Marie Skłodowska-Curie Actions (MSCA)

Research and Innovation Staff Exchange (RISE)

H2020-MSCA-RISE-2017

Intelligence-Driven Urban Internet-of-Things Ecosystems for Circular, SAfe and IncLusive Smart CITIES

D3.2: Security Policy and Mechanisms for Security, Privacy and Trust

Abstract: This deliverable identifies and states the security, privacy and resilience challenges of a Smart City, how security-by-design can be achieved and developed as well as the approach for implementing it. The assessment process is then descriped, which aims to prioritize based on criticality and risk level all the challenges/threats/vulnerabilities related to a Smart City. Furthermore, the security and privacy mechanisms and requirements for Smart Cities and Internet of Things are identified, and the implementation process describes how these mechanisms are going to be applied and used in the Ideal-Cities platform. Moreover, the CRSP patterns are described along with their rules, and finally the Security Policy is stated.

Contractual Date of Delivery	31/12/2019
Actual Date of Delivery	31/12/2019
Deliverable Security Class	Public
Editor	Cablenet
Contributors	ALL

The *IDEAL-CITIES* consortium consists of:

FOUNDATION FOR RESEARCH AND TECHNOLOGY -HELLAS	FORTH	GR
ECOLE NATIONALE DES PONTS ET CHAUSSEES	ENPC	FR
BOURNEMOUTH UNIVERSITY	BU	UK
BLUESOFT SPOLKA Z OGRANICZONA ODPOWIEDZIALNOSCIA	BLS	PL
CABLENET COMMUNICATION SYSTEMS LTD	CBN	CY
NODAL POINT SYSTEMS	NPS	GR

This project is supported by the European Commission under the Horizon 2020 Program (2014-2020) with Grant agreement no: 778229

Document Revisions & Quality Assurance

Internal Reviewers

1. Andreas Miaoudakis (FORTH)
2. Othonas Soultatos (FORTH)
3. Aglaia Nicolaou (CBN)
4. Jakub Rola (BLS)
5. Christos Iraklis Tsatsoulis (NPS)
6. Vasilis Katos (BU)

Document History

Version	Date	By	Overview
0.1	29/07/2019	Aglaia Nicolaou (CBN)	Table of Contents
0.2	30/08/2019	Aglaia Nicolaou (CBN)	Table of Contents and contributors reassignment
0.3	06/09/2019	Othonas Soultatos (FORTH)	First Contribution (First Draft)
0.4	13/10/2019	Jakub Rola (BLS)	First Contribution (First Draft)
0.5	15/10/2019	Vasilis Katos (BU & ENPC)	First Contribution (First Draft)
0.6	21/10/2019	Christos Iraklis Tsatsoulis (NPS)	First Contribution (First Draft)
1.1	10/12/2019	Aglaia Nicolaou (CBN)	Second Contribution (Second Draft)
1.2	16/12/2019	Christos Iraklis Tsatsoulis (NPS)	Second Contribution (Second Draft)
1.3	16/12/2019	Jakub Rola (BLS)	Second Contribution (Second Draft)
1.4	16/12/2019	Vasilis Katos (BU & ENPC)	Second Contribution (Second Draft)
1.5	17/12/2019	Othonas Soultatos (FORTH)	Second Contribution (Second Draft)
2.1	20/12/2019	Vasilis Katos (BU & ENPC)	Third Condribution (Third Draft)
2.2	20/12/2019	Othonas Soultatos (FORTH)	Third Condribution (Third Draft)
2.3	23/12/2019	Aglaia Nicolaou (CBN)	Final Draft
2.4	27/12/2019	Othonas Soultatos (FORTH)	Fixing of Referneces

Table of Contents

1 Introduction

"Economies will be under increased pressure; energy consumption will increase exponentially; the environment will be challenged; healthcare and education systems will demand new approaches; public safety will be further challenged; and the potential for future cyberattacks against cities is high [1]."

The ultimate goal of a Smart City is to create a better world for human beings. The motivation is to optimize the use of public resources, increase the quality of services while decrease their operational costs [2]. The design, construction and maintenance of a smart city is done by using highly advanced integrated technologies. Such technologies include sensors, electronics,versatile wearable devices, and networks are connected with systems comprised of databases, tracking, and decision-making algorithms [3]. The main goal of the Smart City architecture is to implement in a structured way the information services needed for the monitoring of the critical infrastructures and for the organization of the Smart Cities databases [4].

Smart Cities consist of ubiquitous sensing, heterogeneous network infrastructure, and intelligent information processing and control systems [5], and can be used for different application categories such as, smart government (e.g. infrastructure, healthcare and utilities), smart economy (e.g. e-commerce), smart environment (e.g. energy, water, emission, and power grid), smart living (e.g. lifestyle, entertainment and home), smart citizens, and smart mobility (e.g. smart transportation) [6]. Manipulation of such urban operations will help in improving urban living quality in an intelligent and sustainable way [5].

Generating and analysing data and information from all these smart categories, will help the smart city to offer applications in areas such as infrastructure, sustainability, health, commerce, experience and cohesion such as traffic and congestion patterns applications, real time dashboards, gas emission monitoring and air pollution warnings, location specific noise levels and social or health problems in specific neighborhoods, investment maps for attracting new business, real time traffic analysis and school quality in specific neighborhoods respectively [6].

However, in order of a smart city to be considered as efficient, the use of the latest information and communication technologies (ICT), such as Internet of Things, Smartphone technology, Radio Frequency Identification System (RFID), Smart Meters, Semantic Web, Big Data, Connected Supply Chain, Artificial Intelligence, Cloud Computing, collective intelligence, Biometrics, etc., has to be considered [3].

Internet of Things is directly interrelated to Ideal (Smart) Cities. Internet of Things refers to the ability of smart objects to communicate, compute, and coordinate. The vision behind IoT is to create a world where smart objects are identifiable, interconnected by using the Internet technologies, and being able to communicate and interact with each other with as less as possible intervention of human. This means that objects around us will know what we like, what we want and what we need and act accordingly without explicit instructions [2].

The existence of a large network of interconnected smart objects, and the use of IoT for large-scale, and mission critical systems, will definitely pose security, privacy and trust threats and challenges which in turn will put the users of the smart city at high risk [7]. Generally, Smart Cities are exposed to a diverse set of cyber security threats and criminal misuses, a single one of which be exploited may put even the entire city at risk [8]. The fast and wider adoption of

IoT devices in our daily life, as well as the direct impact on users' lives, signifies the urgency of the identification and classification of the challenges, the use of proper security infrastructure and the addressing imposed challenges before deployment, so that to mitigate the all the types of challenges [7].

The two concepts have to be considered as one, and in combination with all the technologies that are used for the implementation of a Smart City, will be used for the identification of the security, privacy and resilience challenges, risks, and requirements as well as the controls in order to mitigate and implement them. This is an urgent necessity so that to be able to include privacy and security requirements into the architectural designs, and thus achieve security-by-design [4].

1.1 Security, Privacy and Resilience Challenges

IoT and participatory sensing based Smart City applications face a number of security, privacy and resilience challenges. They are vulnerable to security attacks (e.g. intruders, unauthorized access, disclosure, disruption, modification, inspect and annihilation) [6] and adverse operating context conditions that can compromise the availability, integrity, confidentiality, security and resilience of any of their components (e.g. local sensors, hardware/software components, network components, application level components, databases components, management system components, etc.)

They may also generate, make use of and inter-relate massive big data, including personal data, in ways that can potentially breach legal and privacy requirements. From such data, smart cities can extract very important information helping real time analysis and ubiquitous computing [3].

Furthermore, they can experience frequent and unpredicted changes in the components and infrastructures that they deploy, compromising the resilience and availability of the service(s) that they offer. Moreover, Smart City applications may face continuity challenges. A lot of interruptions might occur enexpectently. The design and architecture of the application has to be implemented in such a way so that continuity to be ensured and recovery controls to be available.

A lot of researches have been carried out during the last years, after Internet of Things and Smart or Ideal Cities concepts have been introduced, in regards to the different challenges that such applications are facing.

Although security, privacy and resilience have their own objectives, they are all of them somehow interconnected. In order for these challenges to be managed and controlled more easily, it would be more practical to be classified and divided into categories, based on the nature and the origin of each challenge [9].

1.1.1 Challenges based on Sector

Smart Buildings	Transport	Government	Healthcare	Energy	Financial
Infection by malware	Sending false emergency messages	Preventing of cybercrime	Modifying patients record or information	Spoofing addresses and user names	Loss of privacy

Systems failure	Disrupting a vehicle's braking system	Identity theft	Exposing sensitive data unintentionally	Unauthorized access and controls	Accounting fraud
Fraud by staff and unauthorized users	Stopping the vehicle's engine	Disrupting critical infrastructures	Disrupting the monitoring system	Zero day attacks	Disrupting business processes
Controlling the fire system	Triggering false displays in the vehicle's dashboard	Fiscal fraud	Disrupting the emergency services	Botnets	Accessing confidential company information
Causing physical damage such as flooding	Disrupting the vehicle's emergency response system	Altered files	Sending false information	Denial of Service (DoS) and Distributed Denial of Service (DDoS)	Accessing confidential customer information
Disrupting building temperature (overheating or overcooling)	Changing GPS signals		Jamming attacks		Damaging reputation(s)
Damaging or controlling the lifts			Sending an emergency alert		Defacing websites
Open windows and doors			Eavesdropping sensitive information		Financial and reputation concerns due to fraud and data leakage
Modifying smart meters					Denial of Service and DDoS
Opening parking gates					Phishing
Disabling water and electricity supplies					Mobile banking exploitation
Starting/Stopping the irrigation water system					SQL Injection
Stopping the renewable energy systems (RES)					Trojan

Table 1 Security Challenges based on Sector

1.1.2 Technological Challenges for virious technologies

The realization of smart cities relies on the exploitation of various technology enablers which introduce attack surfaces that increase the cyber-security related risks of the smart city infrastructure. Thus the usage of such devices pose new challenges for the city infrastructure.

- **RFID Tags** [3]**:** RFID Tags technology is vulnerable to security threats and attacks. This may include giving away sensitive information through unauthorized access, compromising data confidentiality and privacy, as well as data integrity due to information leakage.
    - **Abuse of tags:** Unauthorized users might illegaly use these tags. The Electronic Product Code (EPC), used for the communication between the RFID tag and RFID reader, might be sabotaged after the attacker collecting it. Additionally, another issue is detaching the tag.
    - **Tag killing:** An attacker might apply delete or kill commands and thus make the tag useless, or through physical destruction. This will result the reader not to be able to identify or read the tag. Denial of Service (DoS) attacks are mainly used for this purpose. Tag killing process can also be used for the enhancement of the security of the system by addressing privacy issues.
    - **Tag cloning:** This is the process where data from an original tag are copied and transferred to a new tag owned by an attacker.
    - **Threats to readers:** RFID reader sabotage is an attack where the attacker gets control of the RFID reader and thus be able to emit electromagnetic waves to destroy that data in the RFID tag.
    - **Threats to privacy:** Due to the uniqueness of the tag's Electronic Product Code (EPC), the RFID tag can be tracked by a hacker without the consent of users of a system. This results in the easy traceability and identification of the tags and thus in the leakage of private information and location of each user of the system.
    - **Signal Interference:** An attacker might induce signal interference in the communication of the RFID reader and RFID tag that will lead to issues of data integrity.
    - **Jamming**: The attempt to disturb the air interface and thus the communication between the RFID reader and tag. This attack can be performed by either powerful transmitters at a significant distance or passive means such as shielding.
    - **Threats to communication:** As the communication between the RFID tag and reader is performed through available wireless signals, threats such as searching, manipulating and jamming wireless signals are feasible. Attacks related to wireless communications can be characterized as active and passive, and mechanisms for ensuring the protection of the communication and the transmission have to be identified and applied, such as encryption and authentication. In addition, security concerns arise in the wired communication between the RFID readers and the middle-ware system, and thus, data confidentiality and integrity is important to be ensured.

- **Denial of Service (DoS):** The purpose of this threat is to disable and make the system useless. A radio signals broadcasting device can be used in order to disrupt or block the RFID reader functionality.
- **Spoofing:** Data included in a tag is duplicated and communicated to a reader. This attack is feasible and can occur especially when the RFID channel's security protocol used is revealed.
- **Software attacks:** The purpose of such attacks is to effect the RFID system functionality. Codded malicious programs that aim to infect and disturb the system making its performance slow or none, such as viruses, buffer overflows and worms, can used and injected in the system.
- **Cryptanalysis and Eavesdropping:** Cryptanalysis and eavesdropping attacks are the most frequent on a RFID system. Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them. The level of the cryptanalysis attack depends on the amount of information the attacker/analyst has about the cyphertext. The purpose of these attacks is to decipher encrypted information such as the ones stored in RFID systems. The attacks include man-in-the-middle attack, chosen plain text and chosen cipher-text attacks, and known plain-text and known cipher-text attacks. In the case of eavesdropping attacks, might occur during the communication of data to RFID readers. The attacker is catching data during the tag is read by the authorized reader, with a reader of the same tag family and frequency as the authorized one.
- **Traffic Analysis Attacks** [7]**:** Confidential information or other data flowing from RFID technologies can be sniffed out by an attacker because of their wireless characteristics. In most of the attacks, network information has to be gained in order to be employed. Such an attack can be done using sniffing applications such as port scanning, packet sniffer applications etc.
- **RFID Unauthorized access** [7]**:** As most of the RFID systems are lucking proper authentication mechanisms, anyone can access tags. This means that data on RFID nodes can be read, modified or deleted by an attacker.

- **Smart Grids** [3]**:** Devices used for communication purposes including sensors and communication networks which help in real time communication of data. When data are transmitted and communicated in a real-time manner, among for example, power generators, distributed resources, service providers and users, any information that is prone to attacks, that would take the system to failure.
  - **Threats to Network Availability:** Such attacks aim and attempt to delay, block or corrupt services by abusing information in the smart grid, eg. Denial-of-Service (DoS) attacks. As most of the smart grid use IP based protocols and as TCP/IP is open to this type of attacks, so smart grid faces a huge problem.
  - **Threats to Data Integrity:** Message injection, message replay, and message delay on a network are some of the means that can be used by a malicious attacker in order to modify information and thus affect the integrity of the

data used in the network. Data integrity threats may cause a lot of issues such as infrastructure and people of a smart city to be harmed, and this is because the main goal of such attacks and threats is the abuse of critical data in a smart grid, such as customer's information or network operation information. False data injection attack is the infusion of wrong data to the monitoring center of a power system and thus make the data integrity being questioned.

- **Threats to Information Privacy:** A lot of personal information of smart city users are captured through smart grid and are communicated in real time. Privacy concerns have to be examined and assessed and controls should be applied in order to ensure the privacy rights of the smart city's users.
- **Threats to Devices:** Smart grid devices are vulnerable to physical threats and attacks such as battery change, removal, and modification.

- **Biometrics** [3]**:** The automated recognition of an individual based on unique bahavioral, physiological and biological characteristics. Such characteristics can be acquired by proper applied sensors and distinctive features used to get a biometric template for authentication purposes. Although biometrics can be used in solving different security issues in smart cities, they can propose a lot of threats and vulnerabilities if proper controls are not in place. Especially, threats related to privacy as such characteristics used for recognition and authentication are considered as personal and sensitive data.
- **Smartphones** [3]**:** Smartphones are used for accessing various services and applications that help in maintaining and developing a better smart city, and as the main source of people's role, and that's why they are one of the core components of an IoT infrastructure in a Smart city.
  - **Malicious smart applications:** Hackers implement and upload to application marketplaces malicious smart applications that can infect smart phone devices and thus make them vulnerable to security and information privacy threats.
  - **Botnets:** A botnet is a network of multiple devices that were infected by malware spread by an attacker, either through email attachments, or smart applications, or malicious websites.
  - **Spyware:** The malicious use of a spyware in order to hijack a smart-phone. The attacker will be able to locate and hear calls, check messages and emails, and truck user's location through GPS updates.
  - **Threats from Bluetooth:** A threat related to Bluetooth could be the fact that wireless devices show their existence and permit unrequested connections, and the fact that there are end users who do not know how to manage and configure their settings properly.
  - **Location and GPS:** The attackers can sabotage the location privacy of individuals by various attempts on the GPS feature of smart phones.
  - **Threats through Wi-Fi:** Information can be catched during the communication between smartphones and Wi-Fi hotspots by an attacker.

The main vulnerability is this type of threats is that the Wifi hotspot architecture is designed in such a way where the transmitted data are not protected with encryption.

- **Threats in social networks:** Links on social networking websites and applications may spread effectively malicious malware. In addition, privacy of individuals might be compromised through social media.

- **M2M Communifcation** [3]**:** In order for a smart city to be a reality, Machine to Machine (M2M) communication is needed. Machine to machine protocols are used for fixing the communication between at least two nodes of a network based on the rules of engagement established. IPv6 protocol plays a critical role in such communications as it fulfils all the requirements of portability, and thus helps different systems work together. The criticality and the importance of such communication type in a smart city, introduces a lot of security concerns:
  - **Physical Attacks:** These attacks include the use of modified software for fraud purposes, and thus breach the integrity of data and M2M software.
  - **Attacks on authentication tokens:** The threats include physical and side-channel attacks on authentication tokens, as well as the cloning of the tokens for malicious purposes.
  - **Configuration Attacks:** Software configuration changes through updates with malicious intentions that might lead to fraud, or misconfiguration by the user.
  - **Protocol Attacks:** Protocol attacks are attacks such as man-in-the-middle, DoS, and attacks on OAM and its traffic, which are attacks mainly designed against the devices.
  - **Threats in network security:** The main target of such attacks is mobile network. Examples are, device impersonation and traffic tunnelling between them. Additionally, a serious network security breach is also the misconfiguration of the devices firewall, as well as DoS attacks.
  - **Breaches in privacy:** the ways that data are collected, mined and provisioned in a smart city is totally different from the ones already known, and the amount of occasions where personal data can be collected is huge. Moreover, eavesdropping can cause major concerns over individual privacy and data integrity. Additionally, masquerading as other user's devices is another security problem that has to be considered and mitigated.
- Wireless Sensor Network (WSN) [3]
  - **Attack on data confidentiality:** During the processes of sending and receiving information, data confidentiality on a WSN might be compromised by various crypt-analysis attacks.
  - **Threats to data integrity:** Various types of attacks can be used in order to abuse, change, and modify data.
  - **Misuse of resources:** The misuse of IoT devices in a smart city for malicious purposes.

  - **Bandwidth degradation:** Information flow can be affected by bandwidth degradation and prone to abuse of data.
  - **Battery or resource exhaustion:** Infection of IoT devices with malicious attacks, compromising their battery life and resources by making them poor.
  - **Unauthorized Access:** WSN resources unauthorized access by an attacker in order to obtain the keys for malicious purposes.
  - **Threats to Authentication:** The attacker could overcome the authentication process and gain access to WSN, by holding the user id and password and thus get hold of all the services provided by the WSN.
  - **DoS:** The services of the whole WSN system can be suspended by a Denial-of-Service attack.

- **Building Automation Systems (BAS)** [8]**:** A Building Automation System (BAS), is an intelligent system consisting of both hardware and software, the role of which is to connect systems such as heating, venting, airconditioning, lighting, security and other included in a building, so that to communicate on a single platform. This makes the BAS able to deliver crusial information abouth the operational performance of a building as well as enhancing the safety and comfort of the occupants. In a smart city, BAS is connected to shared networks, and thus it is exposed to threats such as the ones faced by IT based networks and protocols. Building services are exposed to DoS attacks making it possible for an attacker to take over the complete building control or the access control system, due to the resource constraints of BAS devices. Moreover, BAS protocols are inherently insecure due to the amount of trust they give to sensors and controllers. Generally, source authentication does not exist in BAS protocols, as devices are considered truthful about what they do, and thus limited verification ability is available. Moreover, because of the increased connectivity, BAS can be used as a pivot point into the Cloud to carry out ICT attacks, such as data theft and exfiltration.
- **Unmanned aerial vehicles (UAVs)** [8]**:** Unmanned aerial vehicles such as drones, use an unsecured Wi-Fi connection between a smart device and the onboard system to control flight. A privileged user account (root) is used in the onboard system with Telnet openly accessible and FTP services available for interaction. Drones are mainly faced communication and device level cyber threats. Based on studies performed in civilian drones, they do not employ cryptographic techniques to secure communications between controllers and drones, as well as the employed methods for restricted communications to single controllers are easily defeated. Such drones can be susceptible to remote hijacking, connection denial, video interception and total control takeover by adversaries. Given that they operate at root or equivalent permissions and access rights on the system by default, and in combination with the above mentioned threats, when a malicious adversary managesto establish connection with the drone, then full control of the device is available, with no requirement for commitment of further resources in order to escalate privilege. Furthermore, drone controller has the potential of being vulnerable and a possible attack target. This depends on the type of the controller. For example, a drone controller can be a mobile device, or operated

through cloud platforms, so threats related to these technical characteristics can be exploited against it.

- **Smart Vehicles** [8]**:** Most of the security challenges that smart vehicles face, are the ones faced by isolated networks that are now externally connected.
    - **Physical Threats:** Fault-injection into the Engine Control Unit to defeat central locking systems, side channel attacks to leak information, or introducing data glitches to gain unauthorized access to debug interfaces.
    - **Interception Threats:** Man in the middle, reconnaissance, replay attacks can be exploited to either the data transmitted over the networks, or internally between the engine control units, or between vehicles and the cloud.
    - **Abuse Threats:** Traditional ICT attacks, e.g. Denial of Service, malicious code execution, unauthorized access to the vehicle, remote execution and operation of the vehicle, etc.
    - **Malicious Code:** Nowadays, more and more vehicles include integrated infotainment systems which most of the times run embedded versions of different types of operating systems such as Linux, Windows, or Android. Malicious code could be executed against Vehicles Infotainment Systems having as goal to compromise all the devices connected to the smart vehicle and potentially leak into the cloud.
    - **Data Threats:** Threats against the information contained in the smart vehicle networks, or loss of information through connected cloud, or leakage of personal and confidential information in case the vehicle is resold.
- **IoT Sensors** [8]**:** Smart cities are directly related and interconnected with IoT devices and sensors. This means, that IoT sensors challenges have to be consider while identifying challenges for smart cities.
    - **Confidentiality and Integrity Compromise:** Access rights should be assigned based on the least-privilege principle, in order to ensure that only authorized personnel have access to both sensors collecting data and sensor data stored, and that the integrity of the data is susceptible to compromise by unauthorised parties. Privacy is an other issue, as personal identifiable information and sensor data could be exposed. Thus, confidentiality of data should be maintained.
    - **Eavesdropping:** Communication between the sensor and the centralized server should be enough secure so that integrity of data not to be compromised by eavesdropping attacks. Interception of communications especially during the transmission of data, could result to incorrect sensor actions and the recording of incorrect events by the servers.
    - **Data loss:** Data management including deployment practices, procedures and policies for effective and secure sensor utilization, if insufficient then the smart city operations might be impacted, or if not adequate, the compromising of sensor data collected, transmitted or stored will be possible.

- **Availability compromise:** Procedures and plans should be in place in case of sensor unavailability or failure, so that to avoid negative impact of the smart city's operations.
- **Remote exploitation:** Remote exploitations could be performed to insecure communication channels between sensors and servers. Such exploitations could be launched from the main servers, connecting nodes, or even an individual sensor and potentially propagate through the network.
- **Sinkhole Attack** [7]**:** The traffic of IoT nodes, typicaly transmited over WSN, is lured by the attacker and hence a metaphorical sinkhole is created. Breach of data confidentiality and denial of service of the network by dropping instead of forwarding the packets to the desired destination, might be the results of such an attack.
- **Man-in-the-middle attack** [7]**:** The attacker tries to exploit a vulnerability against the network communication protocols used in an IoT system in order to interfere between two sensor nodes, gain access to restricted data, and gain the ability to monitor, eavesdrop and control two sensor nodes communication with the intention to violate the privacy of the two sensor nodes.
- **Routing Information Attacks** [7]**:** The main goal of such direct attacks is to complicate the network and creat routing loops, and thus be able to allow or drop traffic, send false error messages, make source routes to be shortened or extended, or perform partition of network. This can be done by spoofing, altering or replaying routing information.
- **Sybil Attack** [7]**:** A Sybil or malicious node is a node that claims the identities of a larger number of nodes, so that to be able to impersonate them. This leads to the neighboring WSN nodes to accept false information.

- The Cloud [8]
  - **Data leakage:** When moving to the cloud, either infrastructure or resources, control over data is given to the cloud provider (third party). As cloud is a multitenant environment, and data are hosted there, then they can potentially be accessed by a malicious adversary or by the third party.
  - **Insecure APIs:** Interaction between software and application with the cloud services is done through APIs. Communication with APIs must be secure, and issues related to authentication, access control, encruption, activity logging and monitoring mechanisms must be addressed.
  - **Malicious Insider Threats:** An insider might be an employee of the cloud provider. The procedure followed by the cloud provider for screening and clearance most of the times is not revealed as well as how the cloud provider is granting access to the resources of the client organization.
  - **Denial of Service Attacks (DoS):** The fact that the services are hosted by a third party on the Cloud, makes it easy for an adversary to extract information about the infrastructure of a smart city, as its hosted publicly making data publicly accessible.

  - **Malware Injection:** Web applications are hosted by cloud providers via middleware platforms. In case that the web applications or servers are not configured or patched on a secure manner, then an adversary can leverage this, and carry out various malicious scripting-style attacks.
  - **System and Application Vulnerabilities:** As the technology and applications of the smart city are managed by the cloud provider, and no control in regards of management and security is given to smart city, then the cloud provider has to be selected carefully and based on critiria and requirements so that to be trusted that the services will be offered are going to be robust and secure.
  - **Data Locations and Regulation Boundaries:** The choise on where the data of a smart city are going to be stored is not the case.

- **Supply Chains** [9]**:** An attacker, a determined aggressor, identifies the weakest link between a network of organizations (supply chain), in regards of cybersecurity, which most probably is the smallest organization within the supply chain. Such organizations they luck of cybersecurity arrangements because of the limited resources. The attacker uses the vulnerabilities of the small organizations in order to gain access to the systems of other members of the supply chain. In this case, Advanced Persistent Threats (APTs) can be used.
- **Big Data** [9]**:** Big data storage is a big challenge in IoT systems and Smart cities. As real-time response to different situations is very crusial, data processing and analysis is very critical in order to achieve this. Thus, acynchronization of temporal or spatial information could result in big challenges in regards of data analysis. Accurate and timely decision making in data mining is tremendous. Collection of data by sensors, relay of collected information by communication units, analysis of information by computing units, and service layers take action, and summarized each layer's challenges. Vulnerabilities and challenges of the IoT infrastructure could result from these four layers. Data could be stolen by attackers from any point in the IoT data network.
- **Industry Control Systems** [9]**:** This type of challenges may result in serious implications in regards of security. This is due to the fact that the attack threat moves from manipulating information to controlling actuation. In addition, the threat is expanded to threats against new devices, protocols and work-flows.
- Software Attacks [7]
  - **Phishing Attacks:** The authentication credentials of a user are spoofed by an attacker, either through infected emails or phishing websites, so that to gain access to confidential data.
  - **Virus, Worms, Trojan Horse, Spyware and Adware:** A system can be infected by a malicious software with results such as stealing of information, tampering of data or denial of service.
  - **Malicious Scripts:** Complete system shut down or data theft can be achieved by fooling the gateway connecting the IoT system to the Internet, and run active-x scripts.

  - **Denial of Service (DoS):** A DoS or DDoS attack can be executed by an attacker through the application layer, making the IoT network and users affected. Users could be blocked, even if legitimate, from the application layer (databases and private sensitive data), however the attacker will gain full access.

- Encryption Attacks [7]
  - **Side channel attack:** Different techniques can be used by an attacker against the encryption devices of an IoT system, and thus be able to retrieve the encryption key.
  - **Cryptanalysis attacks:** This kind of attack assume the possession of cipher text or plaintext and the purpose behind it is to break the encryption scheme of the system and find out which is the encryption key used. Such attacks could be known-plaintext attack, chosen-plaintext attack, chosen cipher text attack, or cipher text-only attack.
  - **Man in the Middle attack:** An adversary is positioned between the communication lines of two users of the IoT system, established in order to exchange encryption keys making the communication channel more secure. The attacker intercepts the signals send between the users and performs a key exchange with each user separately so that to achieve interference. Then the malicious attacker will be able to decrypt or encrypt any data received by the two users with the keys he shares with both of them and thus the two users will think that they are talking to each other.

1.1.3 Physical Challenges [7]

- **Node Tampering:** Damage to the sensor node can be caused by an attacker, by either physically replacing it entirely or part of its hardware, or gain access to the nodes through electronic interrogation and thus be able to alter sensitive information (e.g. shared cryptographic keys or routing tables, or impact the operation of higher communication layers).
- **RF Interference on RFIDs:** Noise signals can be created and send to any RFID tag over Radio Frequency signals used for communication. This will result in the implementation of a Denial of Service attack.
- **Node Jamming in WSNs:** The attacker can interfere with the radio frequencies of the wireless sensor nodes, jamming the signals and denying communication to the nodes. If the jamming of key sensor nodes is successful, then the denial of IoT service will be possible.
- **Malicious Node Injection:** A malicious node to be physically deployed and injected between two or more nodes of the IoT system, and thus the data flow from and to the nodes as well as their operation to be controlled by the malicious node (Man-in-the-middle attack).
- **Physical Damage:** The IoT network devices can be physically damaged by adversaries. This attack is directly related with the security of the area or the building that the IoT system is hosted. In this case the adversary tries to damage directly the IoT system with the purpose of service availability impact.

- **Social Engineering:** The users of an IoT system are manipulated by an attacker in order to extract private information or perform certain actions in general so that to reach his goal. In order for an attacker to perform such an attack, he has to interact physically with the IoT network users.
- ***Sleep Deprivation Attack:*** *Replaceable batteries are used for powering sensor nodes in an IoT system, which are programmed t2o follow sleep routines in order to extend their battery life. Performing a sleep deprivation attack to a sensor node will keep it awake, leading to additional power consumption and thus the node will shut down.*
- **Malicious Code Injection:** Malicious code is injected to a node physically by an attacker, which results in the compromise of the node and thus the attacker is given access to the IoT system (e.g. malicious USB stick inserted onto the node). Full control of the node or of the whole system will be gained by the attacker if this attack is exploited.

1.1.4 Governance Challenges [3]

- **Need of security testing:** Usually, the main testing that firms and organizations require to be performed is testing of the functionality of the technology. Awareness in regards of the security testing has to be a key requirement especially in governance authorities (utility, health, infrastructure, education, transport, etc.)
- **Threats to critical infrastructures:** Critical infrastructures are considered the areas where critical services are executed and offered, and if a change happens to a single process then delays or loss of service might be caused. Such critical infrastructures are healthcare, industry and telecommunication. IoT and smart grids are the main technologies used for the implementation of critical infrastructures. Thus, the threats related to these two technologies have to be considered. In addition, the proper storage, management and protection of the big data generated by critical systems have to be considered so that to ensure security, data integrity and resilience. The integrity, availability and confidentiality of critical infrastructure may be compromised due to malicious attacks, and thus crucial damage may be caused to smart city promised services.
- **Smart mobility security and privacy requirements:** During the collection, publication and utilization of trace data in smart mobility, disclosure of personal information may happen which may cause privacy concerns. The sending and receiving of information between devices used in smart mobility infrastructure may be subject to malicious attacks which may cause wrong traffic reports in satellite navigation systems.
- **Energy and utility optimization:** Energy and utility services, in order to manage the distributed energy efficiently, they rely on smart grids that use bidirectional communication with the users. A proper strategy should be made in regards of saving of energy and utilities from frauds and malicious attacks, so that concerns related to data security and privacy as well as cloud computing to be considered and controlled.

1.1.5 Social/Economic Challenges [3]

- **Challenges in smart communication:** As part of the critical infrastructures consisting a smart city, telecommunication sector is considered as vulnerable to various malicious attacks, viruses, frauds and privacy attacks. Threats related to

Machine to Machine (M2M) communications should be taken under consideration. Privacy and Information Security threats might be arised in technologies such as wireless networking, Bluetooth, cloud computing, IoT and other ICT technologies that are part in smart communication.

- **Individual Privacy:** Privacy and Information Security concerns related to social networking have to be considered. Such concerns, are directly dependent on the level of identification of the provided information by an individual, the receivers and the way the information may be used.
- **Banking, finance and business:** Attacks performed for personal financial use is one of the reasons that this component of a smart city is considered as vulnerable to security threats. The attackers may also intend to sabotage the economy of certain organization, or a whole city.

1.1.6 Data Privacy and Trust Challenges

- Secure Authentication and Access Control in Constrained Devices [5]
- Privacy Leakage in Data Sensing [5]
- Security issues in Collecting and Transferring Data [6]
- Privacy and Availability in Data Storage and Processing [5]
- Security issues in Smart Mobility [6]
- Privacy-preserving Sharing of IoT Data [10]
- Trustworthy and Dependable Control [5]

1.1.7 Security, Privacy and Resilience Challenges for 5G Networks

As 5G Networks are currently during their implementation and application phase, information and cyber security challenges related to 5G have to be identified and controls have to be implemented by design, so that to eliminate the risks in the future. Some of the challenges expected are:

- Increased exposure to attacks and more potential entry points for attackers [11]
- Certain pieces of network equipment or functions are becoming more sensitive [11]
- Reliance of Mobile Network Operators on Suppliers [11]
- The risk profile of individual suppliers [11]
- Increased risks from major dependencies on suppliers [11]
- Threats to availability and integrity of networks will become major security concerns [11]

Countermeasures for all the security challenges that 5G Network Technology will bring to Smart Cities and IoT Infrastructure have to be identified and implemented.

1.2 Resilience, Security and Privacy by design

An emerging approach to securing applications, known as “security-by-design”, aims to guarantee system-wide security properties by virtue of the design of software systems and properties of the components used in these systems. A key capability required in security-by-design is the ability to verify the desired security properties as part of the design process.

Security-by-design is central to IDEAL-CITIES. Our aim is to support the design of IoTPS applications assisted with Big Data and Cloud Services that can operate in a secure manner based on patterns that describe horizontal and vertical compositional structures of such applications with proven relations between system wide and component level CRSP properties. These patterns will set necessary and sufficient conditions for composing different components within IoTPS applications in ways that guarantee said CRSP properties.

1.3 Develop the Security-by-design concept

Security of the applications is the everlasting process. It starts by understating the requirements of the application. Based on the specific requirement, potential risks are and the consequences of an attack need to be assessed followed by definition of the security concept and approach. The next phase would be designing the architecture of the security and the verification and monitoring approach. Once all the latter steps are fulfilled, the implementation and development phase starts. Once finished, the last and the longest subprocess of security is constant monitoring and response to any security threats. If the attack would succeed, the security team must have all the necessary tools to be able to implement solutions that will prevent the same accidents in the future.

Security by Design (SbD) is not a specific technology, but a systematic approach to achieving security assurance; as such, it affects design approach, technologies, processes, etc. Within IDEAL-CITIES project we have the ambition to implement such concept in order to consider security from the earliest stages of the project, throughout the research and development process, during the operation of the system and until its end of life. Thus, security is not an afterthought, but a key consideration in every phase, is built into the end product, and the desired security attitude and approach is planned, executed and maintained. This is recognised (and proven in practice) to be the most effective and efficient way to address the security concerns in any environment.

- **Phase 1 – Requirements**
    - Identify assets & possible attackers
    - Conduct threat/risk assessment
    - Define security requirements & means of validation
- **Phase 2 – Design**
    - Design security architecture & associated security components/mechanisms
    - Attack surface reduction, defence in-depth, principle of least privilege etc.
- **Phase 3 – Implementation**
    - Implement security components/mechanisms (e.g. AAA, secure interfaces)
    - Follow secure coding practices, incl. security code analysis/review
- **Phase 4 – Testing**
    - Validate coverage of security requirements
    - Security assessment
    - Dynamic analysis, penetration testing etc.
- **Phase 5 – Deployment/Operation**

- Continuous monitoring
- Incident response & auditing
- Continuous improvement / feedback loop

1.3.1 5 phase of building the platform

This chapter describes our approach to building the Ideal Cities platform. First, we present the generic approach and then we describe the take action during Ideal Cities platform development.

- Phase 1 – Requirements
  - Identify asset & possible attackers
  - Conduct threat/risk assessment
  - Define security requirements & means of validation

D2.2: Risk Analysis, User, Trust and Reputation models for Smart Cities

- Phase 2 – Design
  - Design security architecture & associated security components/mechanisms
  - Attack surface reduction, defense-in-depth, the principle of least privilege, etc.

D3.1: IoT Cloud infrastructure and location sensing in urban environments

- Phase 3 – Development
  - Implement security components/mechanisms (e.g. AAA, secure interfaces)
  - Follow secure coding practices, incl. security code analysis/review
- Phase 4 – Testing
  - Validate coverage of security requirements
  - Security assessment
  - Dynamic analysis, penetration testing, etc.
- Phase 5 – Deployment/Operation
  - Continuous monitoring
  - Incident response & auditing
  - Continuous improvement/feedback look

1.3.1.1 *Phase 1 – Requirements*

In the context of the first phase, Requirements, the following tasks were performed:

D2.2: Risk Analysis, User, Trust and Reputation models for Smart Cities

1.3.1.2 *Phase 2 – Design*

In the context of Phase 2 (Design), the IDEAL-CITIES efforts included:D3.1: IoT Cloud infrastructure and location-sensing in urban environments

1.3.1.3 *Phase 3 – Development*

In the current active phase, as of the time of writing this document, i.e. Phase 3 (Development), the following tasks are underway:

The development of all security elements, as defined in architecture during phase 2. Security code review and static analysis of the developed code is performed in the context of the developer's efforts and reviewed per release cycle.

1.3.1.4 *Phase 4 – Testing*

In the upcoming phase, i.e. Phase 4 (Testing), the following tasks are scheduled to take place:

- Validate/verify coverage of security requirements
- Configuration review (for services/functions and network).
- Penetration testing / dynamic analysis of delivered implementation prior to final release.

It should be mentioned that considering IDEAL-CITIES's development process, part of the Testing is already underway, in parallel with the integration tasks, while other aspects of this phase.

1.3.1.5 *Phase 5 – Deployment/Operation*

This last phase in the lifecycle, i.e. the deployment/operation, is partly out of scope for IDEAL-CITIES as it mostly refers to the day-to-day operation of the framework in the production environment.

1.3.2 Security principles

During the development process, we will follow, described below, security principles, which are based on the OWASP Development Guide [12]. Those rules will help us to develop more resistant to attacks platform.

1.3.2.1 *Minimize attack surface*

Every new part of the application generates some amount of potential risk. The goal of secure development is to reduce the risk by reducing potentially vulnerable points.

For example, the application can implement the search option by inputting text by the user. It allows the SQL injection attack. The sanitization of input is a good idea but the redesigning (better UI) the search mechanism without input box almost eliminates such a weak point.

1.3.2.2 *Establish secure defaults*

By default, the security setting should be set to the height possible restriction (password aging and complexity should be enabled). Only the privileged user should be able to trim the restrictions down.

1.3.2.3 *Principle of Least privilege*

This principle recommends that accounts have only these privileges which are required for their tasks.

For example, if a client can only get data from the specified table in the database and write into the log, it can only access too those resources (read from a table and write into a log). There cannot be any circumstances that this client has administrative privileges.

1.3.2.4 *Principle of Defense in depth*

The idea behind defense in depth is to manage risk with diverse defensive strategies so that if one layer of defense turns out to be inadequate, another layer of defense will hopefully prevent an attack. Controls, when used in depth, can make severe vulnerabilities extraordinarily difficult to exploit and thus unlikely to occur.

1.3.2.5 *Don`t trust services*

This principle recommends security verification of the externally provided services because we have no visibility over the control and security of third-party providers.

1.3.2.6 *Separation of duties*

The basic fraud control method is a separation of duties. For example, the administrator should have the privilege of restarting system, sets password policy but should not be granted super users privileges that can change crucial data of an application.

1.3.2.7 *Keep security simple*

Use simple and straightforward solutions over complex approaches. Developers should avoid the use of double negatives and complex architectures when there is a simpler alternative.

1.3.2.8 *Fix security issues correctly*

If the security issue would be found or the attack would succeed, it is important to understand the root cause of the issue. When design patterns are used, it is likely that the security issue is widespread amongst all codebases, so developing the right fix without introducing regressions is essential.

1.3.3 Certification and legal issues

The legal obligation has to be taken into consideration when designing security. Most of the legal issues are base on some kind of certification which may be obligate for the user of Ideal-Cities platform. In this stage of the project, it is hard to select the specific certifications that we will fulfill but it has to be taken into consideration.

1.4 Approach

As the Ideal-Cities platform is going to be implemented, security and privacy standards and regulations need to be considered in order to ensure the security, privacy and resilience of the platform. The following standards may be applied:

- ISO/IEC 27001:2013 – Information technology – Security techniques - Information Security Management Systems – Requirements
- ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls
- ISO/IEC 27032:2012 – Information technology – Security techniques – Guidelines for cybersecurity
- General Data Protection Regulation (GDPR), 2018
- ISO/IEC 27701 – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
- ISO/IEC 22301:2012 – Societal security – Business continuity management systems – Requirements

- ISO/DIS 22313:2012 – Societal security – Business continuity management systems – Guidance
- ISO/IEC 45001:2018 – Occupational health and safety management systems – Requirements with guidance for use
- Network and Information Security (NIS) Directive

2 Assessment

During the Assessment process, risk-based thinking is essential in order to achieve effective identification and assessment of the threats, vulnerabilities and risks related to all the aspects of smart cities. The assessment process has to establish and maintain risk criteria, including risk acceptance criteria and criteria for performing risk assessments, and to ensure that repeated risk assessments produce consistent, valid and comparable results. Moreover, the risk assessment process has to identify security risks related to the loss of confidentiality, integrity and availability of information falling within the scope of smart cities, and identify the risk owners. In addition, the process has to analyse the security risks and this means, assessing the potential consequences that would result if the risks identified were to materialize, assessing the realistic likelihood of the orccurence of the risks identified, and determining the levels of risks. Finally the assessment process has to evaluate the risks, and compare the results of risk analysis with the risk criteria establishes, and prioritize the analyzed risks for risk treatment.

After the assessment process, the risk treatment process of the risks previously assessed has to be defined and applied. This process includes the selection of appropriate risk treatment options, taking into account the risk assessment results, and determine all the controls that are necessary to be implemented based on the treatment option selected. Furthermore, comparison of the controls determined with the ones suggested by the framework used or with best practices, so that to verify that no necessary controls have been omitted. Then, Statement of Applicability has to be produced, which contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls. Finally, the risk treatment plan has to be formulated and risk owners have to approve the treatment plan and accept the residual risks.

2.1 Security

The security assessment process that needs to be followed in order to identify all the risks, threats, vulnerabilities and data protection impacts that might be phased during the implementation of the Ideal-Cities platform as well as the application of smart city in our daily life, is the same with the assessment process described above. In this case, only information and cyber security challenges and risks have to be identified, as well as risks related to confidential, and/or personal data protection.

2.1.1 Information Security & Cyber Security

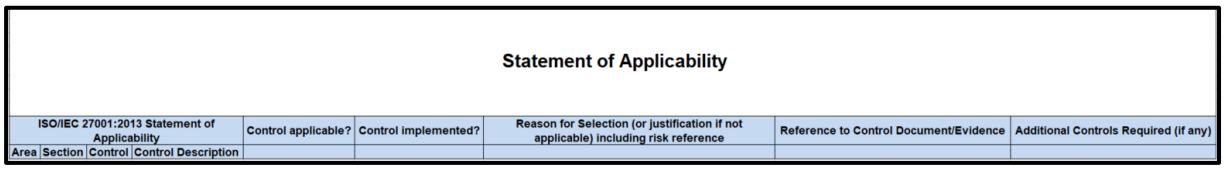
A. Statement of Applicability

The Statement of Applicability describes the controls that are applicable in the smart cities concept in regards of information and cyber security, data protection and other aspects e.g. health and safety, quality, business continuity etc. This Statement of Applicability has to be completed after the identification of assets, risk assessment and treatment process.

A Statement of Applicability template is shown in Figure 1.

B. Information Asset Inventory

Information Asset Inventory is the process confirming the existence, location, and condition of assets. All the assets related to the Ideal-Cities platform need to be identified and listed in the Information Asset Inventory by all partners.



Statement of Applicability

ISO/IEC 27001:2013 Statement of Applicability				Control applicable?	Control implemented?	Reason for Selection (or justification if not applicable) including risk reference	Reference to Control Document/Evidence	Additional Controls Required (if any)
Area	Section	Control	Control Description					

Figure 1 Statement of Applicablility template

In the information asset inventory have to be included all assets associated with information and information processing facilities, as well as assets identified in the lifecycle of information. The lifecycle of information includes creation, processing, storage, transmission, deletion and destruction.

For each asset, the following information has to be defined:

Asset name: The name of the asset

Asset type: Assets are divided into the following types - information, hardware, software, physical, services, people. Examples of each type are:

Information	Hardware	Software	Physical	Services	People
Database & Data files	Computers	Application Software	Contracts	Heating	Staff
Procedures	Servers	System Software	Confidentiality Aggreements	Lighting	Customers
Training Materials	Networking equipment	Test Data & Algorithms	Data Protection Aggrements	Poer	Subscribers
Statutory & Regulatory Specifications	Sensors	Case Tools	Building & property	Water	Extenal Providers
Contracts	IoT devices	Email	Intellectual property	Network	Suppliers
Confidentiality Agreements	Any tangible asset	Accounting	Server/Data rooms	Telephone	Contractors
Records		Intranet	Machinery & Equipment	Postal	Owner/Chief Executive

System Documentation		Website	IT Equipment	Banking	Managers
Software (physical or virtual)		Office applications	Stock (supplies and materials)	Cleaning	Engineers
Applications (physical or virtual)		Industry-specific applications	Vehicles	Gas supply	Knowledge Holders
Operating Systems (physical or virtual)				Network services	
Supplier contract details					
Risk assessments					

Table 2 Asset Types' Examples

Description: Define what this asset is and what information and data it contains

Purpose: Define the purpose this asset is used for

Owner: This is usually the person or group responsible for the operation of the asset. However, occasionally, the ownership and operation of an asset might be assigned to different persons, where the owner owns them but the custodian operates or maintains them. In this case, we are interested for the owner and thus, person responsible for the asset.

Value (low, medium, high): The value of the asset based on its purpose

Personal data (Y/N): Define whether the asset includes any information relates to an identified or identifiable natural person (personal data) or not

Information classification (public, protected, restricted, confidential, sensitive): Classifiction of information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. The levels of classification implicitly dictate that information in different levels, should be handled somewhat differently.

Confidential: Significant, unwarranted breach of a person's privacy, which more likely than not would cause substantial harm. This will certainly include information that the GDPR defines as sensitive personal data. Sensitive personal data is information that concerns an individual's such as Racial or ethnic origins, Political opinions, Religious beliefs or beliefs of a similar nature, Physical or mental health condition, Sex life, Involvement in any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings, Outcomes of criminal convictions or Substantial risk to the health, safety and wellbeing of individuals or groups or Prejudicing the prevention or detection of a crime, or the apprehension and prosecution of an offender or the company being exposed to a civil claim for breach of confidence or Information protected by legal professional privilege, including legal advice privilege and litigation privilege or significant financial loss. E.g. Accident reports, medical information, bank / credit card

details, communications with regulator / legal / police etc., disciplinary proceedings, passwords and other forms of access control credentials.

Restricted: Information that if subject to unauthorized disclosure, dissemination or loss could result in:

a) An unwarranted breach of a person's privacy, which more likely than not would cause a level of harm and/or inconvenience. This will certainly include information that the GDPR defines as personal data. Personal data is information that identifies a living individual and relates to them in a significant biographical sense.

b) Disruption to day-to-day operations of the company, where disruption only affects a department of the company.

c) Damage to commercial relationships.

d) Loss of competitive advantage. E.g. Commercial contracts, contracts of employment, disaster recovery / business continuity plans, payroll / banking details, planning / forecasting reports, procurement / initiation to tender documentation, strategic planning, company risk register and controls.

Protected: Information that would only be made available to a person once they became an employee of the company if needed. The information would not be released into the public domain. E.g. Budget information, draft documents, internal audit reports, key performance indicators, minutes of meetings, employees' contact details.

Public: Information that can be disclosed or disseminated without any restriction on content, audience, time of publication. Disclosure or dissemination would not breach any relevant laws (notably privacy) or a duty of confidence. E.g. Information published in the company's web site.

Location: The asset's location needs to be specified so that its existence may be verified.

Data retention period: Based on laws, regulatory requirements, statutory obligations, organization's policies, contractual agreements etc. each asset has to have a specified retention period, starting to count from the date of acquisition.

Date of acquisition: The date an asset has been acquired.

Status (live, retired, deleted): Live – The asset is still in use, Retired – The asset is permanently taken out of service, or it is not anymore in use, Deleted – The asset has been deleted.

C. Information Asset Risk Assessment

A risk assessment has to be performed based on the information assets identified in the previous section. Along with risk assessment, a risk treatment plan needs to be defined, and relevant controls to be applied for risk mitigation have to be suggested.

For each risk identified, the following information has to be defined:

Asset: Assets that have been already identified in the Information Asset Inventory. Starting with the most valuable assets and the most likely threats that will cause the highest impact.

Risk description – Threat Analysis and Selection

- **Perform a geographic threat analysis** – This will provide an analysis on the probability of each type of threat against all assets in each location

- **Perform a logical threat analysis for each type of asset** – This provides information on all of the logical threats that can occur to each asset type
- **Perform a threat analysis for each highly valued asset** – This will help to identify any unique threats that may have appeared in the geographic or logical threat analysis, but with different probabilities of occurrence

Risk description – Vulnerability Analysis and Selection

- **Vulnerability Analysis:** an examination of an asset in order to discover weaknesses that could lead to a higher-than-normal rate of occurrence or potency of a threat

Risk type: Identify which of the following can be affected by the already selected threats and vulnerabilities.

- **Confidentiality:** property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- **Integrity:** property of accuracy and completeness
- **Availability:** property of being accessible and usable on demand by an authorized entity
- **Resilience:** "the ability to continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities and recover to an effective operational posture in a time frame consistent with mission needs."

Risk owner: The owner of a risk is the owner of the asset that the specific risk is related to. If the same risk appears in different areas of an organization, then in that case the owner of the risk can be considered a director or a chief executive.

Existing controls: The existing controls that have been already implemented and in place need to be considered during the risk analysis.

Likelihood (1-5): The likelihood or probability that the threat will actually be realized

Likelihood	Description	Summary
1	Improbable	Has never happened before and there is no reason to think it is any more likely now
2	Unlikely	There is a possibility that it could happen, but it probably won't
3	Likely	On balance, the risk is more likely to happen than not
4	Very Likely	It would be a surprise if the risk did not occur either based on past frequency or current circumstances
5	Almost Certain	Either already happens regularly or there is some reason to believe it is virtually imminent

Table 3 Likelihood Description

Impact (1-5): Impact analysis is the study of estimating the impact of specific threats on specific assets.

Impact Level					
Impact Rating	**General Description**	**Effect on Customers**	**Financial Cost**	**Health & Safety**	**Legal, contractual and organizational compliance**
1	Negligible	No effect	Very little or none	Very small additional risk	No implications
2	Slight	Some local disturbance to normal business operations	Some	Within acceptable limits	Small risk of not meeting compliance
3	Moderate	Can still deliver product/service with some difficulty	Unwelcome but could be borne	Elevated risk requiring immediate attention	In definite danger of operating illegally
4	High	Business is crippled in key areas	Severe effect on income and/or profit	Significant danger to life	Operating illegally in some areas
5	Very High	Out of business; no service to customers	Crippling; the organization will go out of business	Real or strong potential loss of life	Severe fines and possible imprisonment of staff

Table 4 Impact Level Description

Risk score = Likelihood * Impact

Risk level:

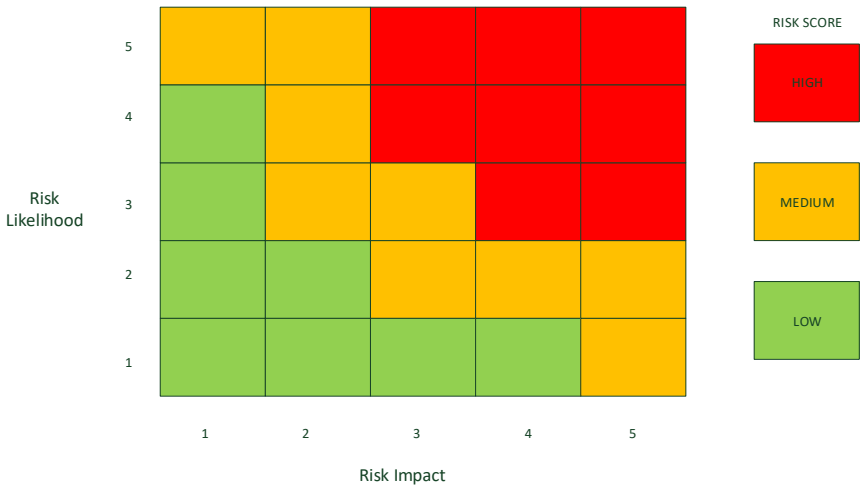


Figure 2 Risk Level

Treatment options:

- **Accept:** Risk acceptance occurs when management is willing to accept an identified risk as-is, with no effort taken to reduce it. Risk acceptance also takes place (sometimes implicitly) for residual risk, after some other forms of risk treatment have been applied.
- **Avoid:** In risk avoidance, the organization abandons the activity altogether, effectively taking the asset out of service so that the threat is no longer present. In another scenario, they may decide that the risk of pursuing a given business activity is too great, so they may decide to avoid that particular activity.
- **Mitigate:** risk mitigation involves the implementation of some solution that will reduce an identified risk. An organization usually makes a decision to implement some form of risk mitigation only after performing some cost analysis to determine whether the reduction of risk is worth the expenditure of risk mitigation.
- **Transfer:** Risk transfer, or sharing, means that some or all of the risk is being transferred to some external entity, such as an insurance company or business partner.

Treatment control & Requirement: Define the control(s) to be applied so that to reduce the likelihood of the risk to occur, or the impact to be faced in case the risk actually occurs.

Post treatment: A post-treatment risk assessment has to be performed here (the same procedure to be followed with the one already described before), in order to show how the implementation of the control selected will affect the likelihood and/or impact of the risk.

D. Threats and Vulnerabilities Identification

During the risk assessment process, threats and vulnerabilities related to the assets, need to be identified. Real-life scenarios of such threats and vulnerabilities to be described, showing the effects on people and cities in the case that a threat is discovered or a vulnerability is exploited.

Threat: Potential cause of an unwanted incident which may result in a harm to a system or an organization. An event that, if realized, would bring harm to an asset, and, hence, to the organization.

Vulnerability: Weakness of an asset or control that can be exploited by one or more threats. A weakness or absence of a protective control that makes the probability of one or more threats more likely.

Categories of threats and vulnerabilities: hardware, software, network, personnel, site, organization

Type	Vulnerabilities	Threats
Hardware	Lack of periodic replacement schemes	Destruction of equipment or media
	Lack of efficient configuration change control	Error in use
	Susceptibility to voltage variations	Loss of power supply
	Lack of care at disposal	Theft of media of documents

Software	No or insufficient software testing	Abuse of rights
	Lack of audit trail	Abuse of rights
	Wrong allocation of access rights	Abuse of rights
Network	Lack of proof or sending or receiving a message	Denial of actions
	Inadequate network management (resilience of routing)	Saturation of the information system
	Unprotected public network connections	Unauthorized use of equipment
Personnel	Absence of personnel	Breach of personnel availability
	Lack of policies for the correct use of telecommunication media and messaging	Unauthorized use of equipment
Site	Inadequate or careless use of physical access control to buildings and rooms	Destruction of equipment or media
	Lack of physical protection of the building	Unauthorized use of equipment
Organization	Lack of information security responsibilities in job descriptions	Error in use
	Lack of procedures of provisions compliance with intellectual rights	Use of counterfeited or copied software

Table 5 Examples of Threats and Vulnerabilities based on different Types

Threat Category	**Threat**	**Example**
Human	**Malicious Outsider**	Someone launches a denial of service attack on your ecommerce website
	Malicious Insider	An employee or trusted third party accesses information in an unauthorized manner from inside your network
	Loss of key personnel	One or more people with key skills or knowledge are unavailable perhaps due to extended sickness
	Human error	An employee accidentally deletes the customer database
	Accidental loss	A manager loses a memory stick with customer bank details on it
	Labor	Work stoppages, sick-outs, protests, and strikes
	Man-made Threats	Leak data via email

		Leak data via upload to unauthorized system
		Leak data via external USB storage device or medium
		Perform a programming error
		Misconfigure a system or device
		Shut down an application, system, or device
		Error perpetrated by any internal staff
		Respond to phishing attack
		Respond to social engineering attack
		Share login credential with another person
		Install or run unauthorized software program
		Copy sensitive data to unauthorized device or system
		Destroy or remove sensitive or critical information
		Retrieve discarded, recycled, or shredded information
		Conduct security scan
		Conduct denial-of-service attack
		Conduct physical attack on systems or facilities
		Conduct credential-guessing attack
		Eavesdropping of a sensitive communication
		Impersonate another individual
		Obtain sensitive information through any illicit means
		Cause data integrity loss through any action
		Intercept network traffic
		Obtain sensitive information through programmatic data leakage
		Perform reconnaissance as part of an attack campaign
		Conduct a social engineering attack
		Power anomaly or failure
		Communications failure
		Heating, venting, or air-conditioning failure

		Degradation of electronic media
		Fire
		Smoke damage
		Fire retardant damage
		Flood due to water main break or drainage failure
		Vandalism
		Demonstrations/protests/picketing
		Terrorist attack
		Electromagnetic pulse
		Explosion
		Bombing
Natural	**Fire**	Your main office burns down due to an electrical fault
	Flood	The nearby river breaks its banks and your main office is severely flooded
	Severe weather	Non-one can get into the office due to the weather
	Earthquake	The area of your main office is affected by an earth tremor that damages all your servers
	Lightning	All your servers are fried by a lightning strike on the data center building
	Severe storms	Tornadoes, hurricanes, windstorms, ice storms, and blizzards
	Earth movement	Landslides, avalanches, volcanoes, and tsunamis
	Disease	Sickness outbreaks and pandemics, as well as quarantines that result
Technical	**Hardware Failure**	A key server has a processor failure
	Software Failure	Your financial system processes invoices incorrectly due to a bug
	Virus / Malicious code	A virus spreads throughout your network preventing access to your data
	Malware	Viruses, worms, Trojan horses, root kits, and associated malicious software
	Hacking attack	Automated attacks as well as targeted attacks by employees, former employees, or criminals

Physical	**Sabotage**	A disgruntled ex-employee takes an axe to your server room
	Theft	You come in on Monday morning to find all of your PCs have been stolen
	Arson	Someone with a grudge against your organization starts a fire during the night
	Violence	Riots, looting, terrorism, and war
Environmental	**Hazardous waste**	A lorry carrying hazardous waste has an accident outside your office
	Power failure	The sub-station supplying your area has a meltdown
	Gas supply failure	There is a suspected leak and all supplies are turned off
Operational	**Process Error**	Your new data transfer procedure doesn't cater for unexpected circumstances and data is lost or sent to the wrong destination
	Crime scene	A crime happens in or near your office and the area is sealed off by police
	Transportation	Airplane crashes, railroad derailments, ship collisions, highway accidents
	Criminal	Extortion, embezzlement, theft, vandalism, sabotage, and hacker intrusion

Table 6 Examples of Threats based on Threat Categories

Vulnerability Examples:

- Missing or inoperative antivirus software
- Outdated and unsupported software in use
- Missing security patches
- Weak password settings
- Missing or incomplete audit logs
- Inadequate monitoring of event logs
- Weak or defective application session management
- Building entrances that permit tailgating

2.1.2 Safety & Physical Security

Because of the direct relation of the health, safety and physical security of people using the Ideal-Cities platform with the security issues previously identified and that need to be addressed, a Health and Safety Risk Assessment needs to be conducted in order to identify this kind of risks as well. Physical Security issues have to be considered as well. Real-life scenarios of such risks have to be described, showing the effects on people and cities.

The same process described above in regards of Assessment needs to be followed for H&S purposes, and the same information for each risk have to be recorded.

2.2 Privacy

The privacy assessment process that needs to be followed in order to identify all the types of data need to be collected and processed in the Ideal-Cities platform, the flow of these data through the data processing, as well as the different consents that need to be collected from the users. To this end, the Privacy Compliance framework (PACT) introduced as part of the Ethics compliance documentation in Deliverables 1 and 4 will be used to maintain alignment between work packages and processes followed for privacy throughout the project.

2.2.1 Data Flow Analysis

The data and information flows need to be analyzed in order to assess the privacy risks.

- The information flow needs to be identified (how the information is transferred from one location to another – inside or outside of the platform). For this the Data Register and Data Journey tabs in PACT will need to be completed together with any data flow diagrams created to support the data flows described; A communication Middleware, in conjunction with Big Data and Cloud services, will support the interconnection between applications and IoT objects (devices, software, and services) based on the use of lightweight standard communication APIs and open software components. In addition, extensions of the capabilities (e.g. networking, adaptation, and monitoring) of Participatory Sensing (PS) platforms are required as PS is intended to be part of applications that might also use IoT, Big Data, and Cloud Infrastructures.
- Identify key elements (such as, data items, formats, transfer method, location, accountability, access, lawful basis, etc.) by completing the “overview” section of PACT framework (step 2);

To effectively map data, we need to identify its key elements.

- **Data items**

Data items are the type of data being processed and the categories into which it falls.

A useful starting point for identifying the relevant data for the system can be the following non-exhaustive list of common categories of personal data:

- Identification and contact data (name, address, email address, etc.)
- Health data
- Genetic data
- Data providing information about personal life and relationships (sexual life, familylife, social life)
- Data about origin
- Judicial data
- Data about personal beliefs (religion, political, philosophical, civil unions, etc.)
- Financial data

- Data about professional life
- Behavioural data (consumption habits, leisure, etc.)
- Location data
- Technical data (IP address, MAC address, URLs, etc.)

Many of these data can be used in multiple applications. For example data related to:

- *Transport applications* - (speed, location, motion, status etc.)
- *Healthcare applications* - (names, addresses, emails, biometrics, patient's historic medical report, location, motion, behavioural events etc.)
- *Environmental Monitoring applications* - (air/water quality metrics, noise measurements, humidity, temperature, waste levels, energy usage/consumption etc.)
- *Building applications* - (level of occupancy, air quality, temperature, HVAC, energy usage/consumption etc.)

- **Formats**

We must clarify how the data has been collected.

The data can be in raw or pre-processed form. Precision is also important, as it defines the granularity level of data (e.g. location). And finally, the volume of data reflects to the format defining the number of data items collected per time period.

- **Transfer method**

The data can be transferred through various mediums depending on the range, power consumption requirements, and bandwidth. For example, cellular networks, Wi-Fi, Near Field Communication (NFC), wide area networks (WAN), low power wide area networks (LPWAN) etc.

Moreover, Edge computing and Fog computing, are technologies that are used to enhance the performance of the network by reducing the latency while also reduce the amount of data that should be proceed and store on the Cloud.

- **Location**

It is important to know the locations involved within the data flow. This could be an office, the Cloud or a third party.

Edge computing is directly related to location awareness as the data are collected and processed closer to the costumer.

- **Accountability**
  - Who is accountable for the personal data often changes as the data moves through the organisation, so it is important to keep track.
- **Access**
  - Visibility is the attribute which shows who has access to the data.

NOTE: increased data flows happen due to the data-driven circular economy requirements (re-use data, etc.) this needs to be explored further.

- Identify unforeseen or unintended uses of data by completing the data risk sections of the PACT framework (steps 3 and 4);
- Completing consider potential future uses of the information collected by walking through the information lifecycle and completing the "PLAN" section of the PACT framework (step 5);
- Make sure that people who will be using the information are consulted on the practical implications. Make sure that controls are in place in order to avoid these practical implications that may arise.

2.2.2 Data Protection Impact Assessment

DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

The DPIA is an important process showing the accountability, and it supports the compliance as data Controller with the requirements of GDPR, but also to demonstrate that appropriate measures have been taken in order to ensure compliance with the Regulation. It is also the key element of the accountability for data protection by design and by default, and a risk-based approach to data protection obligations taken throughout the GDPR.

For the Ideal Cities projects, a full privacy risk assessment is incorporated into the PACT framework.

This privacy risk assessment provided by the PACT framework fully complies will all the requirements for conducting DPIAs under GDPR, and incorporates a Privacy Impact Assessment (PIA) for assessing privacy risks from the organisational perspective as well. In addition, the privacy requirements laid down in Section 3.2.3 of deliverable 4.1, include a series of privacy and security goals to be achieved in designing and implementing any systems as part of the Ideal Cities project. Thus, in conducting a full Data Flow Analysis as described in Section 2.2.1 above, the project ensures that both a DPIA and PIAS are performed as standard.

2.2.3 Consent Process & Consent Form to develop Consent Policy

Any processing of data involving personal data will be obtained following the guidelines as described and outlined in the Ethics Plan (Deliverable 1.1). This includes following the guidelines for obtaining informed consent as laid down in Section 6.3 of the Ideal Cities Ethics Plan (Deliverable 1.1).

2.2.4 Data Processing Addendum

Data Processing Addendum reflects the users' agreement with regards to the processing of personal data in accordance with the requirements of GDPR, has been already defined in Deliverable 1.1 Ethics Plan.

2.3 Resilience Framework (Confidentiality, Integrity, Availability, Sustainability & Privacy)

To date the main approach to enable resilience in CPSs is using hardware redundancy and robust controllers. These proved to be very successful in manufacturing; however, they are very expensive while robust controllers require significant engineering resources to program and modify even by the standards of large industrial companies. In Ideal Cities we will introduce new resilience techniques exploiting symptoms of disruptions to enable overall system health, autonomic response without the need for human intervention, and an ability of the system to reconfigure itself.

We envision an ideal city to contain millions of IoT devices within a Cyber-Physical System of Systems (CPSoS). In accordance to the 5G approach, these devices can fall under the category of massive machine type communications (mMTC), where these are typically high in volume but exchange a relatively low amount of data. Another category is the devices that engage in the so called ultra reliable low latency communications (URLLC) in which case they require high quality of service in communications. The underlying business requirements set by the respective use case which in turn specifies the resiliency requirements.

In this report by an IoT devise, we imply a device that has at least either a sensor or an actuator and is connected to an Internet; while by a Cyber-Physical System (CPS), we imply a system that integrates cyber and physical components using computing and network technologies, sensors, and IoT.

[44] argue that the IoT for CPS should be dependable and secure, where dependability should satisfy five attributes [41] (availability, reliability, safety, integrity, and maintainability) and security should satisfy three attributes (availability, integrity and confidentiality). While, [46] emphasises the importance of information exchange in CPSoS and therefore outlines the following eight attributes: interoperability, scalability, adaptability, usability, resilience, security, trust, and privacy.

A widely adopted definition of a resilient CPS, [43], [45], is that it is a system that can withstand any types of internal changes and continue to deliver services, despite of failures, hardware reconfigurations, and software updates. From security perspective, the resilience of a CPS is an ability to withstand against malicious ciber attacs and accidental threats.

[43] introduce Holistic Resicilncy Cycle (HRC) for cyber-physical systems that consists of four stages: (1) prevention and planning, (2) detection, (3) mitigation and response, and (4) system recovery. To date, the main approach to enable resilience in CPSs is using hardware redundancy and robust controllers. These proved to be very successful in manufacturing; however, they are very expensive while robust controllers require significant engineering resources to program and modify even by the standards of large industrial companies.

While we do not disagree with [43], we propose to distinguish between the levels of resilience to measure the severity of the accident and level of response required from human operators and engineers. In particular we propose the following three levels (Figure 3).

1. Automatic detection of, and autonomic recovery from, symptoms of threat – a system recovers with no human assistance and no distruption to services.
2. Automatic detection of, and autonomoic recover from, a threat – a systems recovers with no human assistance, but there might be some disruptions to services.

3. Automatic detection of threat – to recover a system requires human assistance and there are disruptions to services.

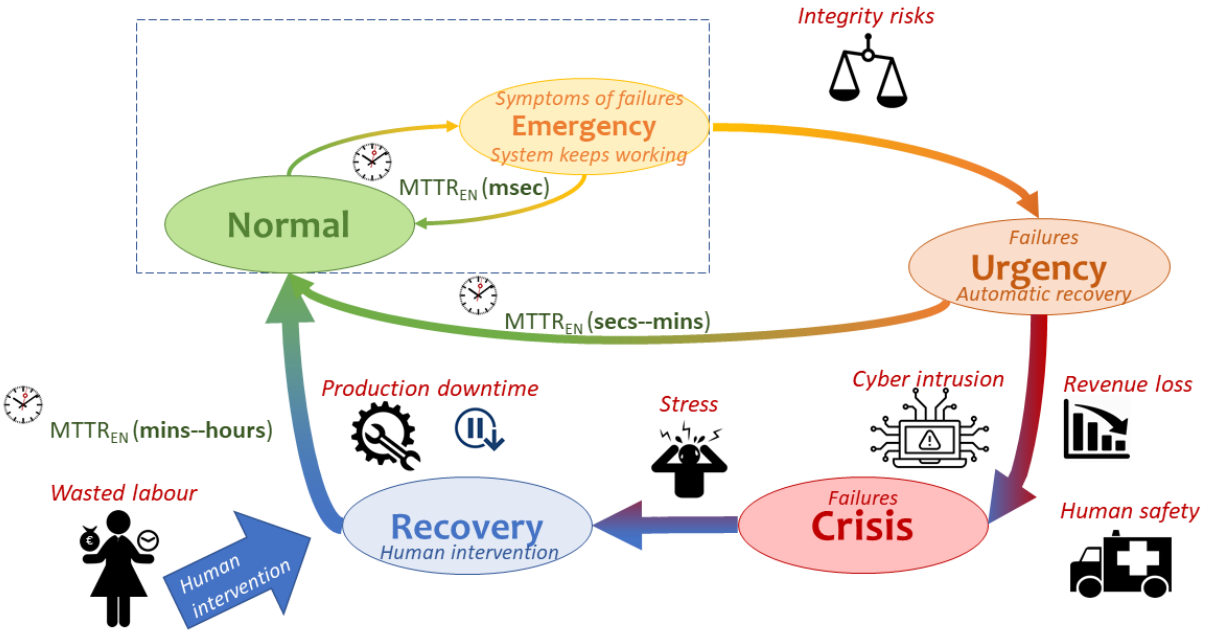


Figure 3 Resilience states in CPSoS.

In Ideal Cities, we will introduce new resilience techniques exploiting symptoms of disruptions to enable overall system health, autonomic response without the need for human intervention, and an ability of the system to reconfigure itself.

Another aspect of resilience, viewed from agent based control systems, focuses on transforming agents into “team players”. Instead of only focussing on making agents more autonomous we will explore opportunities for joint activities with other systems and as a human-agent collaboration.

3 Identification

Identification of the requirements and mechanisms in regards of IoT, security and privacy is mandatory in order to design and implement the Ideal Cities platform and concept.

3.1 Security and Privacy Requirements/Mechanisms for IoT

According to Gartner **Error! Reference source not found.**, the IoT-enabled devices will exceed t he 20.4bn by 2020. These high volumes of interconnected devices constitute an increasingly attractive target for attackers. After the demonstration of several IoT vulnerabilities by researchers and their successful exploitation by attackers (e.g. smart vehicles and smart lights [29]), IoT security has now become an issue of high concern for the main Informatics stakeholders. The figure below depicts the forecasts for the cybersecurity market until 2020, as evaluated by the IoT security report of the Business Insider.

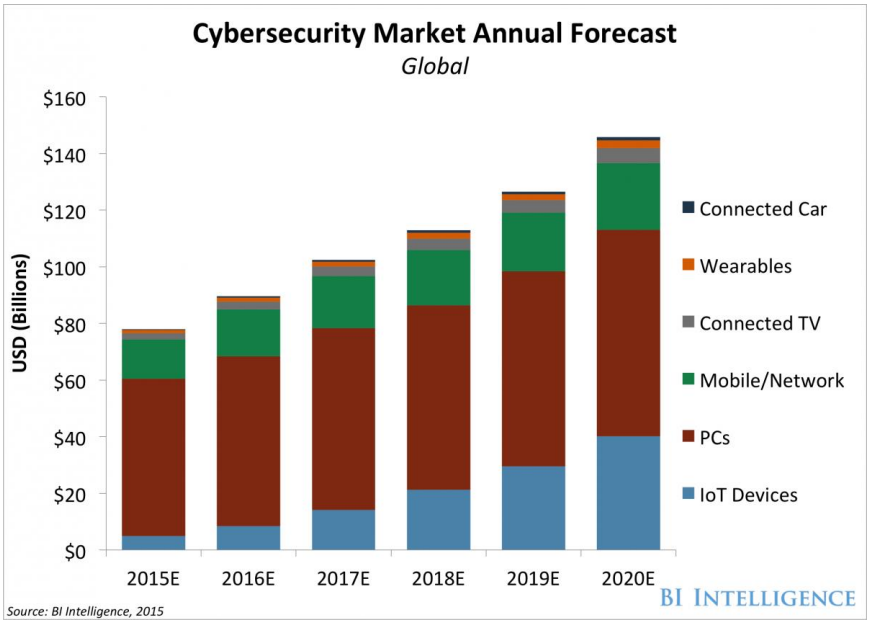


Figure 4 Cybersecurity Market Annual Forecasts by Business Insider

Several methodologies and standards are established in order to assist the secure development of a system. Popular and widely used techniques for specifying security include the *Common Criteria Evaluation Methodology (CEM)* (ISO/IEC 15408 1996-2018) and the *Open Source Security Testing Methodology Manual* (ISECOM 1988-2918).

The three main cyber security principles for any type of security control are referred to as the *Confidentiality, Integrity, Availability (CIA) principles*. Confidentiality is the property where information is not disclosed to users, processes, or devices unless they have been authorized to access the information. Integrity is the property whereby information has not been modified or destroyed in an unauthorized manner. Availability is the property of being accessible. Each of these three principles involve relevant protection mechanisms, which are described in the following table, as they are derived from the abovementioned standards and related research efforts [31].

Aspect	Protection Mechanism	Description
Confidentiality	Confidentiality	Guarantees that a processed asset is not becoming known outside the interacting entities
	Authentication	Challenges credentials on the basis of identification and authorization
	Resilience	Preserves protection in case of failure
Integrity	Integrity	Guarantees that the interacting entities know when an asset has been changed
	Subjugation	Guarantees that transactions occur based on a defined process, removing freedom of choice and liability in the case of disclosure
	Nonrepudiation	Prevents the interacting entities from denying their role in an interaction
Availability	Continuity	Preserves interactivity in the case of failure
	Alarm	Informs that an interaction is happening or has happened
	Indemnification	Includes a contract between the asset owner and the interacting entity. It may also involve warnings as a precursor of legal action and public legislative protection

Table 7 Security aspects and protection mechanisms

Surveys regarding security, architecture, and enabling technologies in the IoT domain are presented in [34]; [7]; [14], while a taxonomy of the related security attacks is proposed in [35]. The guidelines for secure IoT development, as also suggested by large computer and software vendors (e.g., Microsoft, IBM, Siemens, Gemalto, etc.), include the following three security areas:

- *Device security*, i.e., mechanisms and techniques for protecting the device itself, once it is deployed in the field.
- *Connectivity security,* i.e., mechanisms and techniques for guarantying that the transmitted data between the IoT devices and the IoT Hub/Gateway is confidential and tamper-proof.
- *Cloud security,* i.e., mechanisms and techniques for safeguarding data while it is transmitted to, and is stored in the cloud.

Popular IoT platforms, like the Microsoft Azure IoT suite [15] and the IBM Watson IoT Platform [36], tackle these issues and provide the mainstream security solutions, as we have described in Section 3.2 of this deliverable. In the following, we provide an overview of state-of-the-art IoT security grouped in under the three main areas listed above.

3.1.1 Device Security

Device security implements the different aspects for authenticating a device in an IoT application. Two main components are required for this purpose:

- A *unique identity key* or *security token* for each device. The device utilizes this key in order to authenticate and communicate with the IoT gateway.
- An *on-device X.509 certificate* and *private key* for authenticating the device to the IoT gateway. The authentication procedure must guarantee that this private key is not known outside the device at any time, thus achieving a higher level of protection.

In typical device operation, the device token provides authentication for each transaction that is made by the device to the IoT gateway. Thus, the symmetric key is associated to each transaction. The X.509-based procedure enables the authentication of the device at the physical layer during the establishment of the TLS connection (connectivity security). The certificate contains information that is related to the devices, like its ID, and other organizational details.

The security token can be also used alone, without requiring the X.509 authentication, but in a less secure setting. The choice between the two methods is determined by the availability of the adequate resources on the device end (e.g. store the private key securely) and the level of authentication security that is needed by the application.

3.1.2 Connectivity Security

Connecting IoT devices over the Internet poses threats for data confidentiality and integrity. It is, thus, important to ensure that all the transmitted data between the devices and IoT gateways and from there to the cloud is encrypted.

The IoT gateway utilizes the security tokens to authenticate devices and services. The process is managed automatically by the IoT platforms. The seamless communication is supported by relevant protocols, such as the Advanced Message Queuing Protocol (AMQP), MQTT, and HTTP [30], and is safeguarded by the security mechanisms that are implemented by each one of them. Nevertheless, these underlying solutions process the security tokens in different ways and the correct usage should be inspected in each specific case. This is a technical issue and concerns the correct mapping of the token-related information to each protocol's data format. For example, the MQTT connection request utilizes the device ID in the username and the security token in the password field, while HTTP includes the valid token in the authorization request header. In addition, some application settings need the user to generate the security tokens and use them directly. Examples of these scenarios include the direct use of AMQP, MQTT, or HTTP surfaces.

The IoT gateway maintains an *identity registry* for the secure storage of device identities and security keys. Distinct devices or groups of them can be added to allow or block list, achieving complete control over device access. The high-level device provisioning includes the following steps:

- Associate an identifier at the physical device (i.e., the device identity and/or X.509 certificate) at the manufacturing or commissioning phases
- Create a relevant entry at the gateway's identity registry
- Securely store the X.509 certificate thumbprint in the registry

On the other hand, the device must also authenticate the gateway. In the ordinary setting, a root certificate, which is included in the device software development kit SDK, is utilized for authenticating the gateway's credentials. Although the root certificates are long-lived, they can also expire or be revoked. Thus, a secure procedure must be foreseen for updating the root certificate on the device end or, otherwise, the IoT devices may be subsequently unable to connect to the IoT gateway or the cloud services.

Finally, the Internet connection between the devices and the gateway is generally protected by the SSL/TLS 1.2 standards. Old versions of each protocol may also be supported for backward compatibility (i.e., TLS1.1, TLS 1.0).

3.1.3 Cloud Security

Cloud computing suffers from a number of security issues that overlooking them may lead to catastrophic consequences. As seen on [33]; [27] the main security vulnerabilities can be categorized as bellow

- Shared technologies: As seen in [37]; [38] attacker can exploit shared memory technologies to gain access to unauthorized content such as encryption keys
- Data breach: Personal data containing sensitive information such as credit card information can be lost or worse can be leaked.
- Account/service hijacking: If login credentials are lost or leaked, this can lead to attackers gaining access to critical areas of services and could potentially compromise confidentiality, integrity and availability.
- Denial of Service (DoS): As seen in [26] cloud infrastructure mechanisms cope with DoS attacks [48] by providing scaling up its resources but this firstly provides the attacker with more resources to achieve his malicious goals and secondly can this type of attack can have monetary impacts.
- Malicious insiders: A company's employee can leverage his position to access sensitive information of the hosted services.

As a first line of defence to prevent the physical access attacks is obviously a high-level physical security at the data-centres. Furthermore, a scheme using XACML (OASIS 2005) can be used to limit access of employees to decrease the possibility of an insider attack.

To prevent side channel attacks as proposed in [42] KAISER can be used in order to achieve kernel space isolation. Moreover, Intel trusted execution technology provides a trusted way of loading and executing the Virtual Machine Monitor (VMM) or the OS kernel has a serious limitation as described in [39] which is that the attacker can easily bypass it if he has physical access to the servers.

[32] uses misuse patterns to describe the environment, conditions and sequences of an attack based on co-residence between malicious and legitimate virtual machines. The misuse patterns act as a repository, which may then be used by developers for security measures against the attacks. In addition, Intrusion Detection Systems (IDS) that monitor and detect malicious activity in a system can be used to prevent intrusions. However due to the high complexity of the cloud a Hybrid Intrusion Detection System can be used [40].

To prevent data breaches and to guarantee data confidentiality and integrity on the channels and so prevent Sniffing and Spoofing Attacks the basic solution is to use an encrypted network protocol that encrypts all the traffic from the source to the destination over the whole trip.

SSL and TLS can be used to prevent leakage of sensitive information through communication encryption. Another standard commonly used by CPs is IPsec, a protocol suite for securing IP communications implementing network-level authentication and encryption for each IP packet. Usually these mechanisms protect network traffic to the edge of the cloud network, VPN and its techniques as SSH and IPsec tunnels are used to defend traffic between servers within the cloud network.

3.1.4 IoT Privacy

3.1.4.1 *Private Data*

In IoT applications, high volumes of personal data are exchanged by the underlying systems, rising serious concerns regarding privacy and deriving the application of relevant protection controls imperative for the end users. Therefore, several standards (like the ISO/IEC standards 27018 (ISO/IEC 2014) and 29100 (ISO/IEC 2011)) and regulation efforts (such as the General Data Protection Regulation of European Union – Regulation (EC) 2016/679 (European Parliament 2016)) are established, trying to tackle these issues.

This type of knowledge that is referred to a person is defined as Personal Identifiable Information (PII) (ISO/IEC 2011). The data may be categorized as personal sensitive, sensitive, and statistical (ISO/IEC 2011), with the first category demanding the highest privacy protection followed by the sensitive data, while statistical data requires moderate protection with such information becoming often publicly known via survey reports.

Moreover, three actuator types are defined, marshalling the ownership of personal data and the related processing rights (ISO/IEC 2011). The *PII principal/owner* is the person to whom the data is referred to and must have the total control and legal rights over the data. The *PII contracted processor* is the entity (e.g. person or service) that has been granted the explicit agreement of the PII principal for processing his/her personal data for a specific purpose. The processor is restricted and cannot use the data in a way that will trespass the common agreement with the principal. Nevertheless, in order to deliver the required functionality, the processor may need to disclose the PII to a *third party*. The processor has to obtain the explicit consent from the principal, with the corresponding processing terms and access rights also restricting the usage for the third party. For every violation, the contracted processor and the different third parties are accountable to the PII owner.

3.1.4.2 *Protection mechanisms*

Privacy threats include malicious or non-malicious events that affect the protected PII (e.g. exploitation of connection vulnerabilities for smart home equipment [13] or private data disclosure from wearable fitness tracking devices (Zhou and Piramuthu 2014). The private data must be protected during the transmission and storage operations. The aforementioned security mechanisms on the previous subsections are deployed for this purpose and ensure the CIA principles.

Nonetheless, there are other specific protection mechanisms for preserving privacy that safeguard the private data during the collection, access, and usage procedures. Typically, the PII owner must be always get informed about the collection of his/her personal data, the entities that can gain access to them, and how this information is going to be used.

The general privacy framework and properties are defined in ISO/IEC standards 27018 (ISO/IEC 2014) and 29100 (ISO/IEC 2011), and the General Data Protection Regulation of

European Union – Regulation (EC) 2016/679 (European Parliament 2016). The next table summarizes the main privacy properties and the specialized protection mechanisms, as derived by these initiatives [31].

Aspect	**Protection Mechanism**	**Description**
Data Collection	Consent	Demands the PII owner's freely given, specific, and informed agreement to the processing of the PII. The PII must not be shared or disclosed to a third party without the owner's consent
	Opt-in	Includes a policy or process where the PII owner agrees explicitly to the PII's processing, before relevant consent
	Fairness	Guarantees that the PII is collected, used, or disclosed for only the appropriate purposes, implementing the GDPR features of collected data minimization and accuracy
Data Access	Identifiability	Results in identifying the PII owner, directly or indirectly, based on a given set of PII. It should include identifiability, pseudonymization, or anonymity
	Notification	Informs the PII owner that his/hers data are being collected
	Auditability	Provides adequate means to identify and control the access of PII data
	Challenge compliance (accountability)	Guarantees that the PII owner can hold the PII processors accountable for adhering to all privacy controls, supporting the GDPR properties for lawfulness, fairness, and transparency
Data Usage	Retention	Guarantees that the PII, which is no longer needed, is not maintained, as a precautionary measure towards the minimization of unauthorized collection, disclosure, or use.
	Disposal	Includes mechanisms for destroying or disposing of the PII on demand, including and the 'right to be forgotten' of GDPR
	Report	Informs that an interaction with PII is happening or has happened
	Break or incident response	Manages a breach of PII

Table 8 Privacy aspects and protection mechanisms

3.1.4.3 *Identification and Anonymity*

The identification of the user is one of the main concerns of every privacy preserving strategy. An adversary may be able to correlate the exchange data with a specific person by integrating different sources of available information. In some cases, the user may wish to preserve his/her anonymity even from the service provider. Thus, the way that the user has access to an application is important for preserving privacy. In general, three types of user access can be implemented that are also determined by the functionality that is requested:

- An **authenticated user** must login the system and use the provided service using its own identity (real or virtual), for example in e-government services or social-media
- A user that access the system utilizing a **pseudonym**
- Anonymous usage

In the first case, the service provider knowns the user's identity and the system may intentionally or non-intentionally track the user's activity. The user is aware of this fact and participates with his/her own will. If this type of knowledge is available, it can be utilized not only by the provider but also by a third party or an attacker that will gain access to it. In such cases, the undesired effects need to be circumscribed by established security and privacy controls (e.g. store encrypted data in the database and minimize the pieces of personal information that has to be maintained).

When pseudonyms are utilized, the user cannot be tracked directly. This provides a higher privacy protection that is considered adequate for many applications. However, context knowledge can still make it possible to infer information about the user. For example, from service requests that are made by users that are located in a hospital, we can infer that these people are either employees, patients, or patients' companions. A user, that uses an IoT application service from the hospital almost every day, could also be identified as faculty stuff. If the same user also accesses the system frequently from another constantly used location, then we could deduce with a high probability that this other location is his/her home and from it try to figure out the true identity of the user and track back all the service activity to the specific person. Thus, extra protection mechanisms must be deployed as a defence measure, especially for the location-based services (LBS) that are usually provided by the different IoT settings [16].

The main defence strategies include *cloaking areas* [17] and *k-anonymity* [18],[19] . In cloaking areas, the users' mobile equipment deploys automatic procedures where the pseudonyms of different people are randomly interchanged when they are passing through a specified area. For example, in an IoT environment with smart cars the anonymization areas may be located in the traffic lights or in road crossing, where many cars are met and decrease their speed, allowing the identity change to take place. However, context knowledge can still be inferred [20]. The effectiveness of this solution depends on the density of the anonymization areas and the volume of the participating users over time. The higher the density and the volume, the higher the protection. More advanced schemes are proposed to counter such attacks. Semantic obfuscation techniques intermix the data of semantically diverse domains and reduce the deduced amount of context knowledge [21]. Other protection mechanisms can send dummy location data to the LBS provider instead of the accurate location [22]. Also, the cloaking solution is only applicable to LBS or other services that involve the user's mobility.

With *k-anonymity*, an intermediate entity between the users and the service is responsible for blurring the identities of at least 'k' users with each other. The users may need to subscribe in

this entity and access the functionality even through Internet, overcoming the locality restrictions of the cloaking areas. However, the entity must be considered as a trusted participant by the users' community. In other cases, the functionality can be implemented as a peer-to-peer service, running on the user's devices. On the other hand, this option demands the users' active participation and the willingness to consume their own resources for the community's benefit. Nevertheless, one main advantage of k-anonymity for system design is the fact that the protection level can be quantified and configured. Increasing the 'k' factor, enhances the privacy defence. Combinatorial approaches of both cloaking areas and k-anonymity schemes are also suggested [23] taking advantage of the benefits from both approaches.

Anonymous participation requires threshold signature schemes [24]. A community possess valid credentials to a service (i.e., crowdsourcing), which are then processed by the threshold scheme. Each community participant possesses a share of the common secret. In order to decrypt and authenticate the credentials, one would require at least *n* valid shares. Thus, users send their collected data to the service along with their shares. If the service achieves to authenticate the credentials of the group utilizing *n* shares, the data from these specific users are considered authenticated and are further processed. The user provides only partial knowledge to the data collector regarding the credentials of such a group. The collector trusts and processes the data, while the unlink ability with the contributor's identity is retained. These schemes can be centralized, decentralized, or hybrid. The protection level can be configured by changing the *n* parameter of the threshold scheme. One main security concern is the fact that the community signing key dealers must be honest and trustworthy.

On the other hand, anonymous privacy-preserving techniques restrict popular business operations for e-commerce and targeted marketing. Thus, attribute-based credentials (ABC) are proposed as a mean to protect privacy and provide the adequate information to the service provider [25]. In ABC, a cryptographic container stores attribute-related data, similarly with an X.509 certificate. The container is issued by a trusted authority and bounds the ABC owner to a secret key. The user can show only his/her attributes and prove that they are signed by the authority. The selective disclosure feature enables the user to send only an arbitrary attribute subset, like his/hers purchase level that determines discounts or other advantages. As the proof is based on zero-knowledge, the service provider does not learn the secret key of the user. Moreover, some ABC schemes offer multi-show unlinkability that prevent the service from correlating two different showings of the same user.

3.1.4.4 *General Data Protection Legislation (GDPR)*

The development of new technologies, such as the IoT, has somewhat complicated the notion of "personal data" and led to the emergence of various types of data. In the EU, the concept of "personal data" is rather wide-ranging. The GDPR particularly expanded the definition of "data subject" to take account of the online environment and is referred to as:

"An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (GDPR, art 4(1)).

The fact that the definition refers to any information relating to an "identified or identifiable" individual basically means that it includes the name of a person, mobile phone number, e-mail,

location, contacts, credit card and payment data, browsing history, pictures, videos, temperature, blood pressure, insulin level, etc.

Recital 30 of the GDPR elaborates on the issue as follows:

"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

Whithin the Ideal Cities Project, the PACT framework can be used in order to achieve compliance with the GDPR. PACT is a privacy decision tool for assessing privacy risks throughout the data lifecycle by integrating the privacy decision-making function into organisational decision-making-by default [47].

Requirements

The privacy requirements for the IDEAL-CITIES platform will be devised based on an analysis of each partner organisation's security and privacy policies.

This list of Requirements will be organised in accordance with Volere principles[i]. This means that, for each requirement the following information will be captured:

1. ***ID:*** a unique ID will be created for each requirement;
2. ***Type:*** the requirements will be organised by type:

Functional Requirements (FR): i.e. the essential or fundamental requirements that are necessary for the platform;

Non-Functional Requirements (NFR): i.e. the behavioural characteristics that the specified functions must have these include:

NF1. ***Look and feel Requirements***: i.e. style and appearance requirements
NF2. ***Usability Requirements;***
NF3. ***Performance Requirements;***
NF4. ***Operational Requirements;***
NF5. ***Maintainability and Support Requirements:***
NF6. ***Security & Privacy Requirements***: i.e. the security and privacy goals to be achieved, these will, for privacy, comply with the General Data Protection Regulation (GDPR) and be based on the privacy principles of GDPR (P1-7) and those in the Privacy Lifecycle PLAN (i-ix), that forms part of the Privacy and Compliance framework (PACT). These are:

P1. ***Lawful basis for processing:*** the lawful basis for processing data will be specified, recorded and justified;
P2. ***Purpose Limitation:*** personal data should only be processed for needed and specified purpose; no personal data should be reused without informed consent first being obtained;
P3. ***Data Minimisation:*** only necessary data for the specified purpose will be processed;
P4. ***Accuracy:*** the data will be accurate and kept up to date;
P5. ***Storage Limitation:*** data will be pseudonymised or anonymised as soon as practicable and kept for no longer than absolutely necessary

('the data life'). At the end of the data life, data will be securely deleted and/or destroyed.

P6. ***Integrity and Confidentiality:***

i. ***Confidentiality:*** Ensuring data is only accessible to authorised stakeholders

ii. ***Integrity:*** Ensuring non-repudiation and reliability for each piece of data, i.e. processing correct, authentic, and unmodified data.

iii. ***Availability:*** Ensuring data is usable on demand and accessible to authorised stakeholders

iv. ***Unlinkability:*** Ensuring data cannot be sufficiently distinguished to linked across platforms or domains with similar context or purposes

v. ***Unobservability/ Undetectability:*** Ensuring data is anonymised so that the anonymity and undectability of the individual is preserved

vi. ***Anonymity:*** Obfuscating links between data and identity i.e. the ability to distinguish any one individual from the data

vii. ***Pseudonymity:*** Replacing identifying data with pseudonyms ensuring any links to original data cannot be made by unauthorised parties

viii. ***Intervenability:*** Enabling data subject access and/or supervisory authority access to affect action on the records (e.g. request modification and/or deletion). In that way it can be seen as a safeguarding measure that must be included within any process or system involving personal data

ix. ***Transparency:*** Openness - Providing assurance, accountability and traceability for internal and external stakeholders.

P7. ***Proportionality:*** Proportionality requires that any limitation on the rights of the individual have to be justified. For example, making sure that the measure(s) taken in processing the data do not disproportionally limit the rights of the individual whose data is being processed. A pre-condition is that the measure(s) taken in processing or safeguarding are sufficient to achieve the objective while only relevant personal data for the purposes of the processing is collected and processed.

NF7. ***Cultural and Political Requirements***

NF8. ***Legal Requirements***

1. ***Rationale:*** the rationale for each requirement will be noted
2. ***Originator:*** a note of the user/document from which the requirement was derived will be captured;
    a. (with Security and Privacy forming one of those types);
3. ***Use Case:*** reference to the relevant use case (e.g. see Section 2 for pilot use cases) or, where these relate to other elements such as the platform design, a use case will be created for each requirement;
4. ***Fit criterion:*** testing the requirement for 'fitness' this shall include quality Metrics that measure and evaluate whether the requirement has been met i.e. the quality, function and suitability of the requirement.

Following a document analysis approach and the constraints provided by the IDEAL-CITIES selected use cases and proposed architecture, the following high level security requirements for the IoT devices were elicitated:

1. IoT device trust. The IoT assets will need to be assigned a level of criticality following a risk assessment exercise. The latter will classify the IoT devices and will dictate the level of trust needed. For instance, a smart meter will need to offer high data integrity of the measurements and confidentiality of the traffic information as this can potentially reveal citizen's habits.
2. Privacy by design: the IoT devices that handle personal data will need to implement controls to offer privacy requirements (Confidentiality, Integrity, Availability, Unlinkability, Unobservability, Anonymity, Psedonymity, Intervenability and Transparency). The aggregated data residing in the repositories should only support privacy enhancing technologies such as secure multiparty computation and homomorphic encryption in order to perform data analytics without revealing the identity of the subjects.
3. Policy driven end-to-end security. This supports the privacy by design requirement by allowing the design of a policy-driven security model that could enable customisation and extensibility to create a set of best practises.
4. Accountability. Secure logging will be deployed in order to conduct troubleshooting in the event of errors, and to allow forensic investigations in the case of a security breach.
5. Device identification and authentication. Depending on the criticality of the IoT asset, its computing and storage capabilities and energy resources, an appropriate level of identification and authentication should be achieved. At a minimum level, the device will have a unique identifier when joining the network and this should be used to leverage robust authentication mechanisms.

3.2 Security Mechanisms

Define the security mechanisms – a set of modules providing basic device and/or user identification, authentication, access control, privacy enhancing, confidentiality maintaining, integrity and encryption functions to IoTPS applications, in order to ensure data integrity and confidentiality of private information - that need to be implemented. Consider the following:

3.2.1 IoT Physical and hardware security

When deploying an IoT network, it should be taken into account that IoT devices such as sensors, actuators or other networked objects will often be in locations which are remote, unsupervised and with little or no control of who can access them. It therefore makes sense to consider the following points:

- Physical protection: how the hardware of the device itself can be protected from tampering. Futher considerations are preventing unintentional damage (e.g. adverse weather conditions) vandalism or theft. These are however out of the scope of this section given their pre-dominantly non-technical nature.
- Bootstrapping: encompasses the crucial process of powering up the device and the initial loading of the first lines of executable code.
- Processor and memory space: appropriate measures need to taken in order prevent unauthorized access to critical run-time system resources

- Key management and trusted computing: Any keys used by the device itself (e.g. the device's private key) need to be properly managed and stored.
- Storage security: protection of mass storage modules such as flash memory in case the IoT device is stolen. Includes also the proper disposal of storage once the device is decommissioned.

3.2.2 Authentication

Authentication is the process of confirming and ensuring the identity of the devices/users that connect to a network in order to secure data and allow the access only to authorised users. Authentication is considered as a key requirement for IoT[49]; trusting the devices participating in an IoT network is crucial for the well-functioning of the network. A single compromised node can be turned malicious and bring down the whole system or cause disasters[50].

In the surroundings of a smart city with various verticals the authentication processes share a number of common principles like the following;

- Authentication mechanisms should take into consideration the limited resources of the majority of the system's nodes.
- The robustness of the authentication protocols should be judged against attacks like node capture, replay attacks, message forgery, brute force attacks, MITM, DoS, password guessing etc.
- Authentication mechanisms should consider the scalability of the networks and the possibility of the addition of new nodes along with the heterogeneity of the devices.
- Authentication mechanisms should be implemented in the application, network and perception layer.

The smart devices have the following authentication procedures:

- One-factor authentication: During the communication of two devices one party authenticates itself while the other remains unauthenticated.
- Two-factor authentication: During the communication of two devices both parties authenticate each other.
- Three-factor authentication: During communication a central dispatcher authenticates two parties and helps them to mutually authenticate themselves.
- Token-based authentication: Authentication is based on a token created by an authentication protocol.

3.2.2.1 *Security mechanisms supporting lightweight authentication for smart objects*

Due to their resource-constrained characteristics, devices need to be in position to reduce energy consumption during the authentication phase and the communication with other neighboring devices. The fact that the IoT devices communicate over insecure channels constitutes them even more vulnerable to threats. Therefore, authentication schemes that use classic cryptographic algorithms and protocols need to be re-evaluated and adjusted to the needs of the Wireless Sensor Networks (WSN), taking into consideration an inevitable tradeoff between power consumption and security.

3.2.3 Secure communications

Secure communication is about ensuring that information transmitted over a common medium connecting two or more parties cannot be intercepted in any form. Within an IoT network, security of the communication channels needs to be enforced for the Personal Area Network (between the IoT device and the gateway), and the Wide Area Network (between the gateway and the cloud). According to ENISA[51], the following overarching security concerns for communications apply and should be considered:

- Man-in-the-middle: Active eavesdropping attack, in which the attacker relays messages from one victim to another, in order to make them believe that they are talking directly to each other.
- IoT communication protocol hijacking: Taking control of an existing communication session between two elements of the network, allowing the intruder to sniff sensible information, including passwords. The hijacking can use aggressive techniques like forcing disconnection or denial of service.
- Interception of information: Unauthorised interception (and sometimes modification) of a private communication, such as phone calls, instant messages, e-mail communications
- Network reconnaissance: Passively obtain internal information about the network: devices connected, protocol used, open ports, services in use, etc
- Session hijacking: Stealing the data connection by acting as a legitimate host in order to steal, modify or delete transmitted data.
- Information gathering: Passively obtain internal information about the network: devices connected, protocol used, etc.
- Replay of messages: This attack uses a valid data transmission maliciously by repeatedly sending it or delaying it, in order to manipulate or crash the targeted device.
- Network Outage: Interruption or failure in the network supply, either intentional or accidental. Depending on the network segment affected, and on the time required to recover, the importance of this threat ranges from high to critical.
- Device modification: Tampering a device by for example taking advantage of bad configuration of ports, exploiting those left open.

3.2.4 Data encryption

Following the best practices laid out by ENISA[51], data encryption mechanisms should be in place in the disciplines listed below:

- IT Security Administration: for all software and firmware updates, the corresponding mechanisms should ensure via encryption that the senders can be trusted and the software update packages are valid and correct.
- Identity and Access Management: for safe propagation of user credentials, usernames, passwords and similar authentication data must be encrypted
- Physical security: to safeguard for cases where an information bearing device is compromised, the data at rest should be encrypted.

- Communications: to ensure confidentiality when sharing information between parties, the communication channel should be encrypted
- Interfaces: to guarantee end-to-end protection (i.e. including the device endpoints) for the communication session and to avoid hijacking or replay attacks, the entire user session should be encrypted.

Especially for the IoT devices, limitations with regards to power and processing capabilities exist, consequently the extent and degree of encryption needs to be assessed carefully on a per case basis.

3.2.5 Data anonymization

The anonymization of data is increasingly becoming more important as an enabler for privacy, especially when seen also from a regulatory angle such as the European GDPR framework[52]. In general, anonymization is the process where data is modified in such a way that it becomes unattributable to its source or owner. It can be considered particularly attractive for service providers, since, if properly executed, can allow the providers to collect user data to customize/optimize their services to clients while simulatenously respeting their user's privacy. There are two main ways to achieve anonymization of data:

- Removal: Sensitive data is stripped from the content, and/or unlinked from the related data sources (e.g. a data table containing names is unlinked from the related data form or data stream so that it no longer feeds it).
- Obfuscation: Using data processing methods such as encryption, sensitive data is modified in such a way that it becomes unintelligible.

Especially the latter form of anonymization can be achieved by the usage of specialized tools, some of which are open source[53]. In addition to applying anonymziation in the cloud on data-at-rest, there is also an emerging drive to research and apply anonymzation in the bottom layers of IoT networks (i.e. the layers including the device itself, the gateways, and the PAN and WAN communication channels). Within this context, data anonymization can consider the following aspects:

- Denaturing mechanisms, e.g. for blurring of visual media, which can be applied selectively to certain or all parts of the transmitted data, as proposed by [54].
- Seperation of sensitive data from non-sensitive data through the use of different channels and data brokers. Sensitive channels can then apply additional encryption or masking techniques to preserve privacy, while channels conveying non-sensitive data can be optimized for performance. An indicative framework is described by [55].
- Adoption of user-driven privacy policies and preferences, and customizable real-time notification of users about privacy violations. One approach has been portrayed by [56].

4 Implementation

4.1 How to Implement the Security Mechanisms Identified

Implementing data anonymization, encryption and authenticity preserving mechanisms to ensure that user/object sensitive information will not be available to any third parties without the user consent. As IotPS applications can acquire and share sensitive personal information about citizens, IDEAL - CITIES will provide anonymization and pseudonymization mechanisms (based on distributed and/or edge computing mechanisms) to ensure that the data exchanged does not contain personal sensitive information. Provide opportunistic encryption, cryptographic integrity and authenticity mechanisms to ensure that the communications over the various heterogeneous technologies underpinning IoTPS applications are encrypted, at least with lightweight encryption methods.

4.1.1 Physical and Hardware Security

4.1.1.1 *Physical security*

Physical vulnerabilities can be generally classified into two types:

- Non-invasive attacks, where the adversary does not come into physical contact with the device, but is close enough to sense (and manipulate) electrical characteristics
- Invasive attacks, where the adversary can physically manipulate the IoT device and its electronics.

There are various attacks within these two categories. The following non-exhaustive list contains the two most important ones and ways to mitigate them:

- Side Channel Attacks: a non-invasive attack which senses and analyzes the power emitted from a device in order to extract sensitive information. Changes to power measured can be mapped to power signatures, which in turn can reveal information about algorithms or executed commands. Methods to combat these attacks are:
    - Use short-lived session keys for encryption
    - Add randomness in algorithms and randomly pick one out of many different execution commands to perform a function, thereby increasing the attack surface
    - Minimize power leakage and the number of operations required.
    - Where possible, scramble the sequence of execution steps.
    - Add noise into power lines
- Tampering attacks: an invasive form of attack where the adversary gains direct access to the device circuitry and can directly tap information from the wires using microprobes. Methods to address these attacks are:
    - Elimination of access to debug points and channels by removing any unnecessary ports
    - Construct the casing in such a way that unauthorized removal of it will irreversibly damage the circuitry. This can be achieved e.g. by using

industrial-grade adhesives and glue to connect the casing to the circuit board.

4.1.1.2 *Bootstrapping*

The starting point of any IoT device security is to imprint a unique and immutable identity into the hardware. This establishes the anchor for the other critical device attributes such as cryptographic keys or other crucial identification properties. The *root of trust* (RoT) is the process that ties the aforementioned attributes with the device operation. In essence, the different phases of loading sequence are tied together with the form of cryptographic hashes, with the previous phase always verifying the next phase. This is accomplished with the steps in the order indicated hereafter:

- Step 1: On power-up, the device is booted from ROM or from another, non-writeable memory area. Within this area, the device identity is contained, as well as a key to the BIOS, which is used for the next loading phase
- Step 2: The BIOS is loaded, and within the BIOS the public key of the OS kernel loader is stored, which is used for the next loading phase
- Step 3: The OS kernel loader is loaded, and within it the public key of the OS image is stored, which is used for the next loading phase.
- Step 4: The OS image is loaded, and within it a hash of the application is stored. Before loading the application, the expected hash is compared with the actual image hash. If they do not match, the application is not loaded.

Most processor vendors such as ARM and Intel supply off-the-shelf RoT solutions which span multiple steps. However, at least for secure loading of the actual business application, some degree of action needs to be taken by the consortium, e.g. specifying the hash of the application. This will be further determined during the implementation phase.

4.1.1.3 *Key Management and Trusted Computing*

As mentioned in the previous section, establishing a trusted execution environment unbreakably linked to the actual device is the cornerstone for secure operation. Within this context, various standards exist with the most popular one being the Trusted Platform Module (TPM) standard. TPM is at its core a discrete piece of hardware with an etched, unremovable secret RSA key added during the production process. The extent of the TPM varies (vendor- and built-specific), and can hold additional keys in order to enable e.g. Root of Trust booting or other encryption functionalities. For this project, suitable vendor solutions will be determined depending on the criticality of the IoT component in question.

4.1.1.4 *Processor and Memory space protection*

The main technologies that will be utilized to protect the CPU and the OS are:

- Non-execution memory areas: Allows the hardware to designate certain memory areas, which verifiably contain legitimate software as addressable by the OS, while other areas are explicitly marked as non-addressable. This way, exploits which aim to point the instruction pointer to malicious code residing in non-trusted memory space are avoided, given that this memory-space cannot be addressed by the OS in the first place. The project will consider using IoT operating systems that support this functionality.

- Address space layout randomization: An OS feature that randomizes memory space on each boot. Using this technique, it becomes significantly harder for an attacker to map out the memory space layout and understand where the execution code is located. For the purposes of the project, appropriate OS patches enabling this functionality (e.g. Linux ASLR [57])

4.1.1.5 *Storage Protection*

There are several cases where IoT devices deployed outside the secure premises of a data center (e.g. IoT nodes, IoT routers/gateways) require persistent storage. In this case, the storage needs to be encrypted. Using keys and algorithms which are part of the device's TPM (see the previous section) is a secure, convenient and especially performant option, although one must consider that in this case the storage module is tied to the device. This may not be an option given that in case the device fails, is destroyed or is stolen, (see previous section on physical security) access to its data is lost (unless a recovery key exists which may not always be provided by the TPM). As a consequence, within this project the level of storage protection of IoT devices needs to be evaluated on a case by case basis, taking also into account the available backup options for the device (e.g. in the form of a scheduled cloud-based back-up). The generally accepted standard for describing storage security and its related policies and procedures is FIPS 140-2 [58]. The four levels of security are:

- Level 1: Software-only encryption provides limited security.
- Level 2: Role-based authentication is required, as well as the ability to detect physical tampering (e.g. via seals or smart switches)
- Level 3: Physical tamper resistance is required. If the device is tampered with, it should be able to erase critical security parameters. Includes also cryptographic protection, key management and identity-based authentication.
- Level 4: The highest form of physical tamper protection, used for uncontrolled, high-risk environment. The entire contents of device should be erased in case of tampering.

Within a large scale smart-city solution, IoT device deployment scenarios for all security levels exist. As a consequence, a trade-off needs to be made between security, operational requirements, administration effort, and device cost-effectiveness.

Another important item to consider is the secure disposal of storage modules once they have reached their end-of-life. In this context, the NIST 800-88 [59] standard will be considered:

- NIST 800-88 provides three ways of dealing with end-of-life data: Clear, Purge and Destroy. These ways differ in the level of data recoverability, with the last option effectively damaging the media to such an extent that it is incapable of storing data again. In addition to data erasure, NIST 800-88 also provides formal processes for verifying that the erasure methods were truly effective.

4.1.2 Authentication

ENISA in the "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures"[51] has issued the following good practices for the establishment of secure and successful authentication processes:

- GP-TM-21: Design the authentication and authorisation schemes (unique per device) based on the system-level threat models.

- GP-TM-22: Ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.
- GP-TM-23: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., on top of certificates.
- GP-TM-24: Authentication credentials shall be salted, hashed and/or encrypted.
- GP-TM-25: Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices.
- GP-TM-26: Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms

4.1.2.1 *Lightweight authentication security mechanisms for smart objects*

In order to overcome the issues brought by the limitations of the devices and the transmission channels, [60] propose a token-based authentication scheme that reduces computation overhead during authentication by using lightweight computation operations like XOR and hash function. LACO [61] is three-factor lightweight authentication designed for e-health systems that uses a biohash function and also implements preservation of privacy, due to the personal data that e-health systems process. [62] have proposed a lightweight algorithm for the integration of industrial IoT devices in future production systems that offers a mechanism responsible for the confidentiality, authentication and robustness against common attack in the world of industrial IoT.

4.1.3 Secure communications

4.1.3.1 *Secure and trusted communications*

According to the "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures"[51] by ENISA, the good practices for securing communications are listed below:

- GP-TM-38: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud, using data encryption methods to minimise network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.
- GP-TM-39: Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.
- GP-TM-40: Ensure credentials are not exposed to internal or external network traffic
- GP-TM-41: Guarantee data authenticity to enable trustable exchanges (from data emission to data reception - both ways). Data is often stored, cached, and processed by several nodes; not just sent from point A to point B. For these reasons, data should always be signed whenever and wherever the data is captured and stored.

- GP-TM-42: Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for trustable solutions and services. For example, a device measures its own integrity as part of boot, but does not validate those measurements - when the device applies to join a network, part of joining involves sending an integrity report for remote validation. If validation fails, the endpoint is diverted to a remediation network for action.
- GP-TM-43: IoT devices should be restrictive rather than permissive in communicating: When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not traverse the firewall.
- GP-TM-44: Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.
- GP-TM-45: Disable specific ports and/or network connections for selective connectivity. If necessary, provide users with guidelines to perform this process in the final implementation.
- GP-TM-46: Rate limiting – controlling the traffic sent or received by a network to reduce the risk of automated attacks.

4.1.3.2 *Secure Interfaces and network services*

According to the "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures" [51] by ENISA, the good practices for securing interfaces and network services are:

- GP-TM-47: Risk Segmentation - Splitting network elements into separate components to help isolate security breaches and minimise overall risk. Networks can be divided into isolated subnetworks to boost performance and improve security
- GP-TM-48: Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set, since smart objects are often deployed as sets of identical or almost identical devices.
- GP-TM-49: Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family.
- GP-TM-50: Ensure only necessary ports are exposed and available.
- GP-TM-51: Implement a DDoS-resistant and Load-Balancing infrastructure to protect the services against DDoS attacks which can affect the device itself or other devices and/or users on the local network or other networks.
- GP-TM-52: Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc

- GP-TM-53: Avoid security issues when designing error messages. An error message should give/display only the concise information the user needs – it must not expose sensitive information that can be exploited by an attacker, such as an error ID, the version of the webserver, etc.

4.1.3.3 *Implementing IoT endpoint security*

Endpoint security greatly depends on the technology used by the IoT device. There are different security implementation when deploying e.g. a Bluetooth device as opposed to a ZigBee or a 802.11 WiFi device. Taking Bluetooth as an indicative example, a list of points to be aware of is as follows:

- Set up device identity and authentication
- Ensure proper BLE security modes (the minimum level providing authenticated pairing with encryption)
- Use the minimum radio signal power for communicating with the host
- If possible, randomize the MAC addresses with Bluetooth privacy features
- Disable any unused Bluetooth
- If possible, pairing should be performed prior to deployment

4.1.3.4 *Implementing Gateway endpoint security*

Similarily to IoT endpoint security, the security of the gateway endpoints depends on the technologies used both for WPAN communication and WAN communication. General points to be aware are:

- Usage of Access Control Lists
- Usage of firewalls and disable any unused ports (for the WAN-facing endpoint)
- Black & Whitelisting of MAC addresses
- Administration / Control of firmware updates
- Avoid unnecessary pairing to minimize Man-In-The-Middle attacks (for the WPAN-facing endpoint)
- Use of IDS, IPS and VPN (for the WAN-facing endpoint)

Specifically for the WAN communications between the gateway and the cloud, the following the transport protocol should be encrypted with TLS 1.2 and proper device authentication needs to be guaranteed (e.g. via SIM in case of a 4G LTE network).

4.1.3.5 *Implementing Cloud endpoint security*

Cloud endpoint security implementation also depends on the technologies used for WAN communication. General things to consider from a security perspective are:

- Always encrypt data at rest and data in motion
- Enforce device identity and authorization, e.g. via the OAuth 2.0 open standard [63]
- Usage of Access Control Lists
- Usage of firewalls and disable any unused ports
- Black & Whitelisting of IP addresses

- Use certificate-based authentication (TLS 1.2)

4.1.3.6 *Software Defined Perimeter*

Software Defined Perimeters (SDPs) can be seen as an overlay network, i.e. a network on top of another network. SDP shares similar concepts with Software Defined Networking (SDN), but instead of dynamically adapting the networking infrastructure according to demand, it emphasizes on securing all connections at all layers, in line with the shifting levels of security defined by the business needs. SDP is particularly attractive for IoT networks, given that at its core it is a means to establishing communication between untrusted parties. The general principle is that connectivity is based on a need-to-know model, where the device is kept uninformed about the infrastructure until is is adequately identified. As the device is kept in the "dark" for as long as it is untrusted, SDP is also referred to as a "black cloud", where the DNS or IP addresses are invisible to outsiders.

In the context of this project, open source[64] implementations of SDP can be considered in order to avoid attacks such as DDOS, Man-In-The-Middle or even scanning of server ports.

4.1.4 Data encryption

4.1.4.1 *Symetric Data Encryption Implementation*

In symmetric encryption, the encryption and decryption keys are identical. The most widely-used symmetric encryption standard is the Advanced Encryption Standard (AES), which is a block-cipher which can use key lengths of 128, 192 and 256 bits. Due to its relatively low memory footprint, AES is well-suited for computationaly less powerful IoT devices and can be used for many use cases such as encrypting data at rest. An important variant of AES is AES-CCM which due to its mode of operation effectively works as a stream cipher, thus making it ideal for applications where the data quantity to be encrypted/decrypted is unknown a priori, such as wireless connections. Its speed and relative simplicity in implementation have made AES-CCM widely popular and it can be found in e.g. the WPA2 encryption algorithm of IEEE 802.11, Bluetooth Low Energy, ZigBee, IPSec and other technologies.

4.1.4.2 *Public Key Cryptography Implementation*

In public-private (or asymmetric) encryption, the encryption and decryption keys are non-identical and generated in pairs. Contrary to symmetric encryption, the encryption key is public and can be used by anyone to encrypt the data. The key to decrypt the data is kept private by the recipient of the data. In addition to data secrecy, Pubic Key cryptography also ensures authentication of the communicating parties as well as non-repuditaion. The most widely-used encryption standards are RSA, Diffie-Hellman and Elliptical Curve Cryptogtraphy (ECC). The latter, being the most recent encryption scheme of the aforementioned three, is considered the most efficient given that it can achieve similar cryptographic strength with considerably smaller key length. According to the NSA, a 256bit ECC key can provide the equivalent security of a 3072bit RSA key, while doubling the length of the ECC key to 512bits offers the equivalent strength of a 15360bit RSA key [65]. This property makes ECC encryption especially attractive for computationaly constrained IoT devices. Within the context of the project, public key cryptography applications will be applied e.g. in securing communications through the TLS or S/MIME protocol.

4.1.4.3 *Cryptographic Hash Implementation*

The defining characteristic of cryptographic hashes is their one-way nature, i.e. when a hash function is applied on the plaintext, the encrypted result is considered impossible to revert back to the clear. This property is especially useful for generating digital signatures and proving data authenticity and integrity. The most prominent hashing standards are the Secure Hash Algorithm (SHA) variants, SHA-2 and most recently SHA-3 variants with usual output sizes of 256 and 512 bits, as well as the older SHA-1 and MD5 algorithms sporting smaller output sizes of 160 and 128 bits respectively. The older hashing algorithms should be avoided due to their proven cryptographic weaknesses and proneness to the collision [66] [67]. Within the context of the project, only SHA-2 variants will be utilized, mainly for validating content authenticity and TLS certificate signing for HTTPS communication channels.

4.1.4.4 *Application of Encryption Mechanisms to the IoT Network*

The following aspects are to be considered for applying encryption in the IoT Network of the project: (adapted from ENISA [51]):

- Device software/firmware, configuration, and applications should be able to update Over-The-Air (OTA), and any files transmitted should use a secure connection and should be signed by an authorised trust entity and encrypted using accepted encryption methods
- Updates should contain a digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.
- Any authentication credentials will be salted, hashed and/or encrypted.
- Data storage at rest should be encrypted
- Confidentiality, integrity, availability and authenticity of the information in transit on the networks or stored in the IoT application or in the Cloud will be guaranteed by using data encryption methods to minimise network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.
- Communication security will be provided using state-of-the-art, standardised security protocols, such as TLS for encryption
- Web interfaces will fully encrypt the user session from the device to the backend services. Where applicable, care should be taken to ensure that endpoints are not susceptible to XSS, CSRF, SQL injection and similar endpoint attacks.

4.2 How to apply Privacy

Privacy in order to be effective should be applied by design or default.

The relevant policies and procedures need to be developed and implemented at design stage. These include:

- Data protectection policy
- Cookies policy
- Concent Procedure
- Assignment of a Data Protection Officer
- Data Subject Request Procedure

- Data Subject Request Response Procedure
- Incident Management Procedure
- Data Protection Risk Assessment
- Data Protection Impact Assessment (DPIA)
- Data Flow Mapping

Initially, the PACT should be completed by all consortium members regarding their assigned tasks within this project. As a result, a review of all PACT inputs will be reviewed by the Ethics Committee and actions assigned to the relevant parties. These will be reviewed once again upon completion by the Ethics Committee and finalized as policies and procedures.

Following this assessment, the consortium will be in a position to utilize and extend Privacy Enhancing Technologies (PET) to meet goals identified in the planning phase. These will include, but not limited to:

- Design of cryptographic integrity and authenticity preserving mechanisms; and,
- Implementation of data anonymization/pseudonymization techniques.

5 CRSP Patterns

IDEAL-CITIES will develop support for the design and operational management of IoTPS applications that make use of the IDEAL-CITIES runtime platform in ways that can verifiably preserve required resilience, security, data integrity, confidentiality and privacy properties, and govern the three underlying attributes enabling circularity: location, condition, and availability.

The key approach underpinning the development of this support will be the use of Circularity, Resilience, Security and Privacy (CRSP) patterns.

CRSP patterns will be designed so that to be able to:

- provide abstract specifications of compositional structures of IoTPS applications, which are proven to preserve certain composition level of the above-mentioned properties if the services/components that are composed according to the pattern satisfy other atomic level properties, and
- support both the design and operational management of IoTPS applications.

Application Manager is the main component of the IoTPS application backend, which serves as the runtime environment for the various IoTPS application profiles and contains the execution engine for the CRSP patterns.

As a design tool, CRSP patterns will be used to:

a) generate designs of compositional structures of software services/components within a IoTPS application that can guarantee required resilience, security and privacy properties based on the aforementioned security circularity, resilience, security or privacy properties.

At runtime, CRSP patterns will be used to:

b) specify the properties of individual IoTPS application services and components and other operational conditions that will be necessary to monitor in order to ensure that global IoTPS application security, circularity and privacy properties are preserved, and

c) generate possible adaptations of services/components of IoTPS applications that become unavailable, faulty or fail to satisfy the conditions required of them.

This section defines the Pattern Language. Overall, this language:

- provides constructs for expressing/encoding dependencies between CRSP properties at the component and at the composition/orchestration level.
- is structural; It does not prescribe exactly how the functions should be executed nor, e.g., how the ports ensure communication.
- Supports the static and dynamic verification of CRSP properties.

Patterns expressed in this language will enable the pattern-based IoT application management process followed in IDEAL-CITIES, in which patterns are used to

- design IoT applications that satisfy required CRSP properties
- verify that existing IoT applications satisfy required CRSP properties at design time, prior to the deployment of the application

- enable the adaptation of IoT applications or partial orchestrations of components within them at runtime in a manner that guarantees the satisfaction of required CRSP properties

To fulfil the above, CRSP patterns encode proven dependencies between security, privacy, dependability and interoperability (SPDI) properties of individual components of IoT applications and corresponding properties of orchestrations of such components. More specifically, a pattern encodes relationships of the form

$$P_1 \text{ and } P_2 \text{ and } \ldots \text{ and } P_n \rightarrow P_{n+1}$$

where P_i (i=1,…,n) are properties of individual components and P_{n+1} is a property of the orchestration of these components. The relation encoded by a pattern is an entailment relation.

The runtime adaptations that can be enabled by CRSP patterns may take three forms:

(1) to replace particular components of an orchestration
(2) to change the structure of an orchestration, and
(3) a combination of (1) and (2).

5.1 Pattern Rules

This section presents the first set of IDEAL-CITIES pattern rules, using the language and associated constructs. The Security properties of Confidentiality and Integrity are analysed separately in the corresponding subsections below, as different types of property reasoning and monitoring conditions need to be defined for each one of them.

5.1.1 Security

5.1.1.1 *Confidentiality*

Pattern definition

The preservation of Confidentiality requires that the disclosure of information happens only in an authorised manner; i.e. non-authorised access to information should not be possible. Formal definitions of Confidentiality are typically based on the concept of Information Flow (IF), separating users in classes with different access rights to the system's information and distinguishing the information flows within the system according to the user classes they should be accessible to. Based on this concept, the *Perfect Security Property (PSP)* requires low-level users (i.e. a user with restricted access, in contrast to high-level users having full access) who are only allowed to view public information, should not be able to determine anything concerning high-level (confidential) information.

A *sequential orchestration* ***P*** with two activity placeholders, ***A*** and ***B***, whereby *B* is executed after *A*, is depicted in Figure 5. We assume that for each *x* in *{P, A, B}* the following hold:

- IN^x and OUT^x are the sets of inputs and outputs of x, and $E^x = IN^x \cup OUT^x$;
- V^x and C^X are two disjoint subsets of E^x, portioning into public parts and confidential parts respectively.

Further conditions that define P, as depicted in Figure 5, include:

- The inputs of A are the inputs of the workflow P
- The inputs of B are the outputs of A

- The outputs of the orchestration P are the outputs of B

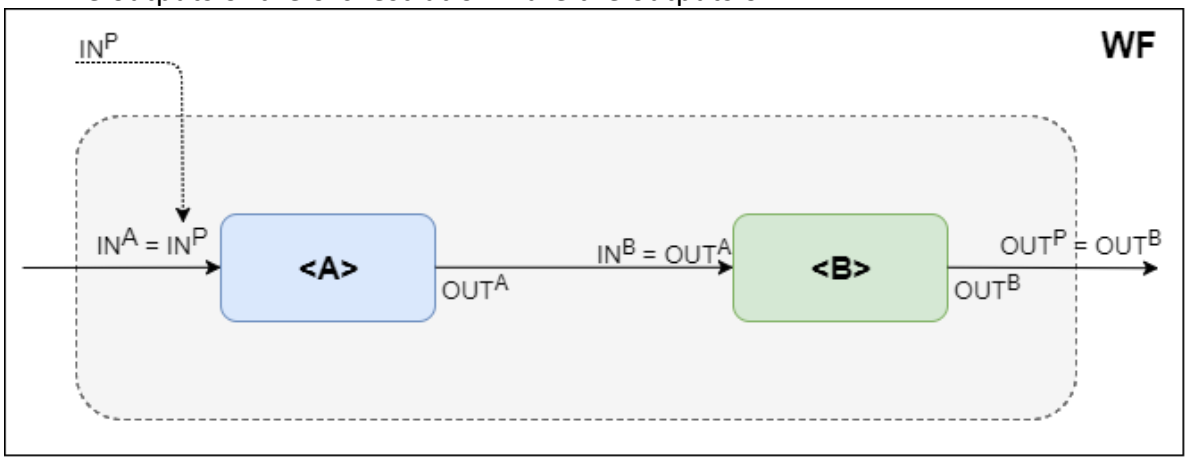


Figure 5 PSP on a Sequential Service ORCHESTRATION

Based on the above, the SPDI pattern for preserving PSP (i.e. confidentiality) on the service orchestration P can be defined as follows:

i. NP:

a. $PSP(A,\ V^A,\ C^A)\ and\ V^A \subseteq V^P\ and\ C^A \cap V^P = \emptyset$

b. $PSP(B,\ V^B,\ C^B)\ and\ V^B \subseteq V^P\ and\ C^B \cap V^P = \emptyset$

ii. OP:

a. $SecReq^P = PSP(P,\ V^P,\ C^P)$

Interpreting the pattern above, PSP holds on the orchestration ***P*** if, for all activity placeholders *x* in *{A, B}*, the following are true:

a) $V^X \subseteq V^P$; i.e. the actions of *x* that reveal public information are part of the actions of P that reveal public information, and

b) $C^X \cap V^P = \emptyset$; i.e. the actions of *x* that reveal confidential information do not include any action of P that reveal public information.

The above conditions are expressed as normal properties *NP* of the pattern and entail the PSP property on P, as expressed in the output property *OP* part of the pattern.

Pattern specification rule

Based on the above, the confidentiality (PSP) pattern defined in above subsection can be represented in Drools as shown in Table 9.

The **when** part of the rule specifies:

- the two activity placeholders A and B of the PSP pattern (variables $A and $B on lines 3-4 and 5-6);
- the order in which $A and $B are executed (variable $ORCH on line 7) and the conditions between the outputs of $A, and the inputs of $B as required by the PSP pattern (lines 7-9), and;
- the OP property that can be guaranteed by applying the pattern, i.e. the PSP property in this case (variable $WP in lines 10-11). Lines 3-9 are the specification of the ORCH part of the pattern.

The **then** part of the rule generates a security plan that includes the NP security properties that (if satisfied by the activity placeholders that will be selected for the pattern's ORCH)

```
1. rule "PSP on Cascade"
2. when
3.   $A: Placeholder($input : operation.inputs,
4.     $intData : parameters.outputs)
5.   $B: Placeholder(parameters.inputs == $intData,
6.     $output : parameters.outputs)
7.   $ORCH: Sequence(parameters.inputs == $inputs,
8.     parameters.outputs == $outputs,
9.     firstActivity == $A, secondActivity == $B)
10.    $OP: Property( propertyName == "PSP",
11.      subject == $ORCH, satisfied == false)
12.    $SP: PropertyPlan (properties contains $OP)
13.  then
14.    PropertyPlan newPropertyPlan = new newPropertyPlan
   ($SP);
15.    newPropertyPlan.removeProperty($OP);
16.    Set V_P = $OP.getAttributesMap().get("V");
17.    Property NP_A = new Property($OP, "PSP", $A);
18.    NP_A.getAttributesMap().put("V", new
   Operation("subset", V_P));
19.    NP_A.getAttributesMap().put("C", new
   Operation("subset", new    Operation("complement",V_P)));
20.    newPropertyPlan.getProperty().add(NP_A);
21.    insert(NP_A);
22.    Property NP_B = new Property($OP, "PSP", $B);
```

Table 9 Specification of PSP property via Drools

would lead to a ORCH satisfying the OP (i.e. the PSP property). Based on the proof of the PSP property detailed earlier in this document, both of the placeholders A and B should satisfy the PSP property; thus, PSP is defined as the NP property that both placeholders should satisfy in lines 17 and 22, respectively. Moreover, the additional conditions defined earlier (i.e. $V^A \subseteq V^P$ *and* $C^A \cap V^P = \emptyset$ for placeholder A and $V^B \subseteq V^P$ *and* $C^B \cap V^P = \emptyset$ for B) are also added to the corresponding NPs, as can be seen in lines 18-19 and 23-24, respectively.

5.1.1.2 *Integrity*

Pattern definition

Data Integrity refers to the maintenance and assurance of the accuracy and consistency of data. Following the definition in 5.1.1.1, a *sequential orchestration* ***P*** with two activity placeholders, ***A*** and ***B***, whereby *B* is executed after *A*, is depicted in Figure 5. We assume that for each *x* in *{P, A, B}* the following hold:

- IN^x and OUT^x are the sets of inputs and outputs of *x*
- $D^x(i)$ the data of x at the given time t
- Hash(i) are the cryptographic hash function result applied to data i

Further conditions that define P, as depicted in Figure 5, include:

- The inputs of A are the inputs of the orchestration P
- The inputs of B are the outputs of A
- The outputs of the orchestration P are the outputs of B

Based on the above, a pattern for preserving integrity for data that are at in processing and in transit on the service orchestration P can be defined as follows:

- $Hash(IN^P)=Hash(IN^A)$
- $Hash(OUT^P)=Hash(OUT^B)$
- $Hash(IN^B)=Hash(OUT^A)$

Interpreting the pattern above, the data that an activity A sends to activity B are not by any chance changed . The data in check are not only the transmitted through datalinks but also through inter process communication.

Moreover, based on the above specification we can define a generic pattern for integrity at data at rest as follows:

$$Hash(D^x(i))=Hash(D^x(i-1)$$

Which means that whenever we check data at rest those data must not be changed.

Pattern specification rule

The specification rule of the above patterns in Drools is shown in Table 10 and Table 11, respectively. Specifically, for the Integrity At Rest rule (Table 11), it specifies the data of the activity that are we check at line 3. Then in line 4 we define a special activity that becomes true every n seconds and forces the Drools engine to run the **then** part of the rule. At line 12

```
1. rule "Integrity"
2. when
3.   $A: Placeholder($input : operation.inputs,
4.     $intData : parameters.outputs)
5.   $B: Placeholder(parameters.inputs == $intData,
6.     $output : parameters.outputs)
7.   $ORCH: Link(firstActivity == $A, secondActivity == $B)
8.   $OP: Req( propertyName == "Integrity",
9.     subject == $ORCH, satisfied == false)
10.    $SP: PropertyPlan (properties contains $OP)
11.  then
12.    PropertyPlan newPropertyPlan = new
   PropertyPlan($SP);
13.    newPropertyPlan.removeRequirement($OP);
14.    Req Hash1 = new Req($OP,
   "equality",sha512($A.input),sha512(operation.input));
15.    newPropertyPlan.getProperties().add(Hash1);
16.    insert(Hash1);
17.    Req Hash2 = new Req($OP,
   "equality",sha512($A.output),sha512($B.inputs));
18.    newPropertyPlan.getProperties().add(Hash2);
19.    insert(Hash2);
```

Table 10 Specification of Integrity property via Drools

```
1. rule "IntegrityAtRest"
2. when
3.   $A: Placeholder($intData : datastore.Data)
4.   $T: Timer(time.Interval("Default time interval"))
5.   $ORCH: Check(firstActivity == $A, secondActivity == $T)
6.   $OP: Req( propertyName == "Integrity",
7.     subject == $ORCH, satisfied == false)
8.   $SP: PropertyPlan (properties contains $OP)
9. then
10.     PropertyPlan newPropertyPlan = new
   PropertyPlan($SP);
11.     newPropertyPlan.removeRequirement($OP);
12.     Req Hash1 = new Req($OP,
   "equality",sha512(&intData),datastore.StoredHash($A));
```

Table 11 Specification of Integrity at Rest property via Drools

we calculate the hash ckecksum of the data and we retrieve the checksum that it is already strored and those must be true since the data are at rest.

5.1.2 Privacy

5.1.2.1 *Pattern Definition*

5.1.2.1.1 Consent

Due to GDPR constrains, patterns should be developed in order for Ideal-Cities to be GDPR compliant. One of the constrains that need to be considered is for the user to give consent on their data to be used.

On a simple service composition as the below depicted on Figure 6, we make the following assumptions

- IN^A and OUT^A are the sets of inputs and outputs of *A*
- D^x Are the data which belong to owner X
- C is a set of users who have agreed their data can be processed and stored

Figure 6. Privacy on a simple service composition

Then in order to be able to able to create every service composition the following pattern should be applied

$$IN^P = D^A \text{ where } A \subseteq C$$

This means that for every service composition we must first check that the data owners have agreed that their data can be processed by this composition.

5.1.2.1.2 Identifiability

In order to guarantee privacy, checking the components that form the service is not enough; their composition should also be checked for privacy. At each layer of composition, the data union that the layer produces should be evaluated. As an example, consider the composition of a service of two components.

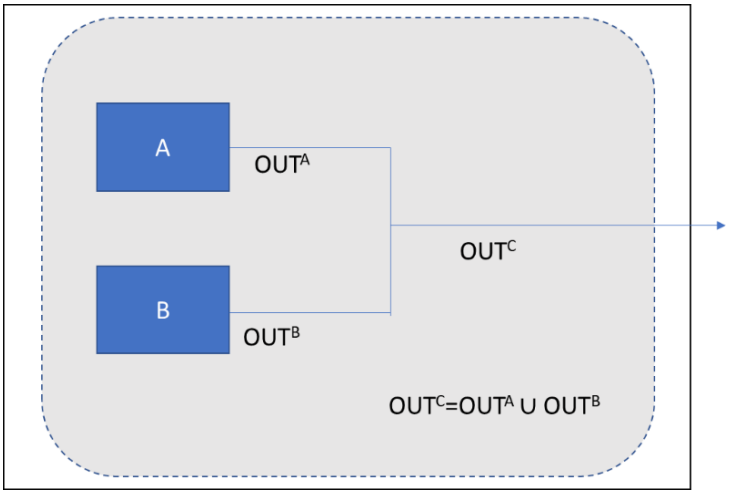


Figure 7. Privacy pattern example

Let us assume that for each *x* in *{A, B, C}*

- OUT^X are the sets of outputs of x
- IN^X are the sets of inputs of x
- $E^X=IN^X \cup OUT^X$
- V^X and C^X are two disjoint subsets of E^X which partition it into public parts V^X and confidential parts C^X
- L is a corpus of sets that are pre-defined that expose privacy

Then in order for the composition to satisfy the privacy requirements, the following properties must hold:

a. $V^A \cap L = \varnothing$
b. $V^B \cap L = \varnothing$
c. $V^C \cap L = \varnothing$

Moreover, when data are at rest (i.e. in storage) we should take precautions that:

d. $(V^A \cup V^B \cup V^C) \cap L = \varnothing$

Still, the following properties should also hold:

a. $(V^A \cup V^B) \subseteq V^C$
b. $(V^A \cup V^B) \cap C^C = \varnothing$

As an example, let us assume that there are two components *A* and *B* that we want to use to create a service *C*. Moreover, a set *L* that exposes users privacy is *L={(name, location), (name,*

medical_condition)}; i.e., we do not want a service that exposes a person's name along with her location and/or her medical conditions.

Component *A* publicly sends the user's ID, environmental temperature and location, while component *B* publicly sends the user's name, user's ID and the humidity of the environment.

In this case, *Req(A, Privacy)* is validated as True (since $OUT^A \cap L = \varnothing$), and also *Req(B, Privacy)* is validated as True (since $OUT^B \cap L = \varnothing$).

Nevertheless, the composition of *A* and *B* to form *C,* as in Figure 7, creates:

$$OUT^C = OUT^A \cup OUT^B = \{userID, temperature, location, UserName, humidity\}$$

This means that $OUT^C \cap L = \{name, location\}$, which is not empty; thus, the composition of those 2 services is not viable, as it violates the privacy pattern rule and creates a privacy leak.

5.1.2.2 *Pattern specification rule*

5.1.2.2.1 Consent

A representation of our pattern in our language can be defined as:

0. **ORCH "Consent"**
1. Activity(_a)
2. AP_1("UserConsensus",_a, pattern)
3. OP(GDPR_Consensus, subject == "Consent", satisfied == false)
4. **Pattern rule: AP_1 ➔ OP**

1. **ORCH "Consent"**
2. Placeholder (A1, (PlaceholderActivity, PlaceholderDescription))
3. Property (UserConsensus, A1, required, (pattern-based, pattern), ?, at_rest)
4. Property (GDPRConsensus, "Consent", required, (pattern-based, PR1), ?, end_to_end)
5. **Pattern rule (PR1: UserConsensus -> GDPRConsensus**

This pattern can be then translated to a Drools engine compatible pattern as the following:

```
1. rule "Consent"
2. when
3.   $A: Placeholder($input : operation.inputs,
   $output:operation.output)
4.   $ORCH: Single(parameters.inputs == $input,
5.     parameters.outputs == $output)
6.   $OP: Property( propertyName == "UserConsenus",
7.     subject == $ORCH, satisfied == false)
8.   $SP: PropertyPlan(properties contains $OP)
9. then
10.    PropertyPlan newPropertyPlan = new PropertyPlan
   ($SP);
```

Table 12 Specification of GDPR Consent via Drools

5.1.2.2.2 Identifiability

Following a similar approach, the pattern definition on our language could be:

0. **ORCH "Identifiability"**
1. Merge(_a,_b)
2. Activity(_a)
3. Activity(_b)
4. AP_1("Identifiability",_a, certificate)
5. AP_2("Identifiability",_b, certificate)
6. AP_3("Identifiability",dataMerge(_a,_b), patern)
7. OP(Identifiability, subject == "Identifiability", satisfied == false)
8. **Pattern rule: AP_1,AP_2,AP_3 ➔ OP**

1. **ORCH "Identifiability"**
2. Merge (A1, A2)
3. Placeholder (A1, (PlaceholderActivity, PlaceholderDescription))
4. Placeholder (A2, (PlaceholderActivity, PlaceholderDescription))
5. Link (L1, A1, A2)
6. Property (Identifiability1, A1, required, (certificate, interface), ?, in_processing)
7. Property (Identifiability2, L1, required, (pattern-based, pattern), ?, in_processing)
8. Property (Identifiability3, A2, required, (certificate, interface), ?, in_processing)
9. Property (Identifiability4, "Identifiability", required, (pattern-based, PR1), ?, end_to_end)
10. **Pattern rule: (PR1: Identifiability1, Identifiability4, Identifiability3 ➔ Identifiability4)**

This pattern can be then translated to a Drools engine compatible pattern as the following:

```
1. rule "Identifiability"
2. when
3.   $A: Placeholder($output_A: Activity.output)
4.   $B: Placeholder($output_B: Activity.output)
5.   $ORCH: Merge($A, $B)
6.   $OP: Property( propertyName == "Identifiability",
7.     subject == $ORCH, satisfied == false)
8.   $SP: PropertyPlan(propeties contains $OP)
9. then
10.     PropertyPlan newPropertyPlan = new
   PropertyPlan($SP);
11.   newPropertyPlan.removeProperty($OP);
12.   Property NP_A = new Property($OP,
   "Identifiability", $A);
13.   Property NP_B = new Property($OP,
```

Table 13 Specification of GDPR Identifiability via Drools

6 Security Policy

6.1 Description and Purpose of Security Policy

Ideal Cities recognises the need to ensure that its operations should run smoothly and without interruption for the benefit of users. In order to provide such a level of continuous operation, Ideal Cities recognizes that Security controls have to be implemented and applied based on the risks identified, the controls that need to be added, specific frameworks and best practises, in order to satisfy the security requirements applied. This will help the continuous improvement and effectiveness of the Ideal Cities and promotes the achievement of the objectives and targets, considering input of the personnel at different levels.

6.2 Scope of the Information Security Policy

The policy relates to all activities undertaken by Ideal Cities users, outsourced personnel and collaborators subcontracted by Ideal Cities and all related facilities. Ideal Cities implements and manages Security Policy, forming the basis and mandatory approaches to all Security concerns, promoting the risk-based thinking and considering the strategic direction and context of Ideal Cities.

6.3 Policy Statement

Ideal Cities establishes and ensures that, the objectives and intentions framed, are expressed and communicated appropriately within and out of the Ideal Cities, supporting the strategic direction.

Ideal Cities understands the external and internal security issues that may affect the performance of the IDEAL-CITIES platform either negatively or positively and understand the needs and expectations of all related users. It also understands, evaluates and addresses risks and exploits the opportunities that affect the Ideal Cities' performance and strengthens leadership and commitment towards the protection of security within Ideal Cities.

Ideal Cities is committed to satisfying the applicable requirements including legal requirements and other requirements, needs and expectations of the relevant parties, taking into consideration the relevant statutory and regulatory requirements related. Ideal Cities is committed to the continual improvement of the Security, considering and understanding the external and internal issues that may affect the performance and strategy of Ideal Cities. Ideal Cities, is committed to eliminating or reducing Security Incidents and Security Risks giving great effort to the constant availability and provision of resources needed to meet intended results in relation with the potential contributions of relevant interested parties.

In relation with the risk-based thinking approach and the determination, consideration and control of the risks, Ideal Cities is committed to deliver Security externds to all levels, which will be demonstrated through this Security Policy, and the provision of appropriate resources to establish and develop the relevant controls and requirements.

Adopters of the Ideal Cities platform should ensure that a systematic review of performance of the Ideal Cities is conducted on a regular basis to ensure that security objectives are being met and security issues are identified through the audit programme and process.

A risk management strategy and process will be used, and risk management will take place at several levels, including:

- Risks to the achievement of objectives

- Security Risk Assessments
- Assessment of the risk of changes as part of the Change Management Process
- At the project level as part of the management of significant changes

Ideal Cities would encourage all related parties, including users and application, to ensure that they play their part in delivering the Security objectives.

7 Future work and Conclusion

7.1 Future work

Trust, security and resiliency are continuously evolving and maturing in the context of smart, responsive cities. In conjunction with D.2.1, the problem domain is security in Socio Technical and Cyber Physical systems. As such, topics for further investigation and development are as follows:

Assess the appropriateness and suitability of risk assessment frameworks for Cyber Physical Systems. Current risk assessment focuses on either cyber or physical systems, but do not consider wider attack surfaces. Therefore, existing frameworks may not be suitable for CPS.

Against the previous point, the set of goals will net to be widened to include both cyber and physical domains. For example, cyber security concerns Confidentiality, Integrity and Availability, whereas the physical domain requires the introduction of safety and resiliency. Hence, further research and development of a unified framework is needed.

Circularity patterns will need to be aligned with the more mature security and resiliency patterns. Circularity will require the reuse and repurposing of the collected data in potentially unprecedented manners. The underlying privacy framework (such as PACT which is used in this project), will need to be extensively tested in a data-driven CE enabled testbed in order to fully evaluate it and establish if it is fit for purpose.

In relation to the previous point, the taxonomy of the data produced and consumed in a smart city environment will also need to be established and agreed upon. This activity will be completed in WP4.

7.2 Conclusion

The goal of Smart Cities is to create a helpful and fruitful environment for citizens and visitors, providing facilities that will make their lifes easier. In order for these goals to be achieved the usage of higly advanced integrated technologies should be adopted. Some examples of these technologies include IoT networks, Big Data, Robotics, Machine Learning, etc. These technologies facilitate the main goals of a smart city concept.

However, these ICT technologies are followed by many security, privacy and trust issues and challenges as the interaction between various smart objects and different networks can be complicated due to the vulnerabilities and threats identified in a smart city context . This aggravating landscape can constitute high risk for citizens, visitors, critical infrastructures, and assets of a smart city.

In this context, the IDEAL-CITIES project defines the security, privacy and resilience challenges, the IoT threats and vulnerabilities, the security and privacy requirements for the IDEAL-CITIES platform, how security, privacy and resilience by design concepts can be adopted in the future, smart, urban environments, in compliance with the GDPR.

To conclude with, the main goal of the design and application of all the aforementioned is the facilitation of the human factor, due to the fact that they are destined for the improvement of the daily urban life.

8 References

[1] Khatoun, Rida, and Sherali Zeadally. "Cybersecurity and privacy solutions in smart cities." IEEE Communications Magazine 55.3 (2017): 51-59.

[2] A. Balte, A. Kashid and B. Patil, “Security Issues in Internet of Things (IoT): A Survey,” International Journal of Advanced Research in Computer Science and Software Enginering, pp. 450-455, 2015.

[3] S. Ijaz, M. A. Shah, A. Khan and M. Ahmed, “Smart Cities: A Survey on Security Concerns,” International Journal of Advanced Computer Science and Applications, pp. 612-625, 2016.

[4] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris and D. Barthel, “Security and Privacy in your Smart City,” Catalunya.

[5] K. Zhang, J. Ni, K. Yang, X. Liang, L. Ren and X. (. Shen, “Security and Privacy in Smart City Applications: Challenges and Solutions,” IEEE Communications Magazine, pp. 122-129, January 2017.

[6] S. M. Hussein, M. J. Donahoo and T. Cerny, “Security Challenges in Smart City Application,” in International Conference Security and Management, 2018.

[7] I. Andrea, C. Chrysostomou and G. Hadjichristofi, “Internet of Things: Security Vulnerabilities and Challenges,” The 3rd IEEE ISCC 2015 International Workshop on Smart City and Ubiquitous Computing Applications, pp. 180-187, 2015.

[8] Z. A. Baig, P. Szeqczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sensurooah, N. Syed and M. Peacock, “Future challenges for smart cities: Cyber-security and digital forensics,” Digital Investigation, pp. 3-13, 2017.

[9] H. He, C. Maple, T. Watson, A. Tiwari, J. Mehnen, Y. Jin and B. Gabrys, “The Security Challenges in the IoT enabled Cyber-Physical Systems and Opportunities for Evolutionary Computing & Other Computational Intelligence,” IEEE Congress on Evolutionary Computation (CEC), pp. 1015-1021, 2016.

[10] J.-M. Bohli, P. Langendorfer and A. F. Skarmeta, “Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities,” in Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, 2013.

[11] N. C. G. “EU Coordinated risk assessment of the cybersecurity of 5G networks,” 2019.

[12] https://www.owasp.org/index.php/OWASP_Guide_Project

[13] Apthorpe, N., Reisman, D. and Feamster, N., 2016. A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic, Workshop on Data and Algorithmic Transparency (DAT), New York, USA, 19 November.

[14] Bekara, C., 2014. Security issues and challenges for the IoT-based smart grid, International Workshop on Communicating Objects and Machine to Machine for Mission-Critical Applications (COMMCA), Procedia Computer Science, Elsevier, vol. 34, issue 2014, pp. 532-537.

[15] Betts, D., Street, C. and Diogenes, Y., 2018. Internet of Things security architecture. Microsoft Azure documentation. Available on-line: https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-architecture

[16] Chen, Z., Xia, F., Huang, T., Bu, F. and Wang, H., 2013. A localization method for the Internet of Things, The Journal of Supercomputing, Springer, vol. 63, issue 3, pp. 657-674.

[17] Buchanan, W. J., Kwecka, Z. and Ekonomou, E., 2013. A privacy preserving method using privacy enhancing techniques for location based services, Mobile Networks and Applications, vol. 18, issue 5, pp. 728-737.

[18] Moque, C., Pomares, A. and Gonzalez, R., 2012. AnonymousData.co: a proposal for interactive anonymization of electronic medical records, Procedia Technology, Elsevier, vol. 5, issue 2012, pp. 743-752.

[19] Yamaguchi, R. S., Hirota, K., Hamada, K. and Takahashi, K., 2012. Applicability of existing anonymization methods to large location history data in urban travel, IEEE International Conference on Systems, Man, and Cybernetics, IEEE, 14-17 October, COEX, Seoul, Korea, pp. 997-1004.

[20] Niu, B., Zhu, X., Li, Q., Chen, J. and Li, H., 2015. A novel attack to spatial cloaking schemes in location-based services, Future Generation Computer Systems, Elsevier, vol. 49, issue 2015, pp. 125-132.

[21] Ullah, I. and Shah, M. A., 2016. A novel model for preserving location privacy in Internet of Things, 22nd International Conference on Automation and Computing (ICAC), IEEE, 7-8 September, Colchester, UK, pp. 1-6.

[22] Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H. and Liao, D., 2017. Efficient location privacy algorithm for Internet of Things (IoT) services and applications, Journal of Network and Computer Applications, Elsevier, vol. 89, issue 2017, pp. 3-13.

[23] Yu, R., Bai, Z., Yang, L., Wang, P., Move, O. A. and Liu, Y., 2016. A location cloaking algorithm based on combinatorial optimization for location-based services in 5G networks, IEEE Access, Special Section on Green Communications and Networking for 5G Wireless, IEEE, vol. 4, issue 2016, pp. 6515-6527.

[24] Alcaide, A., Palomar, E., Montero-Castillo, J. and Ribagorda, A., 2013. Anonymous authentication for privacy-preserving IoT target-driven applications, Computers & Security, Elsevier, vol. 37, issue September 2013, pp. 111-123.

[25] Alpár, G., Batina, L., Batten, L., Moonsamy, V., Krasnova, A., Guellier, A. and Natgunanathan, I., 2016, May. New directions in IoT privacy using attribute-based authentication. In *Proceedings of the ACM International Conference on Computing Frontiers* (pp. 461-466). ACM

[26] Deshmukh, R. V. and Devadkar, K. K., 2015. Understanding DDoS attack & its effect in cloud environment. Procedia Computer Science. Elsevier Masson SAS, 49(1), pp. 202–210.European Parliament, 2016. Regulation (EU) 2016/679, European Union. Available on-line: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[27] Fernandes, D. A. B. et al., 2014. Security issues in cloud environments: a survey. International Journal of Information Security, 13(2), pp. 113–170.

[28] R. Meulen, “Gartner says 8.4 billion connected “things” will be in use in 2017, up 31 percent from 2016, Gartner.,” 2017. [Online]. Available: https://www.gartner.com/newsroom/id/3598917.

[29] Ronen, E. and Shamir, A., 2016. Extended functionality attack on IoT devices: The case of smart lights, IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, Saarbrucken, Germany, 21-24 March 2016.

[30] Hatzivasilis, G., Fysarakis, K., Soultatos, O., Askoxylakis, I., Papaefstathiou, I. and Demetriou, G., 2018. The Industrial Internet of Things as an enabler for a Circular Economy Hy-LP: a novel IIoT protocol, evaluated on a Wind Park's SDN/NFV-enabled 5G Industrial Network. Computer Communications, Elsevier, vol. 119, pp. 127-137.

[31] Hatzivasilis, G., Papaefstathiou, I. and Manifavas, C., 2016. Software security, privacy and dependability: metrics and measurement. IEEE Software, IEEE, vol. 33, issue 4, pp. 46-54.

[32] Hashizume, K., Yoshioka, N. and Fernandez, E. B., 2011. Three Misuse Patterns for Cloud Computing. Security Engineering for Cloud Computing, pp. 36–53.

[33] Jansen, W. and Grance, T., 2011. Guidelines on Security and Privacy in Public Cloud Computing. Director, 144(7), pp. 800–144.

[34] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W., 2017. A survey of Internet of Things: architecture, enabling technologies, security and privacy, and applications, IEEE Internet of Things Journal, IEEE, vol. 4, no. 5, pp. 1125-1142.

[35] Nawir, M., Amir, A., Yaakob, N. and Lynn, O. B., 2013. Internet of Things (IoT): taxonomy of security attacks, 3rd International Conference on Electronic Design (ICED), IEEE, Phuket, Thailand, 11-12 August 2016, pp. 321-326.

[36] IBM, 2018. About Watson IoT Platform. IBM Cloud Docs. Available on-line: https://console.bluemix.net/docs/services/IoT/iotplatform_overview.html#about_iotplatform

[37] Kocher, P. et al., 2018. Spectre Attacks: Exploiting Speculative Execution. Available at: http://arxiv.org/abs/1801.01203.

[38] Lipp, M. et al., 2018. Meltdown. Available at: http://arxiv.org/abs/1801.01207.

[39] Wojtczuk, R. and Rutkowska, J., 2009. Attacking Intel Trusted Execution Technology. Bios, pp. 1–6. Available at: http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf%5Cnhttp://digitalpiglet.org/teaching/stonybrook/CSE509.2012.F/Attacking.Intel.TXT-slides.pdf.

[40] Rajendran, P. K., Muthukumar, B. and Nagarajan, G., 2015. Hybrid intrusion detection system for private cloud: A systematic approach. Procedia Computer Science. Elsevier Masson SAS, 48(C), pp. 325–329.

[41] Avizienis, A., Laprie, J.C., Randell, B. and Landwehr, C., 2004. Basic concepts and taxonomy of dependable and secure computing. IEEE transactions on dependable and secure computing, 1(1), pp.11-33.

[42] Gruss, D. et al., 2017. KASLR is dead: Long live KASLR. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10379 LNCS, pp. 161–176.

[43] Mehrdad, S., Mousavian, S., Madraki, G. and Dvorkin, Y., 2018. Cyber-physical resilience of electrical power systems against malicious attacks: A review. Current Sustainable/Renewable Energy Reports, 5(1), pp.14-22.

[44] Ratasich, D., Khalid, F., Geissler, F., Grosu, R., Shafique, M. and Bartocci, E., 2019. A roadmap toward the resilient internet of things for cyber-physical systems. IEEE Access, 7, pp.13260-13283.

[45] Tomiyama, T. and Moyen, F., 2018. Resilient architecture for cyber-physical production systems. CIRP Annals, 67(1), pp.161-164.

[46] Wang, Y., 2018. Trust quantification for networked cyber-physical systems. IEEE Internet of Things Journal, 5(3), pp.2055-2070.

[47] Henriksen-Bulmer, J., 2019. Incorporating contextual integrity into privacy decision making: a risk based approach. Doctoral Thesis (Doctoral). Bournemouth University. Available at: http://eprints.bournemouth.ac.uk/32385/?fbclid=IwAR1-Abj82XBfGoz1XErAy6WJEUH0-tq5C8NBHfpKmk6r_heMRkPhsMeWLEg

[48] https://readwrite.com/2016/10/22/the-internet-of-things-was-used-in-fridays-ddos-attack-pl4/

[49] https://www.cs.mun.ca/courses/cs6910/IoT-Survey-Atzori-2010.pdf

[50] https://www.researchgate.net/publication/322202119_Analysis_of_authentication_techniques_in_Internet_of_Things_IoT

[51] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[52] https://eugdpr.org

[53] https://arx.deidentifier.org

[54] M. K. Reiter and A. D. Rubin, “Crowds: anonymity for Web transactions,” ACM Transactions on Information and System Security, vol. 1, no. 1, pp. 66–92

[55] J. Sliwa, “A generalized framework for multi-party data exchange for IoT systems,” in Proceedings of the 30th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2016, pp. 193–198, Switzerland, March 2016

[56] I. D. Addo, P. Madiraju, S. I. Ahamed, and W. C. Chu, “Privacy Preservation in Affect-Driven Personalization,” in Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference, COMPSAC 2016, pp. 400–405, USA, June 2016

[57] https://docs.oracle.com/cd/E37670_01/E36387/html/ol_aslr_sec.html

[58] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[59] https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization

[60] https://ieeexplore.ieee.org/document/8651825

[61] https://www.sciencedirect.com/science/article/pii/S0167739X18331297

[62] https://ieeexplore.ieee.org/abstract/document/8006209

[63] https://oauth.net

[64] https://www.waverleylabs.com/open-source-sdp/

[65] National Security Agency. "The Case for Elliptic Curve Cryptography," www.nsa.gov/business/programs/elliptic_curve.shtml. 2009

[66] https://eprint.iacr.org/2013/170.pdf

[67] https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html