



## White Paper

**Task Force 4: Cross-cutting issues: Business & finance, data, education & upskilling**

**Topic B: Data governance and cybersecurity**

**Revision: V2**

## Document information

### Contributors

First name	Last name	Organisation
<b>Co-Chairs</b>		
Joanna	Syrda	ASM
Emmanuel	François	Smart Building Alliance
<b>Task Force members</b>		
John	Avramidis	Ubitech
Mikel	Borras	IDP
Bonnie	Brook	Siemens
Alexis	David	ECTP
Francisco Javier	Díez	Tekniker
Øystein	Fjellheim	SINTEF
Milan	Gabor	VIRIS
Hrvoje	Keko	Koncar
Agnieszka	Kowalska	ASM
Yassamin	Kouraichi	Dowel Innovation
Karine	Laffont-Eloire	Dowel Innovation
Henrik	Lund Stærmose	Neogrid
Leon	Nilsen	CIRCE
James	O'Donell	UCD
Ioan	Petri	CARDIFF
Richard	Petrie	BuildingSMART International
Lasitha Chamari	Rathnayaka Mudiyanselage	TUE
Juan	Sanchez Valverde	Universidad de Murcia
Antonio	Skarmeta	Universidad de Murcia
Natalie	Samovich	Enercoutim
Marta Maria	Sesana	University of Brescia
Jelena	Simjanovic	BPIE
Jean-Christophe	Vanderhaegen	Confédération Construction Bruxelles-Capitale
<b>Reviewers</b>		
Birgit	Vandeveld	VITO

## Document history

V	Date	Status / Changes
1	09/02/2022	K. Laffont-Eloire, Y. Kouraichi and TF contributors
2	14/03/2022	Birgit Vandeveldde

## Funding



This document has been elaborated in the framework of the SmartBuilt4EU project, funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 956936.

## Disclaimer

The views and opinions expressed in this paper are those of the contributors and do not necessarily reflect the views or positions of any entities they represent, nor those of the European Commission.

## Executive summary

---

*The SmartBuilt4EU project has set up four task forces investigating issues related to smart buildings: their objective is to identify the remaining challenges and barriers to smart building deployment, and the associated research and innovation gaps that should be addressed in the near future.*

*Task force 4 (“Cross-cutting issues”) addresses the transversal requirements (Business & finance, data, education & upskilling) to support the market uptake of smart buildings, and the strengthening of the related ecosystem. A first white paper discussed financing and business models and is available via <https://smartbuilt4eu.eu/publications/>. The topic currently addressed by this task force and presented in this paper is data governance and cybersecurity.*

This white paper therefore aims to provide an overview on what is known and what should be further investigated to answer the following questions:

- What are the existing policies, regulations and certification frameworks relevant to the topic of data governance, privacy and security?
- How are data privacy and cybersecurity accounted for by smart devices manufacturers and installers and how should this be improved to better anticipate future threats and challenges?
- What are the goals of optimal data governance policy? What are the key trade-offs to protect the end-users while enabling new data-driven services?
- How to better manage data access and use for the different stakeholders, while securing quality and accuracy of data?


In the first part of this paper an overview of the state of the art regarding the following issues is provided, specific attention being paid to EC-funded projects:

- Regulation and certification
- Smart devices and cybersecurity
- End-users and data privacy
- Data sharing and data users

A brainstorming process with the Task Force members then enabled to identify some key barriers and drivers regarding data governance, privacy and security. The next diagrams provide an overview of the main barriers and drivers discussed.

 <b>VALUE CHAIN</b>	Interoperability issues on data sharing and security technologies, with different privacy policies, and lack of traceability	<i>Top barriers according to the Task Force</i>
	Lack of common and agreed upon trust models and liability frameworks. Certification labelling not globally accepted	
	Lack of skills for installers of smart devices (who can be the home-owners themselves)	
 <b>REGULATION</b>	Fragmented regulatory and market framework, especially for cybersecurity in buildings	
	Regional or national regulations vs. global approach	
 <b>SOCIAL</b>	Unclear value proposition and added value to users	
	Lack of trust from end-users (related to data security, privacy, risk of being hacked, etc.)	
	Lack of knowledge on digitalisation and data sharing, feeding the fear of losing privacy	
 <b>ECONOMIC</b>	Long payback period of smart building devices which limit the commitment towards a secure digital transition	
	Lack of clear and transparent business models for smart devices and smart services	
 <b>TECHNICAL</b>	No standardisation (incl. semantic interoperability) and numerous legacy standards at the building side.	
	Vendor 'walled garden' offering attractive value proposition to clients but expropriating the data and locking it up in their proprietary clouds.	

**Figure 1: Overview of main barriers**

 <b>VALUE CHAIN</b>	Data is the new gold rush: more and more market actors provide data driven services	<i>Top driver according to the Task Force</i>
	Increased data availability and technical know-how	
 <b>REGULATION &amp; STANDARDS</b>	Push from EU Regulation: new Data Governance Act, GDPR, Cybersecurity Act and Cybersecurity Certification Framework	
 <b>SOCIAL</b>	Increasing user awareness, debate and publicity on cybersecurity risks	
	Increasing requests for transparency and traceability in the management and use of data (including in energy market transactions)	
	Increased willingness to share data as it becomes the (social) norm (e.g. social media) and may be given value	
 <b>ECONOMIC</b>	Rising energy prices and real time pricing driving the need for more secure data sharing	
	Data privacy compliance mechanisms as a source of new business	
 <b>TECHNICAL</b>	Push for integration and harmonisation from different stakeholders, to avoid silos and closed solutions	
	Availability of user-friendly tools and user-friendly interfaces to support data management	

**Figure 2: Overview of main drivers**

Based on the state of the art and the barriers and drivers, a number of research and innovation gaps were identified. These are synthesised in the next diagrams.

The identified 'gaps' will feed the elaboration of the Strategic Research and Innovation Agenda (SRIA) on smart buildings that will be produced by the SmartBuilt4EU consortium by mid-2023, together with some recommendations targeting policy makers.

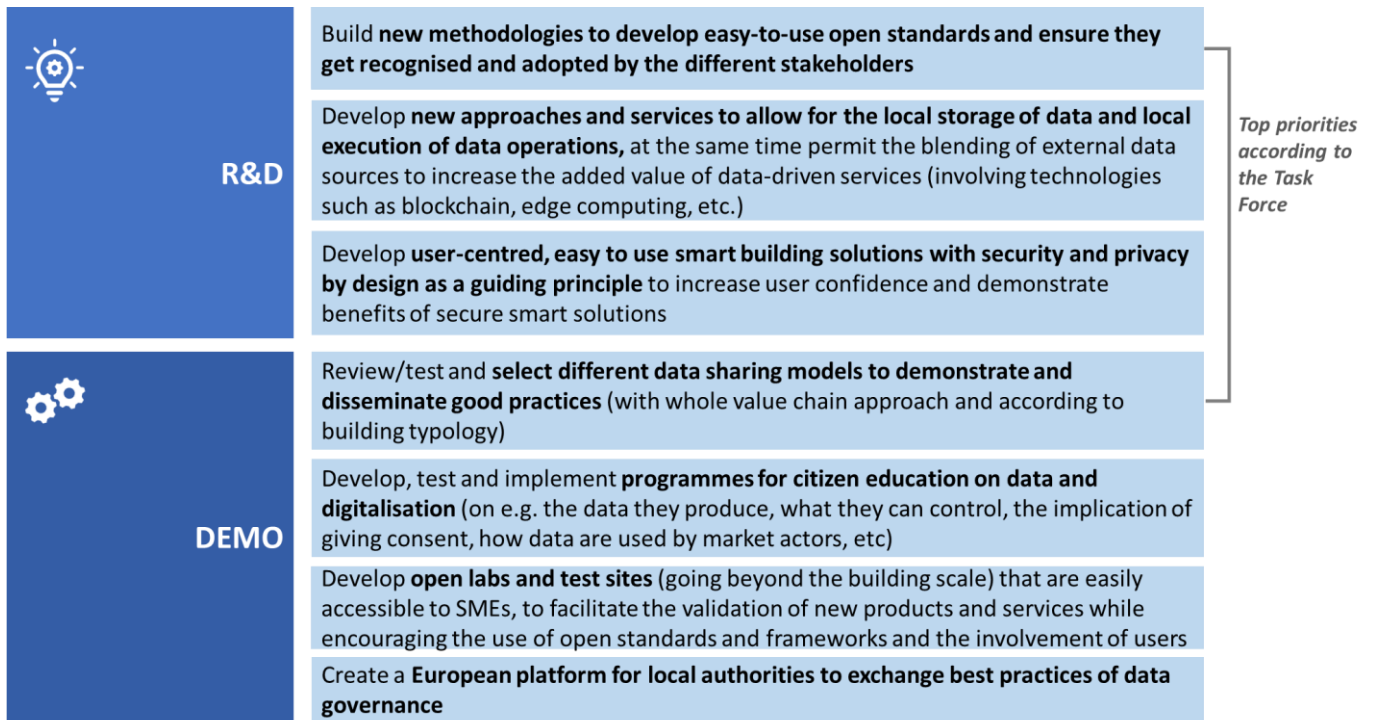


Figure 3: R&I gaps

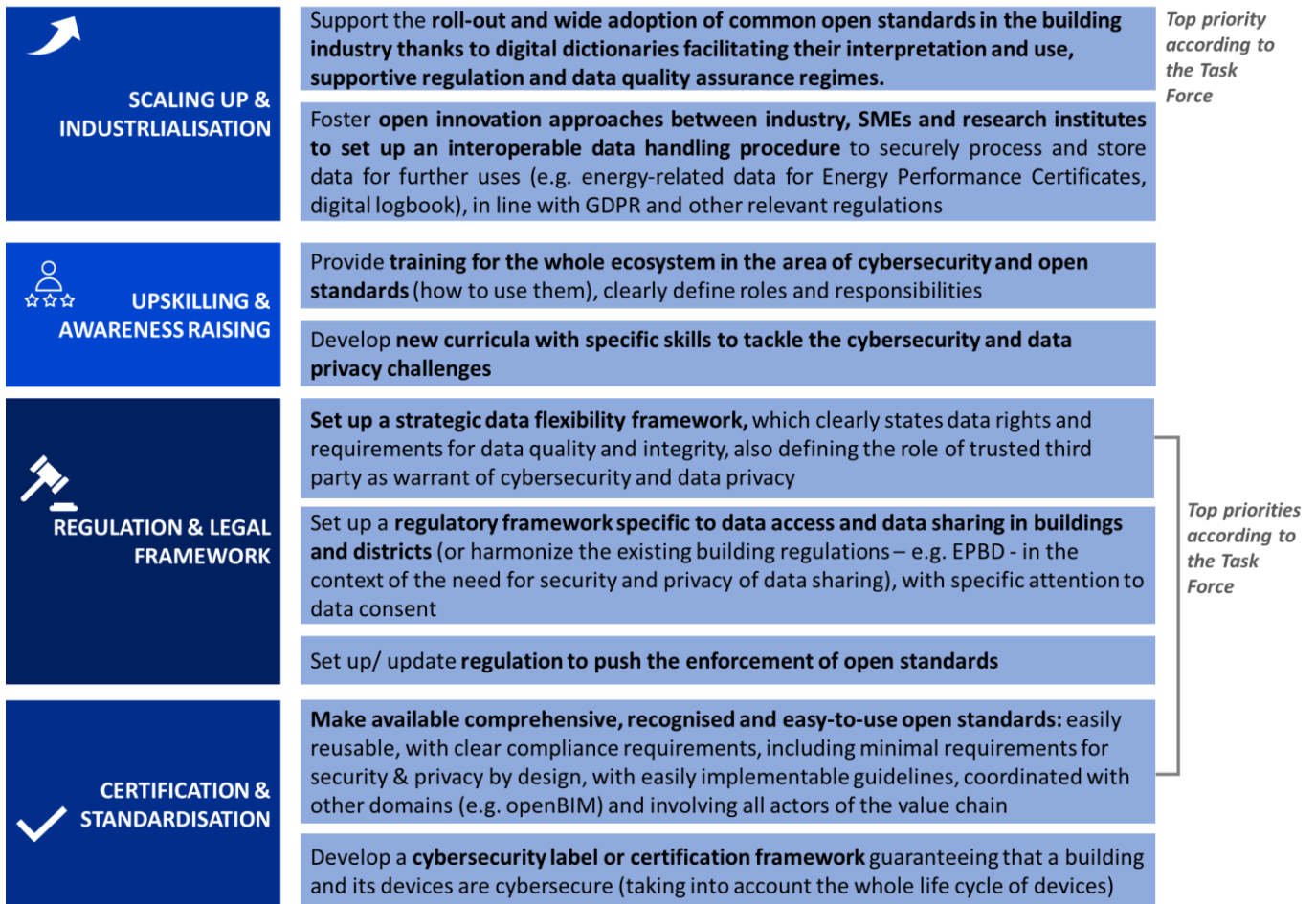


Figure 4: 'Go-to-market' gaps

# Table of content

---

<b>Document information</b> .....	<b>2</b>
<b>Executive summary</b> .....	<b>4</b>
<b>Table of content</b> .....	<b>7</b>
<b>List of abbreviations</b> .....	<b>8</b>
<b>1. Introduction</b> .....	<b>10</b>
<b>2. Topic under investigation by the Task Force</b> .....	<b>11</b>
2.1. RATIONALE .....	11
2.2. SCOPE.....	11
<b>3. State of the Art</b> .....	<b>13</b>
3.1. DEFINITIONS .....	13
3.2. LITERATURE REVIEW .....	14
3.2.1. <i>Overview of relevant regulations &amp; standards</i> .....	14
3.2.2. <i>Smart devices and cybersecurity</i> .....	17
3.2.3. <i>End-users and data privacy</i> .....	19
3.2.4. <i>Data sharing and secure access to data</i> .....	20
3.3. LESSONS LEARNT FROM HORIZON 2020 PROJECTS .....	22
3.3.1. <i>Overview</i> .....	22
3.3.2. <i>Lessons learnt from the PHOENIX project</i> .....	22
3.3.1. <i>Lessons learnt from the PLUG-N-HARVEST project</i> .....	23
3.3.1. <i>Lessons learnt from the FLEXCoop project</i> .....	23
3.4. OTHER INITIATIVES RELATED TO DATA GOVERNANCE, PRIVACY AND SECURITY .....	24
<b>4. Barriers and drivers</b> .....	<b>26</b>
4.1. BARRIERS .....	26
4.2. DRIVERS .....	26
<b>5. Gaps</b> .....	<b>27</b>
<b>6. Conclusion</b> .....	<b>29</b>
<b>7. References</b> .....	<b>30</b>
<b>8. Annex 1: list of H2020 projects reviewed</b> .....	<b>31</b>
<b>9. Annex 2: Additional information provided by EU-funded project PHOENIX</b> .....	<b>34</b>

## List of abbreviations

---

aaS	As a Service
ABAC	Attributed Based Access Control
AEPC	Active Building Energy Performance Contracting
AI	Artificial Intelligence
APPA	Authorized Public Purpose Access
BEMS	Building Energy Management Systems
BIM	Building Information Modelling
BM	Business Model
BMS	Building Management Systems
CC	Common Criteria
CPA	Commercial Product Assurance
CSA	Cybersecurity act
CSPN	Certification de Sécurité de Premier Niveau
DcapBAC	Distributed capability-based access control
DDoS	Distributed Denial of Service
DER	Distributed Energy Resources
DGA	Data Governance Act
DOS	Denial of Service
DR	Demand Response
DSM	Demand Side Management
DSO	Distribution System Operator
EC	European Commission
ENISA	European Union Agency for Network and Information Security
EPBD	Energy Performance of Buildings Directive
EPC	Energy Performance Contracts
ESCO	Energy Service COmpany
eVs	Electric Vehicles
EU	European Union
EUCC	EU cybersecurity certification
FAIR	Findability, Accessibility, Interoperability and Reusability
GDPR	General Data Protection Regulation
HVAC	Heating Ventilation and Air Conditioning
ICT	Information and Communication Technologies
IdM	Identity Management
IED	Intelligent electronic device
IEQ	Indoor Environment Quality
IoT	Internet of Things
ISMS	Information security management system
MUD	Manufacturer Usage Description
OWASP	Open Web Application Security Project
PAP	Policy Administration Point
PDoS	Permanent denial-of-service
PDP	Policy Decision Point
PEP	Policy Enforcement Point



PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RES	Renewable Energy Sources
SBA	Smart Building Alliance
SME	Small and Medium Enterprise
SRI	Smart Readiness Indicator
TF	Task Force
TTP	Trusted Third Party
UL CAP	Cybersecurity Assurance Program of UL
WEF	World Economic Forum

# 1. Introduction

This white paper is produced in the context of the SmartBuilt4EU project, a coordination and support action funded by the European Commission to bring together the research and innovation community on smart buildings.

The SmartBuilt4EU project has set up four task forces with volunteers across all Europe, investigating topics related to smart buildings. They respectively address the interaction between building and end-user, efficient building operation, interactions between the building and the external environment, and cross cutting issues.



Figure 5: The four task forces set up by the SmartBuilt4EU project

SmartBuilt4EU task force 4 on cross-cutting issues addresses the transversal requirements (Business & finance, data, education & upskilling) to support the market uptake of smart buildings, and the strengthening of the related ecosystem.

The Task Force will focus on 3 topics (one per semester):

- **Topic A: Smart financing & business models:** New services and business models (incl. building as a service), integration of new enabling technologies for innovative business models (e.g. blockchain)
- **Topic B: Data governance, privacy and security:** Data ownership and accessibility, regulations protecting the consumer; cybersecurity; data privacy & protection (*this topic will be highly connected to Interoperability addressed in TF2*)
- **Topic C: Education and upskilling:** Better integration of topics related to smart buildings (e.g. smart solutions & user-centric dimensions) in curricula of academic and vocational education; upskilling and training of the building value chain, support to the evolution of businesses (getting digital)

The present white paper focusses on the second topic, i.e. ‘**Data governance and cybersecurity**’. It presents the outcomes of a collective work, carried out with the members of the task force, in several steps:

- Agreement on the scope
- Review of the state of the art and identification of the points to be investigated in particular
- Analysis of barriers and drivers
- Identification of R&I gaps

## 2. Topic under investigation by the Task Force

---

### 2.1. Rationale

---

To reach the EU targets, the building sector must deliver a smarter, more flexible and resilient data-driven built environment. This includes providing technical solutions and services building upon data (including user behaviour data) gathered from smart devices, IoT and embedded sensors. Data storage, protection and accessibility therefore need to be addressed carefully: although data sharing to provide enhanced services and optimise the building operation is highly desirable, buildings cannot turn into “Big Brothers” with potential cybersecurity breaches. Data privacy and cybersecurity of digital assets are indeed pending issues, and there is yet no common data framework for the sector.

While the General Data Protection Regulation (GDPR) entered into force in 2018 and the European Union is developing cybersecurity policies and strategy packages, building occupants and end-users are still largely unaware of their rights with regard to data privacy, of the fate of the data they (sometimes unknowingly) agree to share, and of the cybersecurity risks they are exposed to.

**This white paper therefore aims to provide an overview on what is known and what should be further investigated to answer the following questions:**

- What are the existing policies, regulations and certification frameworks relevant to the topic of data governance, privacy and security?
- How are data privacy and cybersecurity accounted for by smart devices manufacturers and installers and how should this be improved to better anticipate future threats and challenges?
- What are the goals of optimal data governance policy? What are the key trade-offs to protect the end-users while enabling new data-driven services?
- How to better manage data access and use for the different stakeholders, while securing the quality and accuracy of data?

### 2.2. Scope

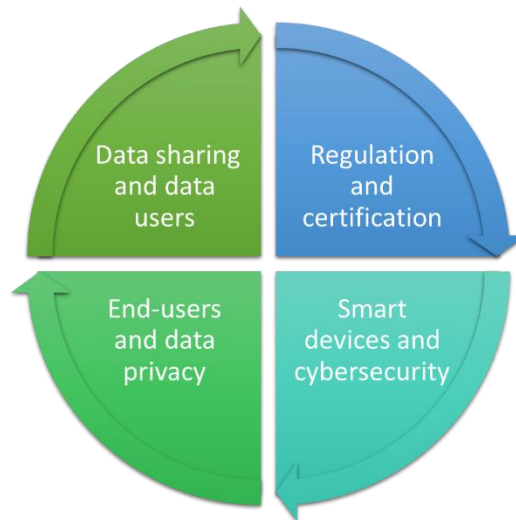
---

The purpose of this section is to define the scope of the topic being investigated. Potential interactions with other topics addressed by the different SmartBuilt4EU Task Forces are also clarified.

The following ‘blocks of knowledge’ were identified by the Task Force:

- **Regulation and certification** framing data governance and cybersecurity. On the regulatory side this includes GDPR, the new Data Governance Act as well as the EU cybersecurity package. With regard to certification, many existing standards are relevant for cybersecurity. However, none of those focuses on smart buildings.
- **Smart devices and cybersecurity:** The widespread use of connected smart home devices and systems provides an attractive platform for targeted cyberattacks by hackers and other unscrupulous operators. Best practices already exist to reduce this risk.
- **End-users and data privacy:** although GDPR gives very clear rules with regard to data privacy and security, it is still unclear how end-users and building occupants can concretely remain in control of their data.

- **Data sharing and data users:** data is a key pillar of the European digital economy. Data sharing and data re-use is however hampered by low trust in data sharing, conflicting economic incentives and technological obstacles.



**Figure 6: Identified blocks of knowledge**

As data governance and cybersecurity is a massive topic, this paper focusses on smart buildings, although interfaces with other systems (e.g. electricity grid for demand response services, eVs) and with the district scale are also included.

Interoperability and data exchange protocols are not addressed in this white paper, as they are already covered by the Topic A of task force 2. For more details related to data exchanges with the grid please also refer to the Topic A of task force 3.

## 3. State of the Art

### 3.1. Definitions

---

#### **Cybersecurity:**

According to European Union's Agency for Network and Information Security (ENISA)<sup>1</sup>, "Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalized telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that cyberspace."

#### **Data governance:**

This notion, crucial for cybersecurity, privacy and the integrity of an activity, is becoming essential at a time when data production can hardly be slowed down. According to the European Commission<sup>2</sup>, the term 'Data governance' means "a set of rules and means to use data, for example through sharing mechanisms, agreements and technical standards. It implies structures and processes to share data in a secure manner, including through trusted third parties".

#### **The Internet of Things (IoT):**

IoT is an interrelated and internet connected system of objects that enables the collection and transfer of data over a wireless network without human intervention. According to Oracle<sup>3</sup>, these objects can range from simple home devices to highly complex industrial tools. With more than 11 billion connected IoT endpoints in 2020<sup>4</sup>, experts expect that number to grow to over 25 billion by 2025.

The European Commission has pinpointed that IoT in Europe should be established on three main pillars<sup>5</sup>: a single market, a thriving ecosystem and remain human centered.

#### **Blockchain:**

Blockchain is a shared, immutable and transparent database (usually referred to as ledger) with a high level of security and no central control unit. The data/ asset recorded in it cannot be modified or falsified. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved. According to the European Commission<sup>6</sup>, blockchain technology allows people and organizations who may not know or trust each other to collectively agree on and permanently record information without a third-party authority. By creating trust in data in ways that were not possible before, blockchain has the potential to revolutionize how we share information and carry out transactions online.

#### **Edge computing:**

Edge computing is used in many applications ranging from smart utility grid analysis, safety monitoring of oil rigs to drone-enabled crop management. According to RedHat<sup>7</sup>, 'Edge computing' is computing that takes

---

<sup>1</sup> <https://www.enisa.europa.eu/publications/definition-of-cybersecurity>

<sup>2</sup> [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_20\\_2103#Data%20governance](https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2103#Data%20governance)

<sup>3</sup> <https://www.oracle.com/fr/internet-of-things/what-is-iot/>

<sup>4</sup> <https://iot-analytics.com/number-connected-iot-devices/>

<sup>5</sup> [https://fsr.eui.eu/wp-content/uploads/2019/09/Isaris\\_keynote.pdf](https://fsr.eui.eu/wp-content/uploads/2019/09/Isaris_keynote.pdf)

<sup>6</sup> <https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy>

<sup>7</sup> [https://www.redhat.com/en/topics/edge-computing/what-is-edge-computing#overview\\*](https://www.redhat.com/en/topics/edge-computing/what-is-edge-computing#overview*)

place at or near the physical location of either the user or the source of the data”. By placing computing services closer to these locations, users benefit from faster, more reliable services while companies benefit from the flexibility of hybrid cloud computing. The European Edge Computing Consortium<sup>8</sup> confirms that the edge computing paradigm enables to execute certain services closer to devices and thereby supplements centralized cloud computing solutions.

### 3.2. Literature review

#### 3.2.1. Overview of relevant regulations & standards

Several regulations, certification frameworks and standards are relevant to the topic of data governance and cybersecurity, as synthesised in the table below. However none of them are specific to smart buildings.

Regulatory document	Main features
<b>General Data Protection Regulation (Regulation (EU) 2016/679)</b>	GDPR, put into effect on May 25, 2018, is the toughest privacy and security law in the world <sup>9</sup> . Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. With the GDPR, Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence.
<b>Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union<sup>10</sup></b>	This regulation aims to ensure that electronic data, apart from personal data, can be processed freely throughout the EU. It bans restrictions on where the data can be stored or processed. The regulation applies to the processing of non-personal data (i.e. any information not linked to an identified or identifiable individual, that is any data other than personal data as defined in point (1) of Article 4 of the GDPR) which is: <ul style="list-style-type: none"> <li>- provided as a service to users living in the EU;</li> <li>- conducted by an individual, company or organisation in the EU for its own needs</li> </ul>
<b>New Data Governance Act</b>	At the end of 2020 the European Commission has announced and presented the Data Governance Act (DGA), a legislative proposal that aims to create a framework which will facilitate data-sharing <sup>11</sup> . According to the European Parliament <sup>12</sup> , thanks to the DGA, <i>“Public sector bodies will have to avoid creating exclusive rights for the re-use of certain data, and exclusive agreements should be limited to a period of 12 months for new contracts, and 2,5 years for existing ones, to make more data available to SMEs and start-ups.”</i>

<sup>8</sup> <https://ecconsortium.eu/>

<sup>9</sup> <https://gdpr.eu/what-is-gdpr/>

<sup>10</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN>

<sup>11</sup> European Commission (25 November 2020). [Proposal for a Regulation of the European Parliament and of the Council on European data governance \(Data Governance Act\) — COM/2020/767 final](#). Brussels, Belgium: European Commission. Retrieved 2021-07-01. Document 52020PC0767.

<sup>12</sup> <https://www.europarl.europa.eu/news/en/press-room/20211129IPR18316/data-governance-deal-on-new-rules-to-boost-data-sharing-across-the-eu>

	A provisional agreement on this new law was reached with the Council and the European Parliament in December 2021. The Commission will also propose a Data Act to encourage data sharing among businesses and between businesses and governance.
<b>EU Cybersecurity Act<sup>13,14</sup></b>	A new EU Cybersecurity Strategy was presented at the end of 2020: it covers the security of essential services such as hospitals, energy grids and railways. It also covers the security of the ever-increasing number of connected objects in our homes, offices and factories. Part of this strategy, the EU Cybersecurity Act strengthens the role of ENISA, which now has a permanent mandate.
<b>EU Cybersecurity Certification framework<sup>15</sup></b>	The purpose of the EU cybersecurity certification (EUCC) framework under the Regulation (EU) 2019/881 is to establish and maintain trust and security on cybersecurity products, services and processes. Drawing up cybersecurity certification schemes at the EU level aims at providing criteria to carry out conformity assessments to establish the degree of adherence of products, services and processes against specific requirements. EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS <sup>16</sup> , was published in May 2021 <sup>17</sup> . The SOG-IS agreement had been produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria.
<b>Legal Framework for Artificial Intelligence<sup>18</sup></b>	The Commission <sup>19</sup> is proposing new rules to make sure that AI systems used in the EU are safe, transparent, ethical, unbiased and under human control. Therefore, they are categorised by risk. The Artificial Intelligence Act stipulates that ‘high-risk’ AI systems that pose significant risks to the health and safety or fundamental rights of persons will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures before those systems can be placed on the Union market.

Standard	Main features
<b>ISO/IEC 27001: Information security management<sup>20</sup></b>	ISO/IEC 27001:2013 is the international standard that provides the specification for an information security management system (ISMS). The standard is designed to help organizations manage their information security processes in line with international best practice.
<b>ISO/IEC 30141:2018 Internet of Things (IoT) — Reference Architecture</b>	This document, published in 2018, provides a standardized IoT Reference Architecture using a common vocabulary, reusable designs and industry best practices. It uses a top-down approach, beginning with collecting the most important characteristics of IoT, abstracting those into a generic IoT conceptual model, deriving a high level system based reference with subsequent dissection of that model into five architecture views from different perspectives.

<sup>13</sup> <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>

<sup>14</sup> <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>

<sup>15</sup> <https://www.enisa.europa.eu/topics/standards/certification>

<sup>16</sup> <https://sogis.eu/>

<sup>17</sup> <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1>

<sup>18</sup> <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

<sup>19</sup> [The role of Artificial Intelligence in the European Green Deal](#)

<sup>20</sup> <https://www.iso.org/isoiec-27001-information-security.html>

<p><b>IEC 62443: Industrial communication networks - Network and system security</b></p>	<p>IEC 62443 is an international series of standards that address cybersecurity for operational technology in automation and control systems. IEC 62443 is relevant for building automation and controls at all levels and does not duplicate any building automation cybersecurity standards<sup>21</sup>. The framework is well suited for unique needs of smart buildings<sup>22</sup>:</p> <ul style="list-style-type: none"> <li>- More predictable failure modes</li> <li>- Tighter time-criticality and determinism</li> <li>- Higher availability</li> <li>- More rigorous management of change</li> <li>- Longer time periods between maintenance</li> <li>- Significantly longer component lifetimes</li> </ul>
<p><b>IEEE 1686-2013: IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities</b></p>	<p>According to IEEE standards association<sup>23</sup>, the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate critical infrastructure protection programs are defined in this standard. Security regarding the access, operation, configuration, firmware revision and data retrieval from an IED is addressed.</p>
<p><b>IEC 62746: Systems interface between customer energy management system and the power management system</b></p>	<p>According to the FLEXCoop<sup>24</sup> project, the IEC 62746 standard defines the system interfaces and communication protocols covering the whole chain between a smart grid and smart home/building/industrial area.</p>
<p><b>RFC 8520: Manufacturer Usage Description Specification</b></p>	<p>The goal of Manufacturer Usage Description specification (MUD) is to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function. The initial focus is on access control. According to the GHOST<sup>25</sup> project, it is a new and very promising standard, focusing on IoT interoperability and security, and which packs a lot of potential in solving some of the IoT-specific security considerations. The project continues to explain that the standard allows IoT device manufacturers to advertise their devices' specifications, and more specifically the intended communication patterns for these devices, when connected to a network.</p>
<p><b>CENELEC - EN 50631-1: Household appliances network and grid connectivity</b></p>	<p>EN 50631-1 defines data models for interoperable connected household appliances, focuses on interoperability of household appliances and describes the necessary control and monitoring.</p>
<p><b>ISO/IEC 27019: Information technology — Security techniques — Information security controls for</b></p>	<p>The ISO/IEC 27019 standard provides guidance based on ISO/IEC 27002:2013 applied to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes. It includes distributed components of smart grid environments, e.g. in energy grids and energy management systems, e.g. of</p>

<sup>21</sup> <https://isasecure.org/en-US/Documents/2019-April-17-Webinar-ISASecure-and-Building-Manag>

<sup>22</sup> <https://www.isasecure.org/en-US/Documents/Saudi-Aramco-Event-Decks/Address-Smart-Building-Cybersecurity>

<sup>23</sup> <https://standards.ieee.org/ieee/1686/5321/>

<sup>24</sup> <https://cordis.europa.eu/project/id/773909/results>

<sup>25</sup> <https://www.ghost-iot.eu/>



<b>the energy utility industry</b>	Distributed Energy Resources (DER), electric charging infrastructures, in private households, residential buildings or industrial customer installations according to the standard's document <sup>26</sup> .
------------------------------------	---

More specifically with regard to cybersecurity, and as pointed out by the EU projects CyberSec4Europe and Eratosthenes, there is an increasing interest to establish a general basis for European security certification and labelling led by ENISA through the cybersecurity act (CSA). In spite of these initiatives, the IoT ecosystem poses specific requirements and challenges to be addressed. Indeed, a security certification methodology for IoT must overcome different obstacles that are inherent to this paradigm. On one hand, the high degree of diversity and heterogeneity of devices and products is in conflict with the need for objective comparisons regarding security aspects. On the other hand, due to the dynamism of typical IoT environments (security and configuration changes, etc.), the certification methodology must take into account these changing conditions, managing the device life cycle and taking into account the context in which the IoT device will be operating. The CSA emphasizes the need for security approaches addressing the lifecycle of any ICT product, service or process for the definition of a cybersecurity certification framework. Therefore, agile self-assessment schemes and test automation environments should be created and evolved to ensure products have a minimum security level appropriate for a context where they are used.

Although there currently are many well-known cybersecurity standards, some of the challenges are not addressed, and the fragmentation between them makes the homogenization and comparison between products certified difficult. The main security certification standard, Common Criteria (CC)<sup>27</sup>, still requires a lot of time and effort to execute an evaluation, and the management of changes in the certified product is limited, since CC certifies a particular version of the product. CC is also complex and difficult to understand, which make an objective comparison<sup>28</sup> more difficult. Other important schemes are the Commercial Product Assurance (CPA)<sup>29</sup>, the Cybersecurity Assurance Program (UL CAP)<sup>30</sup> or the Certification de Sécurité de Premier Niveau (CSPN)<sup>31</sup>. They also use subjective metrics and none of them addresses the challenges related with the dynamism of security, involving a completely heavy recertification in case there is a security change.

Trying to cope with that subjectivity, approaches such as ETSI<sup>32</sup> or ARMOUR<sup>33</sup> decided to combine risk assessment and testing following a test-based risk security assessment, in which testing (ISO 29119) is used to guide and improve the security risk assessment (ISO 31000), adjusting risk values and providing feedback. The ETSI approach only gives some high level guidelines and ARMOUR focuses mainly on the evaluation process, so further connection among the evaluation process and the life cycle changes is still required.

### 3.2.2. Smart devices and cybersecurity

One of the most common examples of IoT includes technologies and applications intended to support the deployment of 'smart home'<sup>34</sup> systems and devices. The smart home market is indeed exploding with

<sup>26</sup> [https://webstore.iec.ch/preview/info\\_isoiec27019%7Bed1.0%7Den.pdf](https://webstore.iec.ch/preview/info_isoiec27019%7Bed1.0%7Den.pdf)

<sup>27</sup> <https://www.commoncriteriaportal.org/>

<sup>28</sup> <https://ieeexplore.ieee.org/document/1264857>

<sup>29</sup> <https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa-security-characteristics>

<sup>30</sup> <https://www.ul.com/offering/cybersecurity-assurance-and-compliance>

<sup>31</sup> <https://www.ssi.gouv.fr/uploads/2015/01/anssi-cspn-cer-p-01-certification-de-securite-de-premier-niveau-v2.0.pdf>

<sup>32</sup> [https://www.etsi.org/deliver/etsi\\_eg/203200\\_203299/203251/01.01.01\\_50/eg\\_203251v010101m.pdf](https://www.etsi.org/deliver/etsi_eg/203200_203299/203251/01.01.01_50/eg_203251v010101m.pdf)

<sup>33</sup> <https://www.sciencedirect.com/science/article/abs/pii/S0920548918301375>

<sup>34</sup> 'Smart home' being understood here as a "home that is equipped with network-connected products connected via Wi-Fi, Bluetooth or similar protocols) for controlling, automating and optimising functions such as temperature, lighting, security, safety or entertainment, either remotely by a phone, tablet, computer or a separate system within the home itself" – as suggested by Coldwell Banker Real Estate and CNET in 2016

internet capability embedded in a large variety of appliances, equipment and systems, including water heater, air conditioner/ heat pumps, thermostat, control systems, smart lighting, security systems and cameras, vacuum cleaner, television, etc. The widespread use of connected smart home devices and systems provides an attractive platform for targeted cyberattacks by hackers and other unscrupulous operators. While the number of reported instances of malicious cyberattacks on smart home systems and devices are relatively small (compared to the billions of deployed devices), university and industry researchers and cybersecurity experts are routinely uncovering vulnerabilities to cyber threats that could compromise consumer privacy, safety and security (UL, 2017)<sup>35</sup>. Common threats include:

- Hackers: Smart devices are particularly susceptible to hacking and device hijacking. Many smart home devices, like thermostats, lights and locks, are of high interest to intruders as they give information about occupancy patterns.
- Data breach / identity theft: IoT devices gather lots of information about the end user. Personal information like addresses, phone numbers, health records and even bank information is handled by smart home devices. Hackers can target these devices and gain the information necessary to steal user identities.
- Man-in-the-Middle: Man-in-the-Middle attacks occur when a hacker interrupts or spoofs the communication happening between two devices.
- Distributed Denial of Service (DDoS): A denial of service attack (DoS) is made to force websites, devices, or entire systems to shut down or become unavailable because of a disruption in its internet connection. DDoS attacks take DoS attacks one step further by flooding a targeted system or device with enough traffic to shut it down and stop it from working. Often, hackers will gain control of IoT devices (usually without a user knowing) and harness the power of hundreds or even thousands of these compromised devices to launch DDoS attacks.
- Permanent Denial of Service (PDoS): Permanent denial of service attacks (PDoS) damage compromised devices to the point of replacement, often referred to as ‘bricking’ a device. One example of a PDoS attack is a feed of inaccurate or faked data to a smart home thermostat that might cause extreme temperature fluctuations, resulting in physical damage to both the device and to the home.

Cybersecurity vulnerabilities in connected smart home systems and devices are most frequently caused by issues related to product design and implementation. The most common causes of cyber-related vulnerabilities generally fall into one of the following five areas:

- Poor product design (lack of even basic security measures)
- Non-secure communication protocols (vulnerable to hacking)
- Inadequate authentication procedures (insufficient password or authentication procedures)
- Limited software updating/patching (e.g. absence of regular system updates or system patches which increases the risk with the passage of time; use of third-party components or open-source software which presents supply chain security issues)

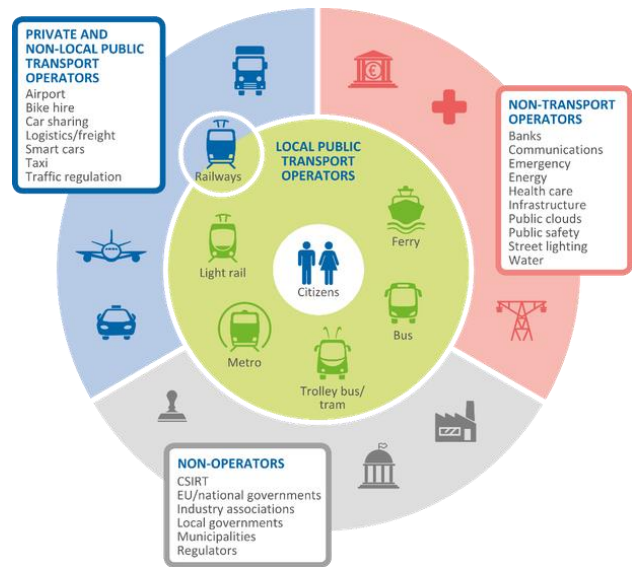


Figure 7: ENISA sectoral approach

<sup>35</sup> UL is a global safety certification company headquartered in the US.

- Improper implementation or device/application use: consumers which install smart homes systems and devices may lack a sufficient understanding of device or network related security considerations

ENISA developed guidance to secure smart infrastructures from cyber threats, by highlighting good security practices and proposing recommendations to operators, manufacturers and decision makers.

ENISA listed more than 80 good practices for IoT<sup>36</sup>, related to privacy by design, authentication, authorisation, hardware security, end-of-life support, secured and trusted communication, secure software and firmware updates, trust and integrity management, training and awareness, etc. ENISA also identified the following gaps:

- Fragmentation in existing security approaches and regulations
- Lack of awareness and knowledge
- Insecure design and/or development
- Lack of interoperability across different IoT devices, platforms and frameworks
- Lack of economic incentives to implement secure design and programming
- Lack of proper product lifecycle management

The recommendations derived from these gaps also provided important inputs to this white paper (Figure 8). ENISA advocates that privacy must be a guiding principle when designing and developing systems, in order to make privacy an integral part of the system.

ID	DESCRIPTION
1	Promote harmonization of IoT security initiatives and regulations
2	Raise awareness for the need for IoT cybersecurity
3	Define secure software/hardware development lifecycle guidelines for IoT
4	Achieve consensus for interoperability across the IoT ecosystem
5	Foster economic and administrative incentives for IoT security
6	Establishment of secure IoT product/service lifecycle management
7	Clarify liability among IoT stakeholders

**Figure 8: IoT Security Recommendations from ENISA (2017)**

### 3.2.3. End-users and data privacy

“Data is the new gold”. According to Deloitte (2018)<sup>37</sup>, technology and data companies have already shown a keen interest in building systems automation for newly-constructed and existing buildings. Specific examples include Alphabet (Nest), Samsung (SmartThings), and Amazon (Alexa). Between technology and the increasing requirements of users and owners, personal and building related data are now accumulating on a large scale.

To ensure trust in data sharing and in line with GDPR, the roles of data processors and data controllers need to be clearly assigned, and all products and services involving access to data should be accompanied with clear information on data handling responsibilities in a clear and transparent language approved through explicit (and informed) user consent, as highlighted by the projects FLEXcoop and HOLISDER, in a paper describing their joint findings on standardisation and interoperability (Keko et al., 2021). However how end-

<sup>36</sup> <https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#IoT> adapted from ENISA (2017) Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures

<sup>37</sup> Deloitte (2018) Data is the new gold: The future of real estate service providers

users can concretely remain in control of their data remains unclear, with no clear data governance framework. The (fine) distinction between personal data and non-personal data is also important: regulation 2018/1807 indeed considers that any information not linked to an identified or identifiable individual becomes non-personal.

The Authorized Public Purpose Access (APPA) approval process, proposed by the World Economic Forum (WEF) in 2021, brings interesting food for thought (Figure 9).

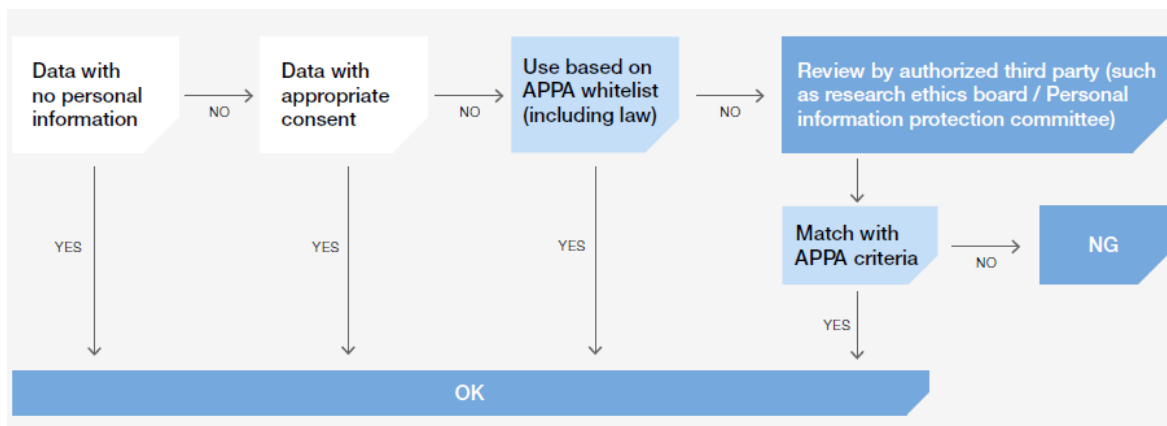


Figure 9: The APPA-based approval process (after World Economic Forum, 2021)

### 3.2.4. Data sharing and secure access to data

Data has become an essential component of tomorrow’s business foundation, and those who can use this data in a profitable way to provide new services will be well-positioned for future success. But, quoting Deloitte, benefiting from it will require settling the question of who controls the data. Legitimately and understandably, both owner and user will claim the right to ‘their’ data.

The projects FLEXcoop and HOLISDER jointly highlighted the challenges related to ‘walled garden’ approaches, i.e. equipment manufacturers offering data services in a vertically integrated cloud solution, with user data and equipment control being then fully captive to the manufacturer’s solution. This lack of interoperability with other solutions prevents the development of new data-driven services, such as flexibility.

For building stakeholders (e.g. real estate) to develop new profitable services, collaboration with users and owners should be intensified and in-house expertise developed to avoid handing over these services (and control over the data) to third parties such as big-data companies (Deloitte, 2018). The new Data Governance Act (DGA), which aims to increase trust in data sharing, create new EU rules on the neutrality of data marketplaces and facilitate the reuse of certain data held by the public sector, should also enable the secure access to data by (new) market players, while ensuring optimal governance and liability.

Experts from the Task Force therefore called for a change of paradigm, from vertically integrated and centralised cloud solutions, fully captive, towards locally stored data (thanks to e.g. edge computing) managed by a third trust party.

The APPA governance structure (WEF, 2021) again brings an interesting approach (Figure 10).

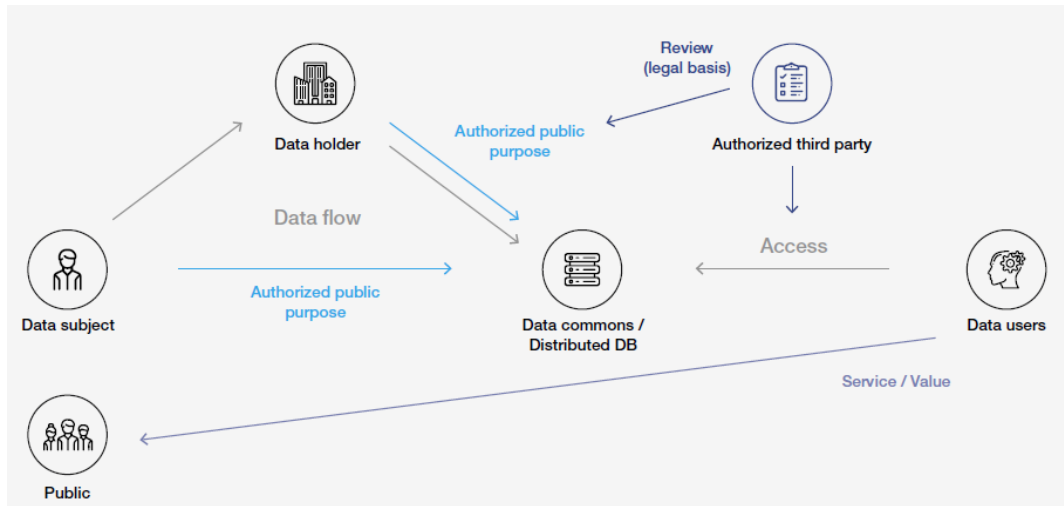


Figure 10: The APPA governance structure (after World Economic Forum, 2021)

### 3.3. Lessons learnt from Horizon 2020 projects

#### 3.3.1. Overview

Many H2020 projects address the topic of data governance, privacy and security: some of them are pictured in Figure 11. Although it is likely that this list is not exhaustive, it covers the projects represented (or mentioned) in the task force.



Figure 11: Relevant H2020 projects identified by the Task Force members

Key lessons learnt or conclusions from some of these projects have already been presented in the state of the art. We will now dive deeper in the lessons learnt from a few selected projects.

#### 3.3.2. Lessons learnt from the PHOENIX project

PHOENIX has a global vision on the new paradigm in which smart homes will be the norm in the near future. An intelligent entity (what buildings will be according to this approach) can establish a dialogue with its peers. For this, part of the project will be dedicated to studying how buildings can communicate with energy suppliers and occupants. The communication will deliver recommendations in both directions so that the occupants have interior spaces brought to the highest standards and on the other hand the energy suppliers can create a more optimized infrastructure.

**Lessons learnt so far include:**

Within project PHOENIX, some privacy and security mechanisms have been designed and developed to achieve data protection from IoT sensors and smart equipment against unauthorised access. Thus, a security and privacy (S&P) framework has been designed to wrap these mechanisms providing a proxy between IoT devices in the building and external applications, as well as a so-called building Smartness Hub.

This S&P framework enables secure authentication and bootstrapping. To achieve that, the framework provides a mechanism to verify the identity of any entity that tries to connect to the PHOENIX Smartness Hub. The bootstrapping process enables the authentication of any entity regarding the required credentials which ends with the generation of an authentication token. The entity can then use this token in future interactions with the PHOENIX Smartness Hub, where the token is held to verify if this concrete entity was authenticated successfully by the S&P framework. This authentication process is performed by an Identity Management (IdM) component.

Regarding anonymised identity management, modern authentication solutions are addressed by PHOENIX to disclose only the minimal amount of data in IoT environments and to allow the user to control this disclosure. These features are not allowed by traditional identity management solutions. The goal of the novel IdM within the S&P framework of PHOENIX is to employ pioneering technologies for keeping the maximum level of entity anonymity, being supported by smart devices and ICT services. Furthermore, the innovations of IdM must enable its deployment at distributed and scalable systems, including deployment at constrained hosts.

Additional information on the solutions developed by PHOENIX can be found in Annex 2.

### ***3.3.1. Lessons learnt from the PLUG-N-HARVEST project***

---

The **PLUG-N-HARVEST** project aims to enhance and enforce ICT safety by understanding how to work safely with computers and environments with lots of technology equipment. ICT Safety puts emphasis on monitoring and controlling access to confidential information, safe transmission of data and secure storage and disposal of data. Based on the project lessons learnt, the consortium has produced a deliverable that contains ethical risks and mitigation strategies regarding the privacy and confidentiality issues. The consortium took into consideration the regulations that concern privacy and data protection in the EU and in each pilot country. All in all, the regulations put a strong focus on the obligation to request consent and fully inform the subject/participant about the data that will be collected while respecting participant's confidentiality.

Worth noting, an Ethical Advisory Board was established within the PLUG-N-HARVEST project to ensure that ethical policy guidelines were communicated to all involved parties and were appropriately adopted, as well as to monitor pilot realization to verify the appropriate use of IT equipment. They also made sure to be assisted by further external experts (or the Commission), if necessary.

#### **Good practices include:**

- Comply with the GDPR regulation and also take into account the Data Protection related regulation in the pilot countries.
- Ensure the respect of anonymity of the participants and requesting consent.
- Fully inform participants about the data collected and their rights.
- The Ethical Advisory Board proved to be a crucial part and the backbone of this project when coming to data privacy issue solving.

### ***3.3.1. Lessons learnt from the FLEXCoop project***

---

The **FLEXCoop** project consortium was composed of ICT and energy experts working hand in hand with energy cooperative actors aiming to develop and demonstrate new demand-side flexibility tools and related business models for energy cooperatives. FLEXCoop's aim has been to contribute to the democratisation of the energy system by providing citizens initiatives with the tools to take a more active role in the energy system and open new services to enable them to accelerate the decarbonisation of the energy system.



In its public deliverable on policy/market reform recommendations (D8.11), the project partners have shared a set of guidelines to implement strong data governance strategies and join the European energy data space initiative. The report includes best practices to secure the citizen approach in the digital sector.

**Lessons learnt so far include:**

- A strong framework must be put in place by energy cooperatives for their own data access and usage.
- Energy cooperatives should follow a clear ‘energy data strategy’ that seeks economic and societal benefits of data availability.
- Cooperatives should consider becoming data cooperatives with respect to the principles on Findability, Accessibility, Interoperability and Reusability (FAIR) of data taking into account the developments and decisions of sector-specific authorities.
- It is essential to clear up the rules about data usage rights and to establish agreements to be used throughout the process.

### 3.4. Other initiatives related to data governance, privacy and security

Name of initiative	Relevant inputs
<p><b>Smart Building Alliance / R2S</b></p>	<p>The R2S framework developed by the Smart Building Alliance (SBA) is a guarantee of cybersecurity and data protection. R2S has indeed an incompressible technical base that makes it possible to define a framework and requirements to promote better information and communication flows, while at the same time compartmentalising access authorisations. The R2S framework is structured in three layers, with rules to ensure that everything is interoperable: a support layer, which hosts the connected objects, an IP (Internet Protocol) channel layer, to convey the data, and an application layer, which delivers services to residents. With this architecture, barriers can be set up within the building's networks, authorising access to certain people and blocking others. The information ‘highway’ can also be traced in the building to determine which data enter, which leave and how fast. The R2S label brings another advantage, in terms of privacy and protection of personal data: R2S requests operators to detail what data is collected and, above all, for what purpose.</p> <p>SBA will soon publish the “Manifesto of the Citizen of the 21st Century”. This manifesto treats the key topics concerning Human rights at Digital Era. SBA will also publish a white book on cybersecurity applied to smart buildings and smart cities.</p>
<p><b>“Authorized Public Purpose Access” Data Governance Model by the World Economic Forum</b></p>	<p>A first white paper<sup>38</sup> published in January 2020 by WEF presented the Authorized Public Purpose Access (APPA) data governance model. APPA postulates that data must be connected in order to create value, in particular for public health purposes. A second white paper<sup>39</sup> (WEF, 2021) proposed a systematic approach to implementing APPA and pursuing public-interest goals through data use.</p>
<p><b>OpenADR alliance</b></p>	<p>The OpenADR Alliance was created to standardize, automate, and simplify demand response (DR) and Distributed Energy Resources (DER) to enable utilities and</p>

<sup>38</sup> <https://www.weforum.org/whitepapers/appa-authorized-public-purpose-access-building-trust-into-data-flows-for-wellbeing-and-innovation>

<sup>39</sup> [https://www3.weforum.org/docs/WEF\\_Resetting\\_Data\\_Governance\\_2021.pdf](https://www3.weforum.org/docs/WEF_Resetting_Data_Governance_2021.pdf)



	aggregators to cost-effectively manage growing energy demand & decentralized energy production, and customers to control their energy future. In order to fulfil industry security requirements and NIST <sup>40</sup> Cyber Security guidelines, the OpenADR Alliance maintains its own Public Key Infrastructure (PKI)
<b>OWASP</b>	<p>The Open Web Application Security Project® (OWASP) is a non-profit foundation that works to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is a source for developers and technologists to secure the web.</p> <p><a href="https://owasp.org/www-project-internet-of-things/">https://owasp.org/www-project-internet-of-things/</a></p>




---

<sup>40</sup> US National Institute of Standards and Technologies

## 4. Barriers and drivers

### 4.1. Barriers

Barriers to the market uptake of smart buildings (and the strengthening of the related ecosystem) related to data governance, privacy and security were reviewed and prioritised by the task force. The top barriers are highlighted below.

 <b>VALUE CHAIN</b>	Interoperability issues on data sharing and security technologies, with different privacy policies, and lack of traceability	<i>Top barriers according to the Task Force</i>
	Lack of common and agreed upon trust models and liability frameworks. Certification labelling not globally accepted	
	Lack of skills for installers of smart devices (who can be the home-owners themselves)	
 <b>REGULATION</b>	Fragmented regulatory and market framework, especially for cybersecurity in buildings	
	Regional or national regulations vs. global approach	
 <b>SOCIAL</b>	Unclear value proposition and added value to users	
	Lack of trust from end-users (related to data security, privacy, risk of being hacked, etc.)	
	Lack of knowledge on digitalisation and data sharing, feeding the fear of losing privacy	
 <b>ECONOMIC</b>	Long payback period of smart building devices which limit the commitment towards a secure digital transition	
	Lack of clear and transparent business models for smart devices and smart services	
 <b>TECHNICAL</b>	No standardisation (incl. semantic interoperability) and numerous legacy standards at the building side.	
	Vendor 'walled garden' offering attractive value proposition to clients but expropriating the data and locking it up in their proprietary clouds.	

### 4.2. Drivers

The drivers identified by the task force are as illustrated below. As for the barriers, the strongest drivers (according to the Task Forces member) are related to users.

 <b>VALUE CHAIN</b>	Data is the new gold rush: more and more market actors provide data driven services	<i>Top driver according to the Task Force</i>
	Increased data availability and technical know-how	
 <b>REGULATION &amp; STANDARDS</b>	Push from EU Regulation: new Data Governance Act, GDPR, Cybersecurity Act and Cybersecurity Certification Framework	
 <b>SOCIAL</b>	Increasing user awareness, debate and publicity on cybersecurity risks	
	Increasing requests for transparency and traceability in the management and use of data (including in energy market transactions)	
	Increased willingness to share data as it becomes the (social) norm (e.g. social media) and may be given value	
 <b>ECONOMIC</b>	Rising energy prices and real time pricing driving the need for more secure data sharing	
	Data privacy compliance mechanisms as a source of new business	
 <b>TECHNICAL</b>	Push for integration and harmonisation from different stakeholders, to avoid silos and closed solutions	
	Availability of user-friendly tools and user-friendly interfaces to support data management	

## 5. Gaps

Various activities required to overcome barriers and leverage drivers (related to data governance, privacy and security) were suggested and prioritised by the task force members (Table 1). The priority ones according to the Task Force are in bold.

**Table 1: Suggested R&I activities**

Type of activity	Activities
<b>R&amp;D</b>	<ul style="list-style-type: none"> <li>- <b>Build new methodologies to develop easy-to-use open standards and ensure they get recognised and adopted by the different stakeholders</b></li> <li>- <b>Develop new approaches and services to allow for the local storage of data and local execution of data operations</b>, and at the same time permit the blending of external data sources to increase the added value of data-driven services (involving technologies such as blockchain, edge computing, etc.)</li> <li>- Develop user-centred, easy to use smart building solutions with privacy by design as a guiding principle to increase user confidence and demonstrate benefits of secure smart solutions</li> <li>- Develop an open source and free cybersecurity software solution for smart buildings</li> </ul>
<b>Demonstration</b>	<ul style="list-style-type: none"> <li>- <b>Review/test and select different data sharing models to demonstrate and disseminate good practices</b> <ul style="list-style-type: none"> <li>▪ Including all value chain stakeholders and users in the building lifetime</li> <li>▪ Tailored to the building typology as data and value chain differ</li> </ul> </li> <li>- Develop, test and implement programmes for citizens education on data and digitalisation (e.g. on the data they produce, what they can control, the implication of giving consent, how data are used by market actors, etc)</li> <li>- Create a European platform for local authorities to exchange best practices of data governance</li> <li>- Develop Open Labs and test sites (going beyond the building scale), easily accessible to SMEs, to facilitate the validation of new products and services while encouraging the use of open standards and frameworks and the involvement of users (also embracing the community of Do-it-Yourself users)</li> </ul>
<b>Scaling up &amp; industrialisation</b>	<ul style="list-style-type: none"> <li>- <b>Support the roll-out and wide adoption of common open standards in the building industry thanks to digital dictionaries facilitating their interpretation and use, supportive regulation and data quality assurance regimes.</b></li> <li>- Foster open innovation approaches between industry, SMEs and research institutes to set up an interoperable data handling procedure to register and securely store data for further uses (e.g. energy-related data for Energy Performance Certificates, digital logbook), in line with GDPR and other relevant regulations. This also includes preparing clear and secure endpoints for data exchange, agreeing upon standards for data exchange, using digital identities for permissions to grant access to data and keeping audit trails on who accessed that data.</li> </ul>
<b>Certification &amp; standardisation</b>	<ul style="list-style-type: none"> <li>- <b>Make available comprehensive, recognised and easy-to-use open standards:</b> <ul style="list-style-type: none"> <li>▪ Permissively licensed implementations of open standards that can be reused by different vendors</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>▪ Compliance requirements with clear cut tests so that the solutions can receive a certification</li> <li>▪ Security &amp; privacy by designing minimal requirements and easily implementable guidelines</li> <li>▪ Coordinated with other domains (i.e. openBIM and openGIS)</li> <li>▪ Involving all actors of the value chain (operators, IT companies, public authorities and users)</li> </ul> <ul style="list-style-type: none"> <li>- Develop a cybersecurity label or certification framework guaranteeing that a building and its devices are cybersecure</li> <li>- Develop a cybersecurity label taking into account the whole life cycle of the device</li> </ul>
<b>Regulation &amp; legal framework</b>	<ul style="list-style-type: none"> <li>- <b>Set up a strategic data flexibility framework</b>, which clearly states data rights and requirements for data quality and integrity, also defining the role of trusted third parties as warrant of cybersecurity and data privacy</li> <li>- Set up a regulatory framework specific to data access and data sharing in buildings and districts (or harmonize the existing building regulations – e.g. EPBD - in the context of the need for security and privacy of data sharing), with specific attention to data consent</li> <li>- Set up/ update regulations to push the enforcement of open standards</li> </ul>
<b>Upskilling &amp; awareness</b>	<ul style="list-style-type: none"> <li>- Provide training for the whole ecosystem in the area of cybersecurity and open standards (how to use them), clearly define roles and responsibilities</li> <li>- Develop new curricula with specific skills to tackle the cybersecurity and data privacy challenges</li> </ul>

## 6. Conclusion

---

This document formalises the collaborative work performed by the members of SmartBuilt4EU task force 4, on a voluntary basis, during the period October 2021- January 2022. It also integrates the feedback collected during 1) a peer review conducted by VITO in March 2022, and 2) an open consultation process during in April-May 2022.

Based on an analysis of the state of the art and the identification of barriers and drivers, the main objective of this paper is to detect some research and innovation gaps that still need to be addressed in the coming years in order to improve and safeguard data governance, privacy and security related to smart building solutions and systems.

This white paper will feed the elaboration of the Strategic Research and Innovation Agenda that the SmartBuilt4EU consortium will present to the European Commission.

Task force 4 will investigate one more topic during 2022: next topic, starting May 2022, will focus on **Education and upskilling**, i.e. it will address key issues such as a better integration of topics related to smart buildings (e.g. smart solutions & user-centric dimensions) in curricula of academic and vocational education; upskilling and training of the building value chain, support to the evolution of businesses (getting digital).

If you have some expertise to share on this topic, you are invited to join the task force and contribute to the next white paper (contact detail below).

**To receive the updates on the SmartBuil4EU task forces, white papers and events, please register here:**  
<https://smartbuilt4eu.eu/join-our-community/>

**Contact point for task Force 4:**

Karine LAFFONT-ELOIRE, DOWEL Innovation, [karine.laffont@dowel.eu](mailto:karine.laffont@dowel.eu)

## 7. References

---

- A. Psychas, A. Androutsopoulou (2020). D8.7 Standardization Report. Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control - GHOST Project.
- B. Kežmah (2020). D3.6 Guidelines for GDPR Compliant User Experience – Cyber Security for Europe.
- Deloitte (2018) Data is the new gold: The future of real estate service providers
- ENISA (2017) Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures
- L. Hernández-Ramos, A. J. Jara, L. Marín, and A. F. Skarmeta (2014) “DCapBAC: Embedding Authorization logic into Smart Things through ECC optimization” International Journal of Computer Mathematics 93(2)
- H. Keko, S. Sučić, L. Luttenberger Marić, P. Hasse, K. Isakovic (2021) Widening the path for demand-side flexibility services in European households: Joint findings of the FLEXCoop & HOLISDER projects in standardization & Interoperability <http://www.flexcoop.eu/blog/widening-the-path-for-demand-side-flexibility-services-in-european>
- R. Tual, S. Cuno, M. Antón, K. Valalaki, P. Bacher, J. Aranda, J. Cipriano, P. Pañella (2021). D8.11-Policy/Market Reform Recommendations Report - Final Version – FlexCoop project.
- UL (2017) Cybersecurity considerations for connected smart home systems and devices (White Paper).
- World Economic Forum (2021) Resetting Data Governance: Authorized Public Purpose Access and Society Criteria for Implementation of APPA Principles. White Paper [https://www3.weforum.org/docs/WEF\\_Resetting\\_Data\\_Governance\\_2021.pdf](https://www3.weforum.org/docs/WEF_Resetting_Data_Governance_2021.pdf)



## 8. Annex 1: list of H2020 projects reviewed

Table 2: list of relevant EU projects

Project	Status	Contact in TF	Weblink	Relevant inputs
 BIGG	ongoing		<a href="https://www.bigb-project.eu/">https://www.bigb-project.eu/</a>	Building Information aGGregation, harmonization and analytics platform
 BEYOND	ongoing	John Avramidis	<a href="https://beyond-h2020.eu">https://beyond-h2020.eu</a>	BEYOND introduces a reference big data platform implementation for collecting, processing and analyzing building data, while transforming them into a tradeable commodity through the development of appropriate data sharing mechanisms for data sharing between different stakeholders.
 Cyber Security for Europe	Ongoing	Antonio Skarmeta	<a href="https://cybersec4eu.ropc.eu/">https://cybersec4eu.ropc.eu/</a>	CyberSec4Europe is designing, testing and demonstrating potential governance structures for a future European Cybersecurity Competence Network using best practice examples derived from concepts like CERN as well the expertise and experience of partners.
 DigiPLACE	Ongoing	Alexis David	<a href="http://www.digiplaceproject.eu">www.digiplaceproject.eu</a>	DigiPLACE is a framework allowing the development of future digital platforms as common ecosystems of digital services that will support innovation, commerce, etc. It will define a Reference Architecture Framework for digital construction platform based on an EU-wide consensus involving a large community of stakeholders, resulting in a strategic roadmap for successful implementation of this architecture.
 ERATOSTHENES	Ongoing	Antonio Skarmeta	<a href="https://cordis.europa.eu/project/id/101020416">https://cordis.europa.eu/project/id/101020416</a>	ERATOSTHENES will devise a novel distributed, automated, auditable, yet privacy-respectful, Trust and Identity Management Framework intended to dynamically and holistically manage the lifecycle of IoT devices, strengthening trust, identities, and resilience in the entire IoT ecosystem, supporting the enforcement of the NIS directive, GDPR and the Cybersecurity Act.
 FLEXCoop	Completed		<a href="http://www.flexcoop.eu/">http://www.flexcoop.eu/</a>	FLEXCoop introduces an end-to-end Automated Demand Response Optimization Framework. It enables the realization of novel business models, allowing energy cooperatives to introduce themselves in energy markets under the role of an aggregator. It equips cooperatives with innovative and highly effective tools for the establishment of robust business practices to exploit their microgrids and dynamic VPPs as balancing and ancillary assets toward grid stability and alleviation of network constraints.
 frESCO	Ongoing	CIRCE Leon Nielsen	<a href="https://www.fresco-project.eu/about/">https://www.fresco-project.eu/about/</a>	New business models for ESCOs and agregators for residential consumers. frESCO aims to integrate existing big data technologies, tools and libraries, with energy-relevant legacy systems and ICT-enabled assets and components to accelerate the data management and analysis cycle for powering the frESCO innovative services, turning the 4 Big Data V's into Stakeholder Value

	completed		<a href="https://www.ghost-iot.eu/">https://www.ghost-iot.eu/</a>	<p>The GHOST project provides high-level cybersecurity to regular smart home users. Using data analytics, GHOST inspects smart home networks for irregular and potentially malicious behaviour. The software notifies the user of any irregular patterns and is designed to be user-friendly.</p>
	completed	Ander Romero	<a href="http://holisder.eu/reports/">http://holisder.eu/reports/</a>	<p>The backbone of HOLISDER project consists in an “open” and modular interoperability and data management framework that will enable open standards-based communication along the DR value chain. It will integrate two main commercial technologies/ products (JACE, EF-i) to ensure seamless information exchange, communication and operation on top of any Building and District EMS, as well as, Smart Home systems/devices.</p>
	Ongoing	Antonio Skarmeta	<a href="https://eu-phoenix.eu/">https://eu-phoenix.eu/</a>	<p>PHOENIX will build an interoperable architecture with advanced capacity to incorporate and process all kinds of building data and knowledge to improve the intelligence of services offered to end-users and stakeholders.</p>
	completed	Antonio Skarmeta	<a href="https://www.plug-n-harvest.eu/">https://www.plug-n-harvest.eu/</a>	<p>The main strategic goal of the PLUG-N-HARVEST proposal is to design, develop, demonstrate and exploit a new modular, plug-n-play concept/product for ADBE - deployable to both residential and non-residential buildings.</p>
	Ongoing		<a href="https://praetorian-h2020.eu/about/">https://praetorian-h2020.eu/about/</a>	<p>PRAETORIAN Physical Situation Awareness (PSA) and Cyber Situation Awareness (CSA) components will gather huge amounts of heterogeneous data from the different sectorial CIs (airports, ports, power plants, and hospitals) involved in the pilot demonstrations. CSA will explore the network and CI's Information System to identify malicious patterns.</p>
	Ongoing	Antonio Skarmeta	<a href="https://www.precept-project.eu/">https://www.precept-project.eu/</a>	<p>PRECEPT's ambition is to deliver the next generation of Smart Home (IoT) industry. The overall vision summarized as follows:</p> <ul style="list-style-type: none"> <li>• Transition to Pred(scr)iptive, Proactive Smart Residential Buildings</li> <li>• Self-managed “plug-n-play” PP-BMS together with federated learning AI algorithms</li> <li>• Combine edge-computing, security, and privacy</li> <li>• Introduction of Novel sustainable business models</li> </ul>
	Ongoing		<a href="https://www.sifis-home.eu/">https://www.sifis-home.eu/</a>	<p>SIFIS-Home aims at providing a secure-by-design and consistent software framework for improving resilience of Interconnected Smart Home Systems at all stack levels.</p>
SMART2B	Ongoing	Antonio Skarmeta	<a href="https://cordis.europa.eu/project/id/101023666">https://cordis.europa.eu/project/id/101023666</a>	<p>SMART2B will develop and deploy non-intrusive IoT sensors and actuators in existing buildings aiming to solve one of the main problems of improving buildings' indoor comfort and energy efficiency: the structural (physical and financial) limits of installing, monitoring, automating and control existing devices in buildings, by proposing plug &amp; play devices able to interact with the appliances and legacy equipment already installed and communicate the collected data to the cloud</p>



				for remote monitoring, data analysis based on AI and machine learning and control.
	Ongoing	Mikel Borrás	<a href="https://sphere-project.eu/">https://sphere-project.eu/</a>	The SPHERE cloud-ICT platform will allow to interact all different stakeholders during any phase of the asset with a building Digital Twin model of information of the building and a scalable set of different software tools, such as energy demand/performance simulation tools, Decision Support and Coaching Systems, BEMs or IoT enabled Predictive Maintenance Algorithms.
	Ongoing		<a href="https://www.synergyh2020.eu/h2020-initiatives/">https://www.synergyh2020.eu/h2020-initiatives/</a>	The EU-funded SYNERGY project will develop a Big Energy Data Platform (Big Energy Data Platform) and an online AI Analytics Marketplace (AI Analytics Marketplace).

## 9. Annex 2: Additional information provided by EU-funded project PHOENIX

Authorization and access control mechanisms are also conditioned by the IoT devices constraints. Lightweight technologies should be used to perform authorization mechanisms. Conventional access control models—i.e., Role-Based Access Control (RBAC), and Attributed Based Access Control (ABAC)— are not suitable to be used in these constrained scenarios. Thus, the S&P framework integrates novel technologies that enable distributed and scalable solutions by design, leveraging access control via authorization policies and distributed access control tokens (called Capability Token)— enabling their processing by constrained end-devices and ICT entities. The capability-based access control mechanism (DcapBAC) proposed in Hernández-Ramos et al. (2014) has been adopted in the S&P system, designed to take part in the authorization of heterogeneous entities in a distributed manner.

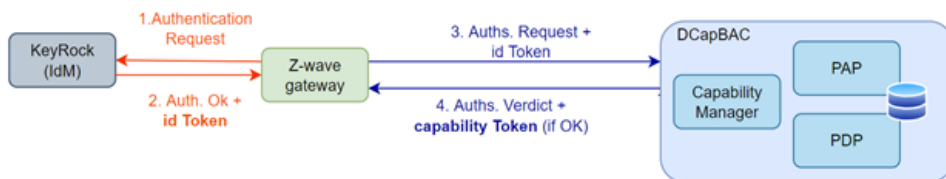
The S&P framework designed in PHOENIX provides novel mechanisms for enabling access to context data in a secure manner. First, after required login with credentials, the Identity Management component provides the identity token which verify the successful authentication. Then identity token is part of the request to Capability Manager which response with certain Capability Token. Finally, this token is used to request to PEP Proxy (Policy Enforcement Point Proxy) which will enforce authorization decisions.

A security components integration sample in PHOENIX is the Z-wave sensor gateway integration into PHOENIX Security & Privacy framework. The Z-wave gateway is in charge of receiving measured data from the Z-wave network and several sensors. So, the gateway process and format sensors data into a compliant PHOENIX data-model to later manage the creation and update of the sensor-related entities in the NGSI-LD broker of the architecture. Therefore, Z-wave gateway need to access that broker in a secure manner by authentication and authorization mechanisms leaded by PHOENIX Security & Privacy Framework.

The authentication and authorization mechanism is based on three main components:

- Identity Manager (KeyRock)
- Capability Manager: implements DcapBAC mechanism. Connects with:
  - Policy Administration Point (PAP): Responsible for managing the authorisation policies.
  - Policy Decision Point (PDP): Decides the verdict by checking the policies
- PEP-Proxy: Responsible for receiving the queries to access a resource.

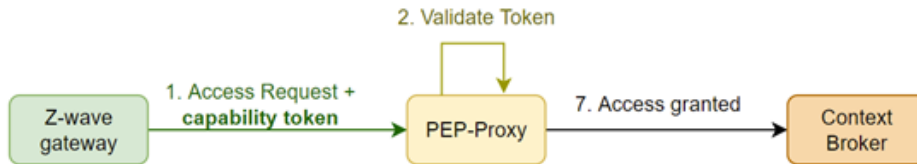
The Z-Wave gateway interacts with the components mentioned above in order to perform the authentication and authorization. First, Z-wave carries out the login-in process with the Identity Manager (KeyRock) and obtains the Identity Token. Then, Z-wave gateway uses the Identity Token as part of the request to Capability Manager, who examines the policies defined in the system and decides the verdict. So, if the verdict is successful, the Capability Manager responses to Z-wave gateway with Capability Token attached. This authentication and authorization process is described in Figure 12.



**Figure 12: Authentication and authorisation of Z-Wave gateway**

The Capability Token has a limited lifetime, therefore, the authentication and authorisation mechanism should be performed periodically in order to refresh the Capability Token and Identity Token. So, Z-wave gateway runs a software routine (which performs the process described in Figure 12) every 30 minutes to refresh his tokens to be able to access to Context Broker by PEP-Proxy.

Therefore, with a valid Capability Token, Z-wave Gateway creates and updates Context Broker Entities through PEP-Proxy. This token is attached in the authentication header of the request, providing a transparent communication with Context Broker. The access to Context Broker through PEP-Proxy is described in Figure 13.



**Figure 13: Access to Context Broker**