stakeholders specifically in construction sector is given below:

Role/skill set	**Construction stakeholder**
Craft	Site Joiner
	Shop fitter
	Wood machinist
	Bricklayers
	General construction
	Laborer

Role/skill set	Construction stakeholder
	Painter and Decorator
	Ceiling Fixer
	Thatcher
	Roofer
	Scaffolder
	Plant Mechanic
	Plant Operator
	Plasterer
	Demolition Operative
	Steel erectors/structural
	Electrician
Customer	Client
Professional/managerial	Project Manager
	Architects
	Site Supervisor
	Structural Engineer
	Geospatial Modeler
	Quantity Surveyor
	Building Surveyor
	Hydrographic Surveyor
	Construction Manager
	Site Foreman
	Planner
	Facilities Manager
	Town Planner
	Managing Director
	Chairman
	Contracts Manager
	Commercial Manager
Funding	Investors
Group or department	Suppliers
	Pressure groups
	Trade associations
	Regulatory authorities
	Emergency services
	Marketing
	Procurement
Technical	Civil Engineer
	Architectural Technician
	Buyer
	CAD operator
	Construction Technician
	Estimator
	Plant Technician
	Roofing Technician

Role/skill set	Construction stakeholder
Statutory authorities/regulators	Environmental regulators
	Planning authorities
	Building Control/Building Regulations
	Transport and Infrastructure
	Waterways and coastal authorities

Note that one can create new roles in a construction process as it is a very complex procedure and there might be many new stakeholders who can be a part of the process. Hence, the above list can be extended.

4.4 Time-Based Access Control, Authentication and Authorization

Time based access control is also crucial because the authorization level of a stakeholder may differ in such a phase.

- Preliminary design (i.e.: architectural contest)
- Building permit:
- Bidding:
- As-Built:
- Exploitation model:

5 Cyber-Physical Protection: Security of the Entire BIMy Platform

Adopting BIM is not just about the choice of software. To realize the benefits everyone in the architecture, engineering, construction and Facilities Management (FM) industries must work in fundamentally new ways. Both the use of technology and collaborative work processes is essential. Cyber protection of BIMy is about more than cyber technology as it encompasses people, process and governance issues, and their inter-relationships. BIM deals with a complex interaction between governance, people, processes and technology. So, the entire protection and security of the BIMy platform, particularly BIMs that should be kept as secrets, is very crucial and all the stakeholders involved in BIMy should understand the cybersecurity implications.

BIMy, as many CPSs, take the cyber security in the center, but not as a retrofitted feature which is considered by-design. The proposed cyber-physical protection scheme in BIMy addresses the challenge in two dimensions:

1. Traditional Cyber Security and regarding prevention mechanisms (Section 5.1)
2. Hardware-based solution to reduce the attack surface (Section 5.2)

5.1 Cyber Security

BIMy platform and other developed applications have been deployed on Microsoft Azure. To handle platform cyber security, Microsoft Azure Cyber Security services were chosen for handling security requirements. The cyber security services completed in line with the needs defined at the beginning of the project are as follows:

Distributed denial of service (DDoS) attacks are one of the biggest availability and security problems faced by applications running in the cloud. The DDoS attack tries to consume the application's resources and renders the application unavailable to legitimate users. DDoS attacks can target any publicly accessible endpoint on the internet. The scale and capacity of the globally distributed Azure network defends against common network layer attacks through always-on traffic monitoring and real-time risk mitigation. DDoS protection does not require basic, User Configuration, or application changes. DDoS protection helps you protect all Azure services, including basic, PaaS services such as Azure DNS.

The Azure DDoS protection standard provides advanced DDoS mitigation capabilities to defend against DDoS attacks, along with application design best practices. It automatically adjusts to help protect certain Azure resources in a virtual network. Active Traffic monitoring and always on detection and automatic attack mitigation properties have been actively working.

For event correlation management, Azure Sentinel has been used. Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security Orchestration automatic response (Soar) solution. Azure Sentinel delivers smart security Analysis and threat information across the enterprise by providing a single solution for alert detection, threat visibility, proactive search, and threat response.

As New Generation Firewall, Intrusion Detection/Prevention System (IDS/IPS) and Web content filtering, Azure Firewall has been installed on cloud platform. Azure Firewall is a managed, cloud-based security service that protects Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unlimited cloud scalability.

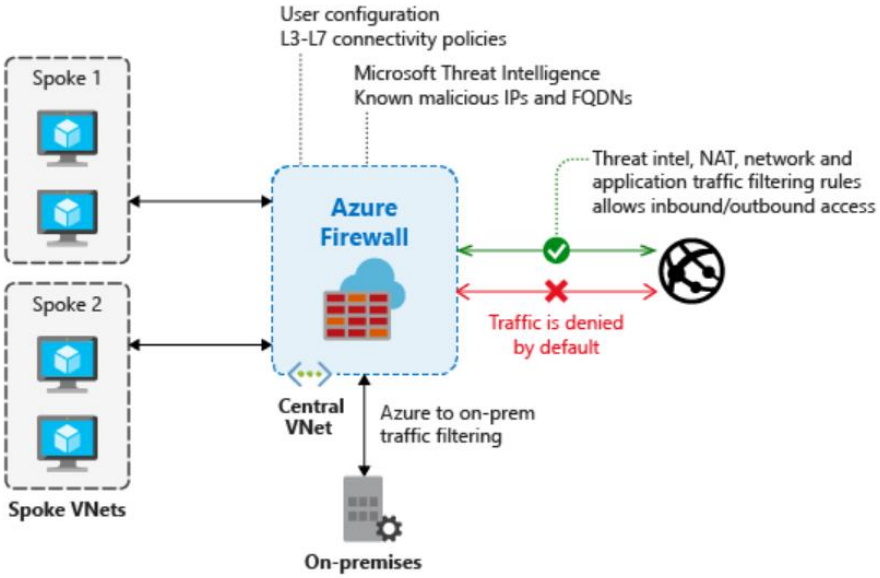

Figure 1: Azure Firewall Architecture

5.2 PRIGM - Hardware Security Module (HSM) to Reduce Attack Surface

In BIMy the security of BIMs will be tackled by integrating sophisticated HSMs in the cyber-physical environment. A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto-processing. By other words, a general-purpose HSM is capable of doing major cryptography operations such as true random number generation, prime number generation, key generation and management, secure key storage and exchange, symmetric encryption (AES, 3DES), asymmetric encryption (RSA, ECDSA), and hashing (SHA). Such a device usually has three different interface peripherals (PCIeX, USB, Ethernet), and it is meant to be connected to a host device (server, PC, etc.) using one of the three available interface peripherals.

The proposed HSM aims to meet the critical security and privacy preservation requirements of BIM environments, especially for trust service providers and for the benefit of BIM owners, decision makers and contractors. As it presents high modularity, the proposed HSM, namely PRIGM developed by ERARGE, can support light-weight or heavy-weight cryptographic functionalities. Among these functionalities and regarding features the following items come forward:

- Electronic signature operations, and electronic sealing operation RSA and ECDSA key pairs.
- Certificate issuance and revocation
- True random number generation using a hardware-based entropy source
- Key generation and derivation

- Key agreement and distribution
- Internal and external secure key storage and management with access control
- Deletion of keys within PRIGM
- Asymmetric encryption and decryption (RSA, ECDSA)
- Symmetric encryption and decryption (AES, 3DES)
- Generation of shared secret values
- Message authentication code generation and verification
- Message digest generation/hashing (SHA)
- Cryptographic support for one-time password, nonces, padding bytes and other non-PKI based authentication mechanisms
- Time stamp operations
- Authentication and authorization

5.2.1 Physical Scope of PRIGM

PRIGM, which is a patented brand of ERARGE [11]–[13], is implemented as an HSM card and is composed of crypto main and daughter boards which are connected to the outer world through an interface daughter board. Note that PRIGM is based on advanced scientific advancements realized within ERARGE and it will be adapted for the use in a cloud environment suitable and fast-enough for BIM storage and processing [14]–[19]. The hardware appliance boundary is depicted with a dashed frame as seen in Figure 1 representing the enclosure of the computing appliances associated with the PRIGM HSM Firmware.

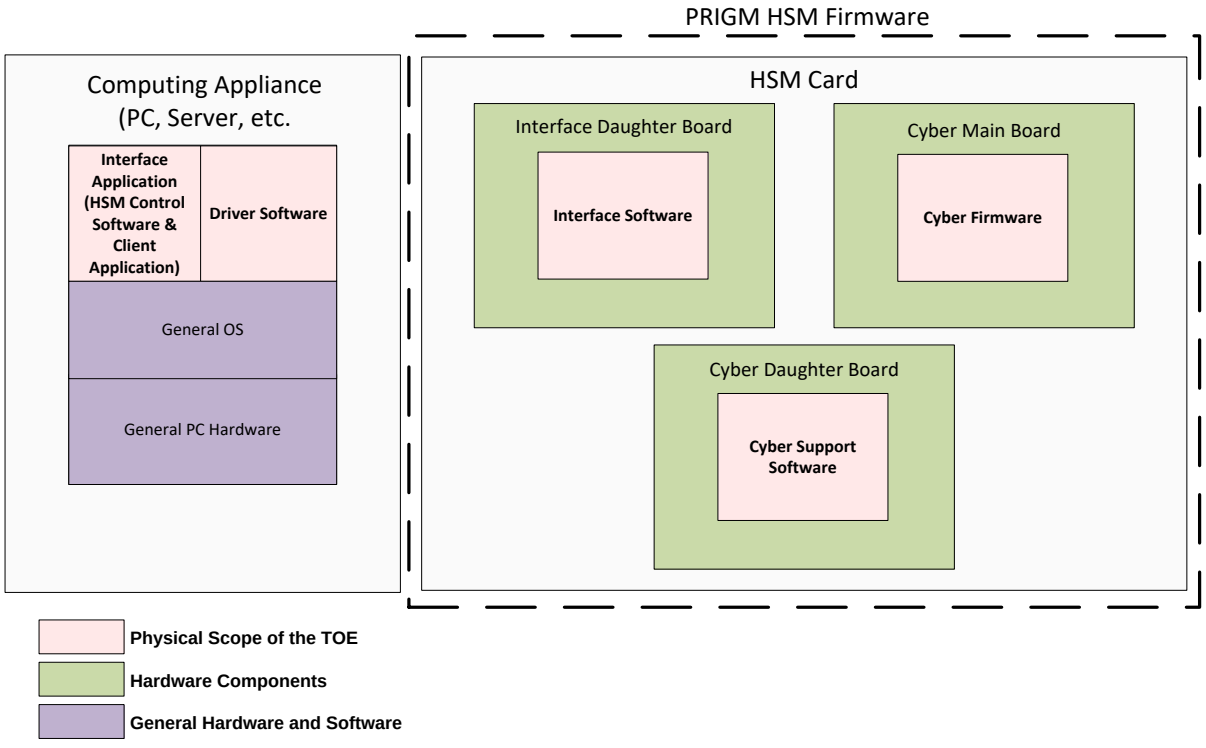

Figure 1. PRIGM® XI-Series HSM

The embedded hardware components are presented in green whereas the PRIGM components are colored in pink in Figure 1. Please note that such a computing appliance can be a server, a PC or an equivalent whose general operating system and its regarding hardware are painted in purple in Figure 1. The HSM Card includes the three software (physical) components of PRIGM, which are listed below:

- **Crypto Firmware**, is a part of PRIGM which is incorporated within the Crypto Mainboard, and is responsible from all main cryptographic functions such as symmetric and asymmetric encryption/decryption, hashing and electronic signing and sealing operations.
- **Crypto Support Software**, is a part of PRIGM which is incorporated within the Crypto Daughterboard, and is responsible from assistive tools like very fast primality check and key management services.
- **Interface Software**, is a part of PRIGM which is incorporated within the Interface Daughterboard, and is responsible for basic two-way data transfer through the PCIeX , USB or Ethernet interface.
- **Interface Application**, is an application on a computing appliance, such as a PC or a server, which performs the main PRIGM functions in close coordination with the HSM Card. Interface Application can be applied in two ways such that:
    - **HSM Control Software** that is developed by the PRIGM provider
    - **Client Application** that is developed by any third-party organization, like an end user

  Such a functionality brings a high practicality as one can directly use the PRIGM by configuring the HSM through the HSM Control Software, or an end user organization can adapt PRIGM's functionality in their own applications.
- **Driver Software** runs on the computing appliance as a typical driver application, which connects the HSM Card to the hosting appliance by utilizing the Interface Software embedded in the Interface Daughterboard.

5.3 User Authorization Strategy Implemented in Year 3

Leading Internet companies, system integrators and security providers have formed the FIDO Alliance (Fast IDentity Online) to revolutionize online authentication with an industry supported standards-based open protocol [Balfanz2015]. The BIMy platform applied FIDO-compliant user authentication integrated with the KeyCloak identity management open-source service. This enables an effective authentication mechanism aligned with the user profiles listed in Section 4.3.2. The integration over BIMy is finalised and reported In the BIMy book [REF????].

As aligned with FIDO, BIMy has an effective authentication and authorization strategy:

- Authentication: In BIMy There is be an authentication mechanism for confirming the user's identity. A registration and login process are applied in order to achieve authentication of users with different access privileges. If a user tries to access the BIMy platform, the user-name and password is asked in order to login the user to the platform. Then, a one-time-password (OTP) is created by the HSM to provide dynamic secure access to the BIMy platform.
- Authorization: Besides authentication, authorization is also be used in the BIMy platform. It is needed because an authenticated user should access only the permitted data not the entire data of a building. For example, a government property should be restricted to the specific users. User role mechanism is used for this purpose. A user is authorized according to his/her role which is defined at registration phase or revised by the authorized persons in the higher hierarchy of the ecosystem.

[Balfanz2015] Balfanz, D., 2015. Fido u2f implementation considerations. FIDO Alliance Proposed Standard (2015): 1-5.

6 Conclusion

This deliverable is prepared to describe the model that is proposed for user authentication and authorization. The model relies on main stakeholders and roles and their access rights according to OAuth2. The deliverable also presents the holistic security strategy that is composed of traditional cyber security components as well as hardware security solutions aiming to provide a better and comprehensive data protection. The proposed tools and devices are planned to be integrated with the BIMy cloud.

7 Bibliography

[1] BIMy consortium, 'BIMy - BIM in the City - ITEA3 Full Project Proposal'. 2017.

[2] Z. Mani and I. Chouk, 'Smart banking: Why it's important to take into account consumers' concerns?', *Work. Pap. HAL*, vol. halshs-01678806.

[3] L. Chin-Lung and L. Judy Chuan-Chuan, 'An empirical examination of consumer adoption of Internet of Things services', *Comput Hum Behav*, vol. 62, no. C, pp. 516–527, Sep. 2016.

[4] S. Sridhar, H. Adam, and G. Manimaran, 'Cyber-Physical System Security for the Electric Power Grid', in *Proceedings of the IEEE 100.1*, 2012, pp. 210–224.

[5] K. Huang and al. et., *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 8153–8162, 2018.

[6] H. Boyes, 'Building Information Modelling (BIM): Addressing the Cyber Security Issues', Institution of Engineering and Technology, 2014.

[7] EU, 'The eIDAS Regulation Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market'. .

[8] IETF, 'The OAuth 2.0 Authorization Framework - RFC6749'. Oct-2012.

[9] BIMy consortium, 'BIMy - BIM in the City - D1.3 Platform and API specifications'. 2019.

[10] BIMy consortium, 'BIMy - BIM in the City - D1.2 Platform applications and requirements'. 2019.

[11] S. Ergun, 'Method and hardware for generating random numbers using dual oscillator architecture and continuous-time chaos', 12006949, EP, 2008.

[12] S. Ergun, 'Method and hardware for generating random numbers using dual oscillator architecture and continuous-time chaos', PCT/IB2007/051938, 2008.

[13] S. Ergun, 'Random numbers generation using continous-time chaos', PCT/TR2006/000035, 2008.

[14] K. Demir and S. Ergun, 'An Analysis of Deterministic Chaos as an Entropy Source for Random Number Generators', *Entropy*, vol. 20, no. 12, p. 957, Dec. 2018.

[15] S. Ergun, 'A Non-Autonomous IC Chaotic Oscillator and Its Application for Random Bit Generation', presented at the Proc. European Conference on Circuit Theory and Design (ECCTD '05), 2005, vol. 2, pp. 165–168.

[16] S. Ergun, 'A high-speed truly random number generator based on an autonomous chaotic oscillator', presented at the Proc. IEEE Asia Pacific Conference on Circuits and Systems (APCCAS '14), 2014, pp. 217–220.

[17] S. Ergun, 'On the Security of Chaos Based "True" Random Number Generators', *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E99-A, no. 1, pp. 363–369, Jan. 2016.

[18] S. Ergun, 'Cryptanalysis of a Random Number Generator Based on a Chaotic Circuit', presented at the 13th conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP '17, 2017, pp. 370–377.

[19] S. Ergun, 'Predicting the Secret Parameters of a Chaotic Random Number Generator from Time Series', in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '19),* 2019, pp. 1–5.