On the Effects of Forced Trust on Implementations of Small Smart Cities

Master of Science in Technology Thesis
University of Turku
Department of Future Technologies
Security of Networked Systems
March 2020
Lauri Halla-aho

Supervisor:
D.Sc. (Tech) Antti Hakkala
D.Sc. (Tech) Seppo Virtanen

UNIVERSITY OF TURKU
Department of Future Technologies

LAURI HALLA-AHO: On the Effects of Forced Trust on Implementations of Small Smart Cities

Master of Science in Technology Thesis, 85 p.
Security of Networked Systems
March 2020

As an increasing number of cities pursue the idea of becoming smart cities, the variety in different approaches to reach this goal also grows. They cover the use of a spectrum of implementations for, inter alia, information systems, smart networks, and public services. In order to operate, these smart cities have to process multiple types of data including personal information. Ultimately, the systems and services that process these data are decided by the city with limited opportunities for their citizens to influence the details of their implementations.

In these situations the citizens have no choice but to trust their city with the operation of these systems and the processing of their personal information. This type of a relationship, forced trust, affects the smart city implementation both directly and indirectly. These effects include additional considerations by the city to guarantee the protection of the citizens' privacy and the security of their personal data, as well as the impacts of forced trust on the willingness of the citizens to adopt the offered services.

In this thesis, privacy protection, data protection and security, system reliability and safety, and user avoidance were identified as the four major domains of concern for citizens with regard to forced trust. These domains cover most of the main impacts smart city projects have on their citizens, such as ubiquitous data collection, scarcity of control over the utilisation of one's personal data, and uncertainty of the dependability of critical information systems. Additionally, technological and methodological approaches were proposed to address each of the discussed concerns. These include implementation of privacy by design in the development of the smart city, use of trusted platforms in data processing, detection and alleviation of potential fault chains, and providing the citizens the means to monitor their personal data.

Finally, these recommendations were considered in the context of a small smart city. The Salo smart city project was used as an example and the recommendations were applied to the planned aspects of the upcoming smart city, such as knowledge-based management, a smart city application for information sharing, and increased transparency and justifiability in governance.

Keywords: forced trust, smart city, privacy protection, data protection, reliability, avoidance, participation, Salo

Contents

List of Figures

Glossary

anonymisation processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject within a set of subjects [3]. 40, 42–45, 48

data a collection of information, facts, or statistics used in analysis. 1, 2, 10, 12–23, 25, 27–33, 35, 37–40, 42–67, 69, 70, 72, 73, 77–85

data controller a party that decides how and why personal data are processed. 18, 19, 39, 45, 59, 74

data processor a party, delegated by the data controller, to process personal data. 18, 19, 22, 39, 44, 59, 61

differential privacy a method for producing anonymised views of a dataset such that the contributions of any one individual in the dataset is indistinguishable from a dataset without them. 43, 45, 55

distrust trust in a trustee to actively and deliberately act against the truster's interests. 6, 10, 11, 18, 20, 78

mistrust misplaced trust; trust that was betrayed by the trustee. 6, 7

nonce in communication, number used only once to prevent replay attacks. 28, 51

pseudonymisation processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information [4]. 42–44

trustee an actor being trusted by another actor. 6–8, 12–14, 16, 82

truster an actor that trusts another actor. 6–8, 11, 12, 14, 16, 82

untrust positive trust, lower than what one deems required for cooperation. 6, 20, 78

Acronyms

6LoWPAN IPv6 over Low-power Wireless Personal Area Networks. 26, 27

AES Advanced Encryption Standard. 27

BLE Bluetooth Low Energy. 26, 27

DoS denial of service. 28, 30, 52

DPA data protection authority. 19

DPIA data protection impact assessment. 19, 56

DPO data protection officer. 19

EU European Union. 16, 19, 55, 58, 71

FE functional encryption. 53–55, 59, 60

GDPR General Data Protection Regulation. 16, 18–20, 39, 40, 42, 47, 53, 57, 60, 61, 70

HE homomorphic encryption. 53–55, 59

HMAC keyed-hash message authentication code. 51, 53

ICT information and communications technology. 9, 21, 24, 34, 55, 62, 66, 75, 83

IDS intrusion detection system. 22, 29, 51, 55

IoT Internet of Things. 26–28, 30, 32, 35, 47, 48, 50, 55, 56

IS information system. 9, 10, 13, 15, 20, 34, 37, 40, 71, 82, 85

KRACK key reinstallation attack. 28

LG local government. 15, 16

LoRaWAN Long Range Wide Area Network. 26, 27

MitM man in the middle. 49

NCSC-FI National Cyber Security Centre Finland. 47, 48

PUF physical unclonable function. 51

SGX Software Guard Extensions. 53–55, 59

SP service provider. 15, 16

TPM trusted platform module. 53–55, 59

Chapter 1

Introduction

Smart cities are a developing concept with potential to significantly improve the efficacy and quality of life for their residents as well as to increase the productivity of industries and the efficiency and reliability of public infrastructure. Through e.g. smart sensing environments and automated decision-making, smart traffic can lower the amount of time vehicles idle at traffic lights, thus reducing emissions and fuel consumption; smart homes can more efficiently regulate their energy consumption, allowing smart grids to improve their load balance, thus reducing the emissions from power or district heating plants; and factories can optimise their production pipelines.

To achieve their goals, smart cities are inherently data-oriented, requiring extensive data collection and processing. The nature of these data ranges from industrial, such as from the aforementioned factories, to environmental, for instance from air pollution or traffic sensors, and to personal, for example location or electricity consumption data.

To reach the status of a smart city, a city must then utilise a wide variety of different types of sensors and often handle the personal data of its residents. Additionally, the services provided by the city, based on the processed data, can require cooperation from the citizens if e.g. the use of specific equipment is required. In the cases where the citizens have no alternatives to participating in the data collection or to using specific public information systems, they as a consequence must trust the systems to respect their

privacy and to function as expected.

This thesis is written in conjunction with, and funded by, the Salo smart city project. Its goal is to enumerate the effects of the aforementioned forced trust on small smart cities, find sustainable methods of smart city development given these effects, and apply these results to the Salo project.

1.1 Research problems

The citizens living in a smart city do not necessarily have any other options, as explained above, but to use the services and systems provided by the city or be negatively affected e.g. in the quality of their daily lives. As a consequence, they are forced to trust the public authorities in the design, implementation, and operation of the smart city.

The concept of forced trust, in the context of information systems and technologies, has not previously undergone a systematic literature review. This is required to provide a frame of reference for later considerations on its effects on smart cities.

The chosen data collection and processing methods, security and reliability considerations, as well as the level of influence the citizens' participation has on the city, inter alia, are affected by, and affect, this trust. Thus, it is important to map the subjects of forced trust in the operation of a smart city and find suitable best practices to ensure their sustainability from the point of view of the citizens.

Ideally, the end-users, i.e. the citizens, should not have to be forced to trust the city they live in. Instead, the city should operate in such a manner that it has earned the trust it enjoys from its residents. However, due to the inherent power imbalance between the city and its citizens, some of the trust will always remain forced but its effects can, and should, be controlled.

1.2 Objectives

Based on the previously defined research problems, this thesis aims to fulfil the following objectives.

- O1 What is forced trust and how does it affect and relate to smart city projects?
- O2 What are the main concerns related to the design and operation of smart cities for their citizens?
- O3 How can the concerns identified in O2 be resolved to minimise the potential negative impacts related to forced trust?
- O4 How can the approaches of O3 be applied to the Salo smart city project?

1.3 Thesis structure

This chapter provides the background and motivation for this thesis as well as the desired outcomes. Chapter 2 discusses and defines forced trust, for the scope of this thesis, through a systematic literature review, as well as considers the effects of forced trust and its relevance to smart cities. Additionally, definitions and forms of trust are covered together with various factors that can affect the trust enjoyed by a city.

Chapter 3 covers the technical and societal backgrounds related to smart cities. It includes a discussion on relevant use cases of smart environments and available technologies for their implementation. In a brief overview, known and potential threats for smart environments are covered. The chapter also focuses on the societal objectives and areas of interest, i.e. the motivation behind their development, in smart cities. Additionally, examples of existing smart city projects and a discussion on the benefits and drawbacks of small smart cities, compared to larger ones, are provided.

In the 4th chapter, the previously identified main concerns are discussed in depth, covering their effects on the citizens' trust. Additionally, methodologies and, where ap-

plicable, technical means are suggested to try to minimise the direct and indirect negative effects that can result from incidents where the citizens' trust is betrayed.

A description of the Salo smart city project is given in chapter 5. The areas of focus of this project are discussed along with practical examples. Additionally, the previous concerns are mapped onto these areas and examples to determine suitable recommendations.

The conclusions of this thesis are included in chapter 6. Additionally, the level of fulfilment of the previous objectives are evaluated. Finally, potential subject areas that could benefit from further research, based on the discussions in this thesis, are identified.

Chapter 2

Forced trust

Societies are largely built on trust. It is not the only building block but a significant one, nonetheless. Every day one has to trust the people they meet as well as the technologies they use. This trust is shaped by e.g. their past experiences and their and their peers' opinions. The resulting "trust" then shapes their actions, behaviour and attitudes towards the subject of trust.

This chapter covers some of the commonly used definitions of trust, and its various forms, that are used throughout this thesis in section 2.1. Additionally, a literature review of the concept of forced trust is done in section 2.2. Its effects on, and its relation to, smart cities are discussed in section 2.4. Finally, a few factors that affect or can affect the citizens' trust in their smart cities, including regulation and past public project, are covered in section 2.5.

2.1 Trust

Trust, as a concept, has a variety of descriptions and definitions depending on the context of its use. Human-human, human-machine, and machine-machine interactions differ greatly in e.g. the perceived trustworthiness of the other party, the number of potential actions each party has during the interaction, and the expected outcomes. Technologi-

cal solutions are limited in the number of ways they are able to communicate, with e.g. pre-defined protocols and states of operation. In comparison, humans are more flexible in their behaviour, with e.g. their actions shaped by, as Schneier [5, p. 11–12] describes, personal and group interests in addition to societal pressures. Here the focus will be on the trust relating to human-human and human-machine interactions.

The relevant definitions of trust in the online Oxford English Dictionary [6] are:

> **1a** *Firm belief in the reliability, truth, or ability of someone or something; confidence or faith in a person or thing, or in an attribute of a person or thing. Chiefly with in (formerly also †of, †on, †upon, †to, †unto).*
>
> **2** *The quality or condition of being trustworthy; loyalty; reliability; trustworthiness.*

In addition to trust, Marsh and Dibben [1, p. 19–20] discussed three additional concepts: *distrust*, *untrust*, and *mistrust*. They describe distrust as a form of negative trust. In the state of distrust, a *truster* actively trusts the *trustee* to deliberately act in a way that is detrimental to the truster. On the other hand, the two additional types of positive trust are untrust and mistrust. When untrusted, one enjoys some level of trust but not enough for the trusting party to be convinced of the trustee's actions being in their best interest. Finally, mistrust is a state of trust one enters once their trust has been betrayed. That is, mistrust is simply misplaced trust.

These terms can thus be used to describe the state of trust a truster is in towards a trustee. The truster can change from one of these states to another based on their experiences with the said trustee. An interpretation of their relationship is shown in figure 2.1. In the figure, the truster's instantaneous trust is represented by a numeric value denoted t. Positive experiences with the trustee increase this value, and similarly negative ones decrease it.

There are two important thresholds, which determine the current state: *zero trust* and the *cooperation threshold*. The former is simply the boundary between distrust and un-

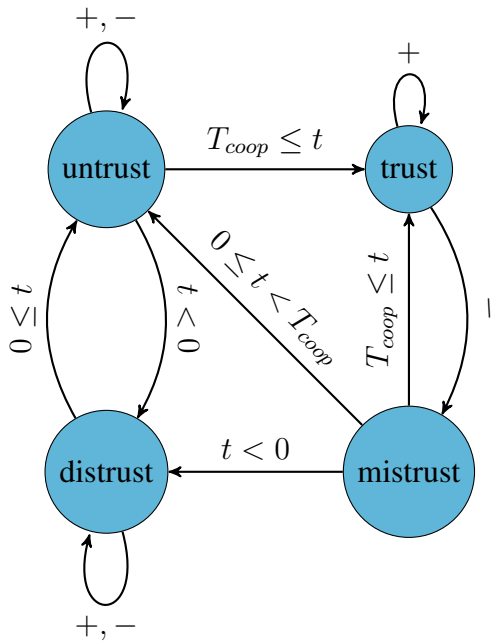

Figure 2.1: A finite state machine representation of trust. Loosely based on the trust continuum figure by Marsh and Dibben [1, p. 21].

trust, albeit the exact meaning of zero trust is difficult to define [1, p. 21]; the latter a subjective minimum value for trust before one willingly cooperates with the trustee without external acting forces.

The state of mistrust is entered when the trustee betrays the truster's trust. Mistrust, then, is not a permanent state of trust akin to the others but a temporary one. Depending on the severity of the breach of trust, the final state can be any of the others. As Marsh and Dibben mention in the discussion on modelling mistrust [1, p. 25], a mistrust incident will also affect future trust-related interactions between the truster and the trustee. The magnitude of this effect depends on the intentions of, and their transparency to, the trustee. An unintended betrayal of trust by a benevolent actor will not affect the truster's future behaviour as strongly as if it was done by a malevolent actor. If, for example, the trustee's malevolent intentions when betraying the trust are revealed, the truster will most likely be unwilling to cooperate in the future.

2.2 Literature review

The previous discussion on trust assumed the premise that the trust between the truster and trustee is voluntary. However, there are many cases in which the truster has no choice but to cooperate with the trustee despite the trustee's actions.

Strong dependency relationships are normal between the public sector and people, such as those involving healthcare, law enforcement, and education. Similarly, people can also be strongly dependent on the private sector, as is the case with information networks, and electricity. The citizens are then, even if paying for the service, forced to trust the other party in order to operate normally in their everyday lives.

To examine the previously published literature on forced trust, a systematic literature review has to be done. Six online article databases are used in this literature review: Volter, ACM, arXiv.org, IEEE Xplore, ScienceDirect, and Scopus. Each of these databases are queried with the search term "forced trust" and from these results the duplicates and irrelevant papers, where the phrase occurred in a different context, are filtered. This process, and the number of results in each phase, is shown in figure 2.2 below.

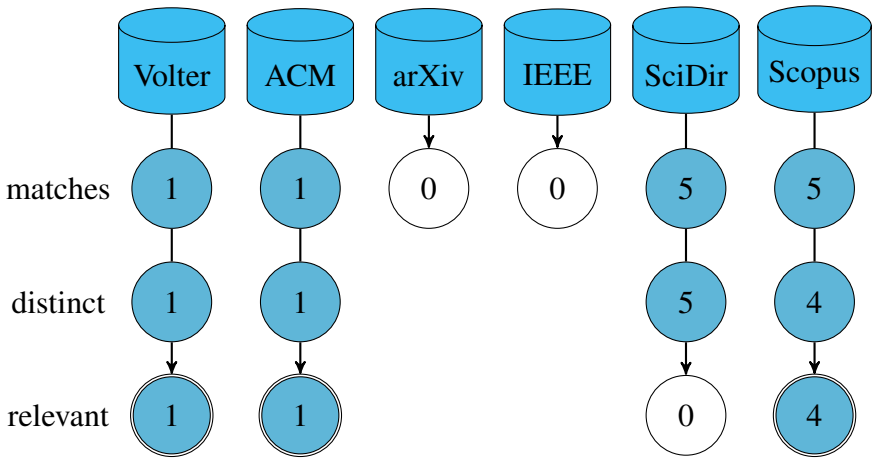

Figure 2.2: Literature search process with the remaining number of papers in each phase.

Three of the six results, Hakkala [7], Hakkala et al. [2], and Madhisetty and Williams [8], discuss forced trust in relation to information technology and information systems.

The remaining three, Ledeneva [9], Hosking [10], and Tikhomirov [11], discuss the topic from a societal perspective, as it relates to the Soviet Union. The number of results is limited, thus limiting the universal applicability of results from their analysis. Nevertheless, the aforementioned papers are analysed in the following subsections.

2.2.1 Prior definitions

In his dissertation [7, p. 86] Hakkala defines forced trust as a situation *"where the user has no choice or opportunity to affect any part of the information system, including the choice to use the system itself"* and *"in which a user is dictated to use and to trust an information system or an ICT product"*. As such, he defines the term in the context of systems and products that citizens are forced to use, especially critical governmental information systems, and consequently trust, without being able to opt out or influence their design or implementation. This also means that a designer of said systems *"has to take into account the potential misbehavior of users -- and implement security measures and safeguards against such events"* [7, p. 86]. Forced trust, then, can be interpreted as a trust relationship between users, administrators, and designers of information systems, where the use of these systems is externally mandated and the participating parties cannot rely on others' intentions to not be malevolent.

Similarly, in [2, p. 72–73] Hakkala et al. define forced trust as a situation *"where an entity – whether a customer, an organisation or even a governmental agency – does not have a privilege to choose but is instead mandated to use a dictated information system"*. The mutuality of this trust is described with the system suppliers' inability to trust the *"benevolence of all forced users"*, which could lead to increased costs as they are *"forced to implement security verification for inputs and maintain backup plans"* [2, p. 73].

In the third information technology -related result, Madhisetty and Williams discuss the effects of forced trust on the users of social media. They defined forced trust both as a situation where a publisher of media *"does not trust that their content will not be*

misused via networks of friends they have shared" [8, p. 132], and as an experience of *"participants who have no alternative but to trust that sharing their data as photos or videos will not violate their notion or expectations of privacy"* [8, p. 136]. Thus, they focus on the trust relationship between services that require or utilise personal data and their users.

Ledeneva describes the deeply ingrained form of collective responsibility, or krugovaya poruka, found in the former Soviet Union as forced trust. It meant that entire groups were held responsible for the deeds and tasks of their individual members [9, p. 86]. This social pressure meant that each citizen was forced to trust their peers to operate in an expected manner. Such collective forced trust was utilised e.g. with tax collection and crime prevention [9, p. 89]. As such, Ledeneva mainly discusses forced trust as it relates to interpersonal relationships between peers.

Hosking discusses the all-encompassing distrust within the Soviet population. The post-revolution societal turmoil, upheaval, and reform resulted in an environment that rewarded distrust [10, p. 6–7]. This encouraged the people to actively distrust their peers and try to identify and unveil political enemies. As a result of this social atmosphere, the populace were forced to trust the party leaders and often sought aid for their ailments or punishment to their perceived enemies [10, p. 16].

Finally, Tikhomirov bases his concept of forced trust on Ledeneva's description of the krugovaya poruka for his examination of forced trust in Soviet communication. Individuals would attempt to escape the feeling of distrust and vie for the trust of the state. This was often felt obligatory, for the alternative could lead to being sent to the gulags or execution [11, p. 80]. Like Hosking, Tikhomirov discusses one-directional forced trust between the citizens and the state. The available options for these citizens, in their political environment, were either to trust the communist party or risk one's welfare.

Unlike in the case of the Soviet Union, the forced trust in information systems (ISs) is not deliberately manufactured and fostered by the state or local governments. It is instead

an emergent side effect resulting from the general deployment of these systems and the strengthening dependence of the society on smart environments.

State- and government-run services based on information technology and systems are often planned and executed without the citizens' input. Additionally, these systems are usually partially or even completely outsourced, as will be discussed in the section 2.5.3. As such, the citizens do not only have to trust the public authorities with the operation of the system but also, potentially undisclosed, third parties.

An important distinction, then, is the source of the experienced forced trust. In the Soviet society it was caused by a combination of distrust for one's peers and trust of the communist party to be a reliable source of stability. Comparatively, in information societies it is formed by the citizens' general lack of options in the use of publicly operated systems and services leading them to have no choice but to rely, and trust, them and their operators. In this sense their potential distrust towards each other could have some effect on the rate of adoption and perceived risks of the systems but not on the trust itself.

2.2.2 Described effects

Hakkala [7, p. 90–91] and Hakkala et al. [2, p. 77–78] describe three major effects forced trust can have on the trusters' reactions with the provided systems: *acceptance*, *avoidance*, and *resistance*. Acceptance is the desirable outcome where the users decide to use the services and systems. This does not, however, imply that they are fully informed or accepting of the details of the chosen implementations. Instead they could e.g. be aware of issues but deem them to be insufficient to prevent the use of the services or systems, or indifferent to potential issues altogether [7, p. 90], [2, p. 77].

Avoidance, on the other hand, leads to the users partially avoiding the use of the said services [7, p. 91], [2, p. 77]. This could e.g. lead to the users misusing the system by providing it with false information [2, p. 77] or circumventing its intended functionality [7, p. 91]. These example cases could, in the worst-case scenario, cause automated

decision-making to malfunction. Thus, avoidance is undesirable especially in critical and data-sensitive systems. Causes and effects of avoidance, and potential methods for their mitigation, are further discussed in 4.4.

Akin to avoidance, resistance among the userbase lowers the usage of the systems and services. However, resistant users actively fight against them, even to the point of sabotage [2, p. 78–79]. This is the most severe user reaction to forced trust and should then be avoided. The aforementioned mitigation methods are also applicable in some cases of resistance.

According to Madhisetty and Williams, user trust and confidence in a service encourage them to further use the said service [8, p. 129–130]. The amount of control the users have e.g. over their privacy works alongside the forced trust to shape their confidence in the service. To maximise their confidence, an optimal ratio of 1:4, in terms of forced trust versus user control, was found based on interviews [8, p. 137].

2.3 Definition

In order to consistently discuss the effects of forced trust on the design and considerations of smart cities, a definition for the term is given here. It is based on the results of the previous literature review and delimited to the context of this thesis. This definition is given below in definition 2.3.1.

Definition 2.3.1 (Forced trust)**.** *Forced trust is a situation where a truster has no choice but to trust a trustee, or services provided by the said trustee, with no or minuscule ability to influence the function or behaviour of the target of trust, i.e. the trustee or the services.*

Corollary 2.3.2. *A truster is in forced trust with a trustee if they are mandated to provide, or use services that utilise, personal data in order to avoid their quality or ease of life being negatively affected.*

Corollary 2.3.2 is a consequence of forced trust due to the sensitive nature of personal

data. The owner of the information relies on the receiving party to respect the privacy and confidentiality of the data and the owner. Because their only option without negative consequences is to comply with the handover of information, they are in forced trust with the trustee.

This definition, and where applicable its corollary, thus covers all of the cases discussed in the literature review. That is, the forced trust relationships between the citizens and relevant individuals and parties involved in public information systems, in both directions; as well as between the said citizens and the mandated systems. Additionally, through the corollary, the definition is directly applicable in the context of smart cities.

Nevertheless, the low quantity of relevant literature can have a limiting effect on the broader applicability of this definition. With more research on the subject, it could shift from the one given above but, given the term is primarily applied to information systems and services of smart cities in this thesis, the effects of such a shift should remain minor.

2.4 Forced trust in smart cities

Details of smart city implementations are largely decided by the governing bodies. These details include choices of suppliers, technologies, ISs, and devices among others. Even if the end users are involved in the design and testing processes, in the end it is the city that decides on the final implementation. Thus, the citizens are forced to trust the smart city.

An intrinsic part of the function of smart cities is the collection of data. They are collected e.g. from sensors and smart devices used by the citizens or installed around the city. These data can include information of various levels of privacy, from location information to water consumption. In addition, in the increasingly electronic societies, as the use of cash declines steadily in favour of debit and credit cards, contactless payment, and online transactions, the citizens' consumer habits can be easily used in their profiling.

In addition to the citizens, the involved governmental bodies are also subjected to

forced trust in certain scenarios. This is especially apparent in cases where at least some of the functionalities of the smart city are outsourced to foreign third-party companies. In these cases, e.g. the location of data storage has to be considered due to varying national laws regarding data privacy. An illustrative representation of the different participating parties and their trust relationships with each other is shown in figure 2.3.

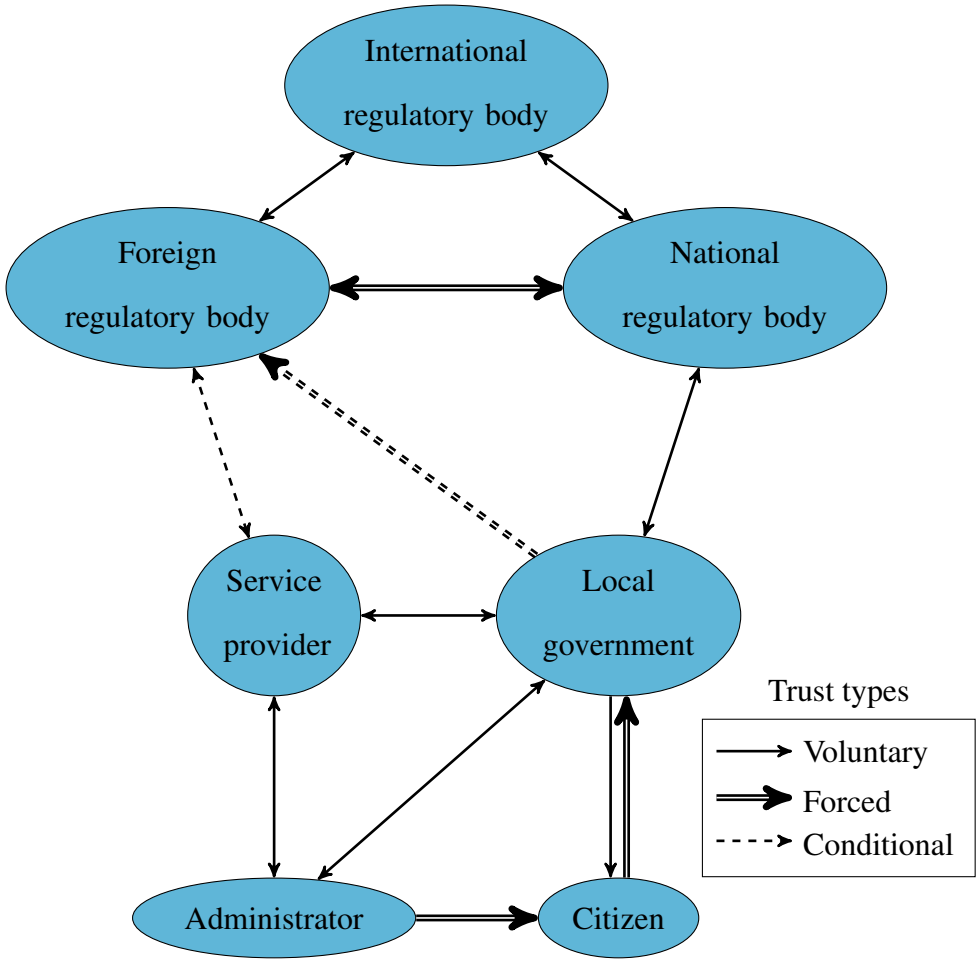

Figure 2.3: A simplified illustration of the trust landscape of a smart society. Based on the critical governmental information system landscape in [2, p. 74].

As can be seen from the figure, the trust landscape between the numerous directly and indirectly participating parties is complex, even when simplified like in the said directed graph. In the figure the directed edges display a trust relationship, starting from the truster and ending at the trustee. Single arrows denote voluntary trust and double arrows forced

trust. Dashed arrows designate trust relationships that exist if some conditions are met. These relationships are transitive, and the shortest path between two actors is interpreted as the effective trust. However, it is not guaranteed that a unique relationship exists between two actors. For example, a citizen is forced to indirectly trust the administrators because they are trusted by the city, which the citizen is forced to trust.

The citizens, as users, are in an asymmetrical trust relationship with the local government (LG), as they are forced to trust the said governments, such as cities. This trust applies to decisions regarding the choice of used IS as well as service provider (SP), whether internally produced or outsourced. At the same time, if the systems utilise any form of an identity and access management system, allowing the users to for example log in to monitor and manage their own data, the users could have an additional responsibility of maintaining the security of their personal credentials. In these cases, citizens could be seen to also be forced to trust the other users of the services, whether peers or public workers, since reused credentials leaked from an unrelated service can allow attackers to compromise the system.

A system administrator is appointed to oversee the operation of the IS. They can be a public employee or work for a third-party SP depending on the implementation. Administrators enjoy the users' forced trust, transitioned through the local government, as well as the mutual trust of the government. At the same time, the administrators themselves are forced to trust the users not to actively try to breach the IS used. Additionally, the administrators can be seen to be in a mutual trust relationship with the service provider due to their reliance on the provided systems.

The aforementioned LG enjoys mutual trust with the national regulatory body, the administrator, and the chosen service provider or supplier. In the case the used SP is an international entity and operates under the jurisdiction of a different nation, the local government is forced to trust the foreign state in question. Similarly, in these cases the service provider also enjoys a mutual trust relationship with the governing body. However,

while the LG chooses the used SP, and thus they are not equals in this relationship, the nationality of the supplier can have an effect on matters related to the handling of data.

The service provider in this context is the actor that is responsible for providing the required products and services that e.g. a smart city requires. The services they provide can range from physical devices to software as a service. As such, they have to comply with both their own regional regulations as well as those of their customer. These could be defined by the nations or derived from international directives, such as the General Data Protection Regulation (GDPR) of the European Union (EU).

At the national and international levels, the regulatory bodies set laws and directives that they trust other nations will abide by. Each national regulatory body is forced to trust their peer states, especially due to the potential presence of classified intelligence programs that could violate the directives. Additionally, they mutually trust the international bodies since, while the international regulations affect themselves, too, they are able to affect the said regulations.

The most significant forced trust relationships from the point of view of a citizen are those between themselves and the government, as well as the administrator. Additionally, the choice of services of the city can force them to trust a foreign state not to influence the SP negatively. These cases and their effects are further discussed in the following sections 2.5.1, 2.5.2, and 2.5.3.

2.5 Factors affecting trust

As discussed previously, a truster's trust towards a trustee develops over time based on their interactions. However, in addition to the direct effect these have, there are a number of external factors that can affect e.g. the initial trust or the impact each time the trust changes.

Three of these sources are discussed in this section: national regulations, the GDPR,

and experiences from past and on-going projects of the public sector. The first two place restrictions on the use and collection of data and as such limit the potential impact the systems used in the smart cities could have on the citizens' lives, albeit the impact they have on a given citizen's trust depends heavily on their awareness of the regulations. Finally, experiences from past and current projects have a significant effect on their initial trust towards new ones, as well as on their confidence that a new project will be successful.

2.5.1 National regulations

The regulations set by the national regulatory bodies have a direct effect on how, when, and where the citizens' data can be used. These data are often stored in registers and contain data points of various types such as healthcare, personal data, and vehicles. These registers, when introduced, are usually defined with a specific purpose and usage limits.

The modern data economy encourages businesses to harvest, trade, and process increasing amounts of data about existing and potential users. These data can be used for e.g. targeted advertisements or consumer-centric product development. These factors emphasise the importance of having a set of clearly defined, unambiguous citizens' data rights set in a national law. Giving everyone autonomy over their personal data will have a positive effect on trust and potentially on the willingness of citizens to use data-based services.

Finnish law enforcement authorities can use the national registers for e.g. crime prevention or investigation, or to protect the safety of the general populace [12]. These rights are limited by the legal definitions for allowed use cases of each register. Some of these restrictions, such as the limited use of biometric data in crime prevention, have been weakened in the recent years. Such is the case, for example, with the use of biometric photographs, used in passports, in automated facial recognition [13].

The Finnish police and customs received permission for automatic facial recognition from e.g. a live video feed at the beginning of June 2019 [13]. This extension of the

allowed uses of person registers was justified with an increased efficiency in crime prevention since automated facial recognition produces more accurate matches. As such, the new law traded some of the citizens' privacy in exchange for a claim of increased security.

The previous changes were a part of a larger new intelligence legislation which allows the Finnish Security Intelligence Service to perform increased surveillance of military and civilian network traffic. This also required a change in the constitution to allow the communication confidentiality laws to be bypassed beyond criminal investigations if national security is deemed endangered. [14]

The regulatory cases mentioned above are examples of changes to the legislation affecting the collection, processing, and storage of the citizens' personal information. While they could result in an increased level of security, their immediate effects are a reduction in the rights concerning one's privacy. The effects these changes have on the trust they experience towards authorities varies depending on the person. Some might become increasingly distrusting; others could be indifferent, as they feel they don't have anything to hide; and some might be inclined to trust the authorities more. However, an inherent risk is present whenever the constitution is weakened: it is impossible to predict if the new capabilities will be abused in the future.

2.5.2 GDPR

GDPR came into force in May 2018 [4] and introduced a number of new rights to the European citizens with regard to their data ownership. They include the rights to what data are processed where, why and by whom, to access the said data, and the right to object to their automated processing [15]. The citizens are then also able to withdraw their consent and demand the deletion of the data when the data controllers or data processors no longer have a need for or legal rights to the data.

Under the regulation, data controllers and data processors are obligated to clearly communicate to the users if their personal data are processed and are required to receive

the data owners' consent [16, p. 8]. This communication must be done using clear and unambiguous language. Additionally, the data processor is obligated to follow a contract, which clearly specifies specific instructions for the processing, with the data controller while processing the data [16, p. 9]. Participating organisations must also appoint a data protection officer (DPO) if they e.g. actively monitor or process the users' data [16, p. 13]. The DPO acts as their contact with the local data protection authority (DPA).

In cases where the data owners' individual rights and freedoms could be jeopardised by the processing, the organisation has to run a data protection impact assessment (DPIA) [16, p. 16]. The risks identified in the assessment have to be removed prior to the processing. The three example cases given in [16, p. 16] apply well in the context of smart cities: systematic evaluation of individuals, large-scale monitoring of public spaces, and large-scale processing of sensitive data.

The data controllers must additionally ensure sufficient protection of the data between their collection and deletion. The principle set by GDPR is *"Data protection by design and default"* [16, p. 14]. This means introducing data protection early in the design processes of new products and services and selecting the most privacy-preserving settings for users by default.

The penalties of data controllers and data processors that do not comply with the regulation range from warnings and reprimands to fines of up to €10 million or 2 % of annual revenue in the cases of smaller infringements and €20 million or 4 % of annual revenue in severe infringements [4]. In severe cases the offender could also be forbidden from any future data processing. However, the regulation is lenient towards violations of GDPR when they are done by public authorities:

> *It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines.*
>
> *General Data Protection Regulation [4]*

It is then allowed by the regulation for the member states of EU to, in their own dis-

cretion, not fine incidents where the citizens' data freedoms and rights have been violated. This is also the case under the Finnish data protection act:

> *An administrative fine cannot be imposed on central government authorities, state enterprises, municipal authorities, autonomous institutions governed by public law, agencies operating under Parliament or the Office of the President of the Republic, or the Evangelical Lutheran Church of Finland and the Orthodox Church of Finland or their parishes, parish unions and other bodies.* *Finnish data protection act [17]*

It can be seen that the regulation, as well as the Finnish law, treats public and private sectors differently. While this reduces the amount of expenses and required changes to policies, it has the potential to severely weaken the citizens' data protection. Additionally, the penal code for a gross violation of the provisions of the person register law was mostly repealed in the beginning of 2019, to avoid overlap with the GDPR, and appended with clauses pointing to GDPR and the new data protection act [18].

Such a difference in the treatment of infractions and violations of the regulation could have a negative outcome on the users' trust in a forced trust environment such as a smart city. They might expect private corporations to be more likely to e.g. perform blanket data collection and use the data for targeted advertisements. These expectations could manifest themselves as untrust, or in some cases distrust, towards the private sector. In these situations, regulations such as GDPR benefit smart cities because of the knowledge that misuses of data would be penalised, thus lowering the users' threshold for cooperation.

By virtually giving the public authorities a blank cheque with data protection violations, the trust and confidence in the authorities' capabilities can be reduced. This perception, combined with the recent weakening of the citizens' rights to privacy such as those discussed in section 2.5.1, as well as the citizens' experiences with earlier and current IS implementations, has a potentially chilling effect and, due to the forced trust environment, could lead to user evasion.

2.5.3 Implementations of information systems and services

The main concerns of an end-user, when considering the locally or externally provided services, are the usability, security, and reliability of the supplied systems. When older methods of performing a task, e.g. paper-based filing of taxes or reserving appointments, are replaced by newer information and communications technology (ICT) -based solutions, the new methods should always be better, that is e.g. more convenient or faster to use.

Problems with the ease of use of a system can directly affect the lives of citizens e.g. through unintuitive or lacking user interfaces, or indirectly e.g. by slowing the workflow of healthcare professionals. The former could dissuade users from adopting systems introduced later or encourage them to misuse the system in order to make its use easier. Additionally, the latter can cause more severe issues, such as complications in patient care in the used example. This type of a problem has been encountered e.g. with the Apotti healthcare system, where data entry is slower and requires some of the work to be done twice, and the system introduces potentially dangerous situations due to restrictions on the access to the patients' data [19].

Design flaws and vulnerabilities in these ICT systems can cause varying levels of damage to their operators and users. Potential damages include, but are not limited to, data corruption, leakage, or theft, and system outage. Corruption of data, such as sensor measurements, can cause irreversible damage e.g. in systems where decision-making uses automated data processing, such as insulin pumps, centrifuges, or home automation.

Data leakage and theft both describe a breach of confidentiality, whether large or small, but with differing intentions. Leakage occurs when the access rights for a piece or collection of data are too lax, allowing them to be accessed without authorisation. This can occur both inside the system, by a user, or externally, with the data accessible to non-users. As an example, the patient data protection of the Apotti system was found wanting [20], allowing medical workers to access an excessive amount of patient information.

Data theft, on the other hand, is an intentional breach of the system resulting in the extraction of data. These breaches could occur as a result of external or internal attacks, e.g. through the use of malware or intrusion. Theft, as well as leakage, should be protected against with both technical and non-technical means, such as intrusion detection systems and personnel training. More approaches are covered in section 4.2.

Ensuring the systems and services are reliable is important to gain their users' trust. If they relate to operation or functionality of a smart city that the citizens require regularly, such as smart infrastructure, transport, or healthcare, the smart functionality should only act as an enhancement of the capabilities of the systems or services. Alternatively, if their outage could have a noticeable effect, such as traffic congestion or impeding of patient care, sufficient countermeasures to prevent their known causes. These countermeasures include fault analyses and redundancy, which are further discussed in 4.3.

Finally, if collection or processing of personal data is necessary to provide the intended benefits to the users, the data collection mechanisms should be non-invasive and provide the users control over the collection e.g. through opt-in consent. This protects the users' privacy, thus aiding in building trust towards the implementation, and can be used to encourage citizens to voluntarily provide their data in exchange for additional services or improved quality of their current services. An example of a relevant data management model is MyData [21], which focuses on providing users control over the flow of their personal data between the datasets and data processors. These issues are covered in more detail in section 4.1.

Chapter 3

Smart cities

In this chapter, the background and main aspirations of smart cities are discussed. Due to the emerging and shifting nature of smart cities, some of their definitions are initially covered in section 3.1. In general, smart cities utilise data gathered from smart sensors to optimise their operation. The consequently inherent dependency of smart cities on smart environments and networks is examined in section 3.2, where different types of networks and used technologies, as well as potential security threats against these smart environments, are focused on.

Some of the beneficiaries of the aspects of smart cities are examined in section 3.3, such as improved efficiency and citizen participation. Additionally, in section 3.4 some examples of cities that currently identify as, or are progressing towards becoming, smart cities are given. Finally, as the focus of this thesis is on small cities, the advantages and disadvantages of small smart cities, compared to larger cities, are discussed in section 3.5.

3.1 Definition

Emerging as a nebulous concept as cities develop increasing connectivity and automation based on different types of data, smart cities have many different definitions. Three of those are examined here, given by Deakin and Al Waer [22], Frost & Sullivan [23], and

IEEE [24].

Deakin and Al Waer make a distinction between a city that simply utilises technologies in its operation, an intelligent city, and a smart city. They list four requirements a city should fulfil before claiming to be a smart city: wide utilisation of ICT, use of those technologies to transform life, embedding the previous ICT in the city, and bringing them and the people together to aid innovation, learning, knowledge, and problem solving [22, p. 141]. Additional emphasis is placed on involving the citizens in the development of the city in order to take advantage of the social capital in the adoption of ICT.

Frost & Sullivan list eight parameters, a minimum of five of which are required for a city to possess in order for it to be a smart city. These parameters are smart governance and education, smart healthcare, smart building, smart mobility, smart infrastructure, smart technology, smart energy, and smart citizen [23]. They also distinguish four types of market participants that shape the smart cities: integrators, network service providers, product vendors, and management service providers [23].

Finally, the IEEE Smart Cities Community define six sectors that make a city smart: smart water, smart energy, smart mobility, smart health, smart food and agriculture, and smart waste [24]. Additionally, they specify five domains that enable the various applications in smart cities. These domains are sensors and intelligent devices, networks and cyber security, systems integration, intelligence and analytics, and management and control platforms [24].

Each of the above definitions involve ubiquitous use of smart technologies in the basic functions of the city, and the involvement of the citizens in their integration into the communities and systems. However, Frost & Sullivan's and IEEE's definitions specify explicit fields of application but do not establish recommended approaches for execution. On the other hand, Deakin and Al Waer's list is generally applicable to each of these fields but does not specify any of its own.

Based on the previous discussion, the definitions proposed by Frost & Sullivan [23]

and IEEE [24] are succinct and can be combined to provide the following definition for smart cities will be used for the rest of this thesis. The term has already been used during the discussion on forced trust in chapter 2 but due to the focus on forced trust this definition was not yet necessary.

Definition 3.1.1 (Smart city)**.** *A city can be classified as smart if it realises at least five of the following properties of a smart city: smart governance, smart education, smart healthcare, smart building, smart mobility, smart infrastructure, smart technology, smart energy, smart citizen, smart waste, and smart agriculture.*

3.2 Smart environments

In order to supply the systems related to e.g. smart infrastructure, mobility, or healthcare, with a sufficient amount of data, a smart city needs a ubiquitous network of smart sensors. The collected information includes environmental measurements and observations, e.g. air quality and amount of traffic; personal, such as medical or location, data; and metrics, such as power and water consumption. To accommodate each of these types of information, multiple separate, and specialised, sub-networks are needed.

Smart sensor networks can be separated into three distinct main layers: the sensors, or sensor nodes, forming the edge layer; the gateways forming the fog layer; and the cloud layer. Data processing can occur at any of these levels, albeit the capabilities of the systems increase towards the cloud layer. As such, edge computing is advantageous in situations where the data analysis is not resource-intensive, as the delays in ensuing automation is minimised. Alternatively, fog computing can be used to aggregate and lower the amount of bandwidth required to transmit the information by gradually processing them on the gateways.

The smart sensor nodes collect and transmit the data automatically, and can be networked using various topologies, such as star or mesh as shown in figure 3.1. In a star

topology, edge nodes communicate only with a central node. This topology will be able to function even if some of the sensors malfunction. A mesh topology, on the other hand, consists of sensor nodes that are connected to as many neighbouring nodes as possible.

(a) Star topology (b) Mesh topology

Figure 3.1: Examples of sensor network topologies.

The wireless sensor nodes are capable of forming networks with their neighbours independent of external influence. This makes them viable for use in remote areas and, if they utilise long-range communication technologies, when the sensors are sparsely distributed. As such, these ad-hoc networks remain functional even if some of the sensors malfunction.

Some of the notable and commonly used smart network solutions are discussed in subsection 3.2.1. Both the technologies and relevant examples of their implementations are covered. Additionally, subsection 3.2.2 attempts to paint a comprehensive picture of the threat landscape associated with the aforementioned technologies.

3.2.1 Available technologies

A network comprising of interconnected devices capable of independently communicating with each other without a need for human intervention is commonly called an Internet of Things (IoT). These IoT devices can utilise a number of different communication technologies, such as Bluetooth Low Energy (BLE), ZigBee, Long Range Wide Area Network (LoRaWAN), and IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN). They have been designed to operate on low power, as the IoT devices are usually signifi-

cantly constrained in their available resources, e.g. energy, processing power, and memory. Additionally, Wi-Fi can be used with IoT if a sufficient power supply is available, such as in smart home devices.

BLE, ZigBee, and 6LoWPAN are suitable for low-range communication. While ZigBee is capable of supporting networks with star, tree, or mesh topologies, BLE supports device-to-device communication and a limited mesh-like topology, which simulates the functionality of a mesh by forwarding data via a chain of devices. Thus, BLE is viable for e.g. wearable accessories used to monitor health, and ZigBee could be used, inter alia, in devices designed for smart homes, healthcare facilities, or industrial control.

6LoWPAN devices are usually more resource-constrained than the previous short-range solutions. The technology has been designed to function with low-performance hardware, small amounts of memory, and at low cost, both manufacturing and during operation [25, p. 28–29]. Due to these limitations, the 6LoWPAN is further restricted in e.g. its packet size and bandwidth usage. It communicates over IPv6 in order to take advantage of the existing network infrastructure and thus supports both star and mesh topologies.

LoRaWAN, on the other hand, is a long-range network standard. LoRaWAN networks comprise of end devices directly connected to gateways, which forward the traffic to network servers [26, p. 329]. As such, it supports a star-of-stars topology, where the nodes connected to the central server, gateways, have end devices connected to them. Communication over LoRaWAN networks is encrypted using 128-bit Advanced Encryption Standard (AES). These properties make it suitable e.g. for healthcare, utility metering, and environmental monitoring.

3.2.2 Security threats

While the wide range of potential applications of IoT, and consequently new opportunities for business and services, is often the cynosure of discussion in the public sector and

consumer domain alike, the state of IoT security requires extra attention. Their inherent shortage of resources available for, inter alia, processing or memory has a direct effect on the range of applicable approaches to securing the devices and their communication. For example, due to the limited resources, most commonly used cryptographic primitives are often not viable.

The main threat surfaces of the systems used by smart cities are the network, connected devices, and the chosen software [27, p. 612]. As the smart network spans a majority of the city, its communications should be secured. Networked, whether wired or wireless, communication is susceptible to, for example, interference, eavesdropping, and modification attacks [27, p. 617]. Interference attacks include radio jamming, and denial of service (DoS). Their objective is to disrupt the data transmission e.g. by making the originally sent packets indistinguishable from noise, preventing the communication by overloading the recipient with requests, or, in the case of Wi-Fi, de-authenticating them.

Eavesdropping attacks, on the other hand, focus on listening in on the traffic to determine its contents or analyse its metadata. The former can be achieved e.g. by capturing unencrypted packets, breaking the used encryption, or nullifying the encryption with vulnerability exploits. If the used cryptographic algorithms, or their implementations, are weak, an attacker can break them through cryptanalysis, brute force, or known attack vectors. This process can include, but does not necessarily require, the extraction of the encryption key.

One example of an attack where the packets could be decrypted without the leakage of the key is the key reinstallation attack (KRACK), where the nonce of the packets is reset by repeating the third message of the 4-way handshake. This causes the key stream to be reused, allowing the attacker to decrypt packets using known packets [28]. This attack is also an example of a replay attack, where the attacker affects the target by repeating previously sent messages.

Alternatively, an attacker could try to modify the sent packages, by first decrypting and

later re-encrypting them, or by guessing or deducing which sections of the data to modify. If the attacker is capable of the former, e.g. with an extracted key or the aforementioned nullification, e.g. data from sensors and transactions could be forged at will. Additionally, if the structure of the packets is known, the attacker could repeatedly try to modify the information by flipping bits of the payload and checksum until the modified packet is accepted.

The devices and systems connected to the network could also themselves become compromised. In the smart city, they range from the small, resource-constrained edge layer devices, through more capable fog layer gateways, to the systems used in the cloud layer. Additionally, as discussed by Ijaz et al. [27, p. 619–620], smart devices such as smart phones of the citizens, if used to participate e.g. through applications, can be compromised and enable attacks against the city. These devices are susceptible to, inter alia, malicious applications, and Wi-Fi and Bluetooth vulnerabilities. They could thus be compromised either via physical access or remotely, such as over the network.

Unauthorised physical access can be exploited in a number of ways, depending on the system. Sensors, connected to the wireless network, can leak the authentication or encryption keys through power consumption or execution time analysis. Additionally, in some cases they could also be extracted in plaintext from memory of a device. Lacklustre device identification could then be exploited by impersonating the sensor and transmitting forged data. Larger systems, such as gateways and servers, usually have a larger variety of interfaces through which to access or connect to them. This can enable the attacker to attach external devices to, for example, remotely monitor or access the system.

The devices could also be attacked through the network, e.g. when it is not isolated from the Internet, allowing attackers to discover and target them. Potential attack vectors include configuration errors, such as open ports or default credentials, or malicious payloads. Configuration errors can occur on each of the levels, i.e. edge, fog, or cloud, as well as in supporting systems such as firewalls or intrusion detection systems (IDSs).

In these systems, misconfiguration can allow malicious activity to bypass the intended security measures.

In addition to the threats described above, the utilised software can contain vulnerabilities, whether local or due to vulnerable dependencies. The top 10 common software vulnerabilities, as listed by MITRE [29], include out of bounds reading from and writing to memory, insufficient or erroneous user input validation, and unauthorised access to information. These concerns apply whether the software is embedded, such as in the case of sensors and most IoT, an operating system, or an application. Left undiscovered or unpatched, these issues can jeopardise the privacy and security of sensitive data handled by the systems.

Besides the individual threats, the vulnerabilities and issues discussed above can be used together in attempted attacks against the information infrastructure of a smart city. Disabling the communications e.g. through DoS or corrupting the data flow from the sensors will render the data-dependent smart systems used in the city unreliable or inoperative. Additionally, breaching the confidentiality of the communications through vulnerabilities related to the used wireless technologies, or analysing the structure of the network with captured traffic threaten the security and privacy protection of the citizens' data.

Finally, attention should be paid to the potential of cascading effects, as described by Braun et al. [30, p. 506–507], during security incidents. Issues encountered in one subsystem can propagate further if, for example, they introduce new attack surfaces in related or dependent subsystems. Such chains of incidents can erode the citizens' confidence and trust in the smart city [30, p. 506]. This could consequently reduce their willingness to participate or cooperate in the development and operation of the smart city, as well as lower the rate of adoption of new services and functionalities.

This concludes the brief, non-exhaustive summary of existing security threats against smart networks such as those used in smart cities. The above threats were focused on

due to their prominence in the context of networked and wireless devices and systems. Potential approaches to resolve these issues are discussed in later in chapter 4, specifically in sections 4.2–4.4.

3.3 Major areas of interest

Ubiquitous information networks with a maximal coverage can benefit smart cities by enabling the development of new services and businesses based on the available data. These endeavours include improvements to the efficiency and functionality of the public sector and the capabilities and quality of life of their citizens. As such, assuming cooperation between the potentially participating parties, the beneficiaries are, inter alia, the public authorities, local businesses, the industry, and the citizens.

Synergy between the smart city and its local industry and businesses is beneficial in the evolution of the city. The city benefits from increased employment and commerce. The industry and business, on the other hand, can take advantage of e.g. improved logistics and product development opportunities enabled by analysis of data provided by the city.

Among the forefront of the possible use cases of this information are increased efficiency in operation, better capabilities to iteratively develop the city based on realistic and locally applicable data, and increased citizen participation in various aspects of the development of the city. These areas of interest are further discussed and examined in the following subsections 3.3.1, 3.3.2, and 3.3.3, respectively.

3.3.1 Performance

One of the main benefits of smart cities, and their information infrastructures, is the opportunity of using previously unavailable data to improve the performance of various aspects of the city. In this subsection, the effects this has on infrastructure and buildings, traffic and public transit, healthcare, agriculture, and education.

Infrastructure, including power grid, water supply, communication network, roads, and bridges, like buildings, can be made more stable and more efficient with the introduction of e.g. smart meters for consumption or used capacity, as well as detection of strain, wear, and damage using sensors. Real-time measuring with smart meters can be used to improve the load balance of the respective networks as well as load redistribution during partial outages. Similarly, being able to monitor the condition of structures makes their maintenance more efficient and can act as a pre-emptive measure against severe structural damage.

Automation of traffic control, and eventually vehicles themselves, enables the sustainable, both economically and ecologically, development of transport. Smart traffic systems, based on sensor and user data, could be used to reroute traffic in case of accidents, reduce the idle time of vehicles, and better plan public transit routes.

The healthcare of a smart city benefits from its data infrastructure through the use of medical IoT, such as wearable sensors or medicine dispensers, which can be used to reduce the number of medical visits and more accurately prescribe medicine and adjust their dosage. Additionally, automated analysis can be used at healthcare facilities as well as in the patients' homes in order to e.g. alert a doctor when the condition of their patient deteriorates.

Climate-smart agriculture is enabled with the use of IoT in the monitoring and tending to the crops, livestock, storage and logistics [31, p. 11]. Efficiency is also improved by automating the monitoring of soil quality and prediction of weather patterns. These approaches reduce the amount of waste, environmental pollution, and the cost of farming [31, p. 11]. Additionally, due to the enhanced and more accurate methods, the agricultural yield is increased.

The systems of a smart city are not limited to the cyber-physical systems and examples described above but can also affect, for example, education. Electronic and virtual learning environments can be used to improve children's learning experience, e.g. with

gamification, detect learning difficulties earlier, and provide personalised guidance. These data can be collected throughout the children's education and analysed to discover and improve inefficacious areas. However, as this data collection spans through the majority of the pupils' and students' lives, care must be taken with regard to their retention period, as examined later in the discussion on privacy risks in section 4.1.

3.3.2 Iterative city development

Iterative development is suitable for smart cities, as the effects caused by changes in the functionality of the cities, e.g. traffic, services, or education, can take a notable period of time traditionally before they are directly observable. With the capability of the smart cities to process myriad data, the influence of the development can be detected earlier. This enables a gradual process where features based and built on earlier ones can be effectively tested and, if necessary, adjusted.

For example, traffic planning can be made significantly more efficient through smart traffic, as data from air quality sensors, movement sensors, and traffic cameras are constantly available. Similarly, education, especially when utilising virtual environments, can be evaluated both on the general and individual level to identify areas that require further improvements during the next iterative cycle.

Private and public services can use their customer data to improve their operation and supply. Examples of such targets of improvements include user or customer experience, convenience, and competitiveness in private businesses, as well as accessibility, simplicity, and availability of public services.

In addition to more effective detection of issues, iterative development allows the city to reap the benefits of the digitalisation earlier as the changes are modular instead of monolithic. This modularity can be beneficial for the adoption of new systems if the citizens do not feel overwhelmed by the number of changes. The granularity of the gathered data will also aid in pinpointing specific issues, which require further improvement.

3.3.3 Citizen participation

As technology advances, and consequently new types of e.g. services are enabled by this, cities can focus too much on what they can achieve instead of what the citizens require. Additional driving forces behind public initiatives in smart cities include vendor lobbying, and optimistic visions of future. [32, p. 100] These issues can result in information systems and services which do not serve the needs of the users, e.g. citizens, but could instead make tasks more complex or time-consuming, akin to the Apotti system discussed in 2.5.3.

During the design and development of smart cities, and the relevant information systems, their citizens could be considered to be their users or active participants [32, p. 97–98]. If they are seen as users, their potential of influence is limited to e.g. using or avoiding the services. However, if they are involved as active participants, the city can benefit from the perspective and experience in tailoring the services to more effectively improve the function of the city and the quality of its citizens' lives.

Participation of the citizens in the city development, e.g. through direct influence or feedback, can be seen as a form of co-production. They are more likely to get involved in this process if they find the end result, such as a service, valuable. [32, p. 104] When they do, the participation can be due to demand or on their own initiative. In the former case, the smart city could, for example, set objectives, such as environmental sustainability, and obligations for the citizens to achieve these objectives. If the citizens change their own behaviour to accomplish these goals due to the obligation, the former description applies. Albeit this form of participation is necessary, it is often better for the citizens to contribute of their own volition.

An example of voluntary participation is the sharing of the knowledge, expertise, and needs of the citizens. Traditionally, this could be achieved e.g. via gatherings and public meetings. The ICT available in smart cities introduces additional methods, such as through social media platforms, that can be used to reach the same goal. Gathering these

data, as well as the citizens' opinions on and propositions for public initiatives is also called citizen sourcing [32, p. 106].

In addition to the above type of citizen sourcing, smart cities require data to ensure a steady operation of their services. In order to receive the necessary personal data to develop, inter alia, healthcare, mobility, and education services, citizen cooperation is required. They can be collected e.g. through smart devices, medical IoT, and online services [32, p. 108]. However, due to their sensitive nature, this should be performed with the consent of the data subjects. As such, there should be accessible and available ways for the citizens to participate, be it via feedback, voicing opinions, or generating usage data. Some examples are covered later in the discussion on avoidance in section 4.4.

3.4 Contemporary smart cities

There are multiple currently ongoing smart city projects around the globe. Most of these are undertaken by large cities, such as Amsterdam, Copenhagen, New York, Toronto, and Vienna. Depending on the city, the emphases of the projects have been placed in a variety of aspects, such as public transit, energy, or citizens. In this section, the focus is on Amsterdam and Vienna, and their approaches to becoming smart cities. These cities are chosen based on the availability of information on their strategies and projects.

The smart city project of Amsterdam focuses on six different themes: digital city, energy, mobility, circular city, governance and education, and citizens and living. These themes cover projects such as storage and trade of excess renewable energy, use of electric vehicles as a backup battery during blackouts, a portal for accessibility to open data of the city, a traffic management system, and a protocol for interconnecting smart cities. [33] Overall, Amsterdam aims to provide an all-encompassing smart environment that improves the quality, and increased reliability, of the lives of their citizens.

Vienna, as per their framework strategy, focuses on three main sets of goals: resources, quality of life, and innovation. Resource goals include energy, mobility, infrastructure, and buildings, e.g. improved energy efficiency, increase in carbon-free modes of transport, standardising zero-energy buildings, and establishing a city-comprehensive wireless network. Quality of life issues, on the other hand, cover social inclusion, participation, healthcare, and environment, such as emphasis on remote patient healthcare, and environmentally friendly waste management. Finally, innovation issues are comprised of education, economy, and research, technology and innovation, e.g. increasing importance as a research and business centre, and higher average education level. [34]

Vienna, then, attempts to utilise its population density together with technology to minimise the amount of travel required during workdays and spare time, thus reducing emissions and energy consumption. Additionally, they aim for open governance e.g. via allowing the citizens to partake and follow public projects with digital services.

The framework strategy of Vienna [34] sets clear goals and approaches for reaching those goals within the allotted time frame. This framework also specifies that the citizens are free to participate by ”voicing, discussing and implementing” their ideas for the city. However, it does not provide means to accomplish this. Comparatively, the smart city project of Amsterdam provides an accessible list of currently on-going, as well as past, projects [33]. They enable the citizens, as well as potential third party collaborators, to submit projects related to the development of the city development. Nevertheless, the lack of a clear, accessible strategy makes it more challenging to keep a track of the overall goals and progress of the smart city.

3.5 Small smart cities

Smart city projects, due to their magnitude, benefit from the resources available in large cities and metropolitan areas. However, their inertia can slow down the implementation

of the infrastructure and information systems. Small smart cities are inherently more agile and able to experiment with alterations of these systems. This subsection covers the advantages and disadvantages small smart city implementations when compared to larger cities.

Small cities are likely to have a homogeneous population where their demographic variance is small. This has the benefit of making it easier to develop solutions that are useful and valuable for most, if not all, of the citizens. Additionally, the smaller scale enables more agile iterative development, as discussed in 3.3.2. With agile development, the process could be parallelised by simultaneously designing the next, developing the current, and gathering feedback and suggestions for the previous features. This improves efficiency of time usage and can, as a consequence, reduce the total cost of the project.

The expansion of the ”smartness” of a small smart city, whether through integration or augmentation of commercial solutions, or development new ones, is helped by the potential to use the city itself as a living laboratory. This applies especially if the project involves cooperation with local businesses or industry specialised in the relevant technologies. Testing locally, if any of the citizens' personal data are processed during, also strengthens their protection as the data remain close to their source. Additionally, collaboration between the city, businesses, and industry could be utilised to productise, partially or wholly, the resulting smart city.

Small smart cities, as a result of their smaller scale and population, can be influenced by fluctuations in the public opinions on the details of smart city implementation. These sways can be caused by e.g. experiences from testing; spread of new information, misinformation, or disinformation about the chosen technologies or approaches; or changes in trust towards one or multiple of the participating parties. Additionally, if the chosen approach is too closely tailored to the requirements of a given small city, it could suffer from scalability issues. These issues could then hinder or even prevent potential attempts of applying similar methodology to larger instances of smart cities.

Chapter 4

Primary domains of concern

This chapter covers the primary domains of concern with regard to trust in smart city implementations, identified in the previous chapters, in more detail. The concerns discussed in sections 4.1–4.4 are protection of the citizens' privacy as their data are collected and processed, approaches for protecting these data whether at rest or in process, reliability of the used systems as it effects the lives of citizens, and users' potential avoidance of the provided systems, devices, and services required for the smart cities to operate optimally.

These concerns are focused on because they directly affect or are affected by the citizens' trust towards their smart city. Some of these effects influence their initial trust and expectations of the outcomes of projects, while others are primarily in place during the operation of a smart city. Additionally, recommended approaches are given for each of the discussed concerns. These approaches aim to solve the underlying problems or mitigate their negative effects if no solutions are readily available or require further development outside of the scope of the smart city.

4.1 Privacy protection

Given the citizens living in a smart city are strongly dependent on the operation of their smart environment comprising, inter alia, of interconnected devices, online services, and

sensor-based automated systems, they should be able to expect the city to ensure the protection of their privacy. To fulfil this expectation, and thus to help transition the citizens' trust from forced towards earned, privacy should be incorporated to the implementation from design on. However, as the implementation of privacy-enhancing and -protecting features inherently increases the cost of the systems, limitations apply based on the available resources.

One of the foremost concerns with ubiquitous data collection is that of privacy. For a while, the various forms of data collection utilised by products and services, the methods of data processing, and the retention periods, among others, were not systematically regulated or supervised. This enabled the collection of comprehensive datasets of users, sometimes gathered without their owners' consent, which could have been received unambiguously or e.g. through ambiguous notices or hidden in a long list of terms and conditions.

As a response to the "wild west" of data economy, the recently enforced GDPR has introduced a number of new data rights for European citizens as well as obligations for data controllers and data processors. The notable rights and obligations related to privacy are discussed here and those related to data protection in section 4.2.

The articles 5 and 6 of GDPR limit both the collection and processing of personal data. Collecting such data is allowed, with the subject's unambiguous and explicit consent, for clearly and explicitly specified purposes. These purposes are not allowed to be expanded after consent has been originally given. Additionally, the amount of data collected should be kept to the minimum that is required by their specific purpose, and the data should remain personally identifiable *"for no longer than is necessary"* for the purposes the subject consented to. [4]

These principles are important, especially in the context of smart cities, for the minimisation of risks relating to the citizens' privacy and the potential of misuse of the collected data in the present or in the future. Their retention periods should be limited, and

where longer periods are required, for example for statistical purposes, the data should be appropriately anonymised so as to prevent them being linked to the persons. This anonymisation process is not without its own complications, however, and these are further discussed in the following subsection, 4.1.1.

The minimisation of personal data is emphasised in GDPR and should be a focus e.g. in conjunction with sensors located in public spaces if these sensors are able to record such data. Use cases of such sensors could be e.g. cameras detecting the amount of motorised or pedestrian traffic in each direction at intersections to determine an optimal schedule for traffic lights. In such cases it would be sufficient to only detect the amount of people from their body shapes, whereas being able to detect facial features would be excessive.

If personal data are not sufficiently anonymised during the processing or after they are no longer needed for their purpose, a risk of their potential future abuse remains. In a similar vein to the changes in surveillance and privacy laws discussed in section 2.5.1, it is not enough to rely on the current trust a person might have to e.g. the administrators or council members of the smart city. The data should then be future proofed sufficiently to prevent them from being used in any unintended ways in the future.

In addition to devices, services, and information systems tailor-made for the smart city, third-party products are also likely used especially inside the smart homes. When their use is required by the city, the following considerations must be taken into account. Additionally, the citizens should be made aware of potential privacy risks associated with consumer-grade smart home devices and simple unambiguous ways they could improve their security.

In the case the use of externally produced services or devices is required, their functionality should be thoroughly dissected. In cases where they are used to handle data, the necessity of inclusion of personally identifiable information in the processing should be closely scrutinised. If such information has to be transferred to external services, a risk

evaluation on the citizens' privacy should be performed in order to avoid cases of abuse [35]. Additionally, voice-controlled devices should not be used to transmit recordings of the users to the service providers without the users' explicit and informed consent [36], [37].

In addition to indoor devices, privacy risks are also caused by e.g. security cameras or IP cameras. These could be used, for example, by the city to monitor traffic, or by the residents to protect their homes. The latter use case, especially, has evolved into a major market within the past decade with a number of consumer-grade home security solutions being offered with varying levels of Internet-connectivity. This connectivity can be used for remote access, device interoperability, or cloud storage and processing.

Unfortunately, some of these security cameras are actively developed towards a surveillance network [38], with warrantless access provided to law enforcement agents [39]. In some cases, the lax approach to security of their manufacturers can lead to attackers gaining access to these devices and being able to monitor their owners.

One issue with smart doorbell cameras, as well as other road-facing cameras, is their potential for the surveillance of the neighbourhood beyond their intended use. While these devices could be purchased to monitor one's personal property, in the case of houses, or immediate vicinity of apartments, the cameras will also record any traffic and people that enter their field of view. The captured footage could then be combined with e.g. facial recognition to continuously watch the people, such as passers-by or neighbours, nearby [40].

These are examples of cases where privately purchased equipment can become a privacy risk to citizens. However, this risk is not preventable as the devices are not owned by the city. Thus, the citizens should be adequately informed of the risks involved with network-connected security devices.

4.1.1 Anonymisation and pseudonymisation of data

Pseudonymisation of data is a form of reversible privacy that ensures the processed data cannot be attributed to a single subject without the use of additional external data [4]. Comparatively, data anonymisation ensures that subjects cannot be identified through the processing of their personal data even in the presence of extra information [3, p. 2].

In order to protect the citizens' privacy, their aggregated data should be limited in range, in accordance with point (c) of GDPR Article 5(1), and remain identifiable or linkable to specific persons for a limited time, as specified in point (e) of Article 5(1). However, if only anonymised data are collected, the GDPR does not apply as per Article 11(1) [4]. Thus, during the processing and storage of data, pseudonymisation should be used while the subjects' identifiability is required, and anonymisation at other times.

The effectiveness of pseudonymisation and anonymisation methods can be evaluated e.g. based on the level of protection they grant against singling out, linkability, and inference [41, p. 11–12]. A subject can be singled out if they can be identified by an attacker through isolating their personal data contained in a database. This does not imply the revelation of the subject's identity to the attacker; only the presence of a singular owner of the data is revealed. As a direct result, pseudonymisation does not protect individuals against being singled out.

Linkability means the possibility of linking separate records from one or more databases to the same individual or group [41, p. 11]. This type of linking can be achieved with multiple types of data such as a subject's person, role, relationships to other subjects, and transactions [3, p. 6]. Respectively, the linkability of each of these types can be reduced through the use of pseudonyms. Reuse of these pseudonyms, especially in the context of a person, increases the likelihood that two records can be linked through analysis but can be used by the data subject to build a reputation.

Alternatively, e.g. by using a sufficient number of databases or sophisticated algorithms, an attacker could infer unknown variables, at a statistically significant probability,

from available data [41, p. 12]. Thus, this type of an attack can be made more effective for example through the use of machine learning. Like being singled out, pseudonymisation does not provide protection against inference attacks.

Two examples of data anonymisation methods are differential privacy [42] and t-closeness. Differential privacy is used to e.g. provide anonymised views of processed data such that the subject of the original data cannot be deduced from the output. This is achieved by inserting noise to the published results of the queries used to process the data [41, p. 15]. Consequently, analyses performed on two databases, where only one of them contains the contribution of a given individual, should provide results that differ by a small amount, ε. This principle is shown below in figure 4.1.

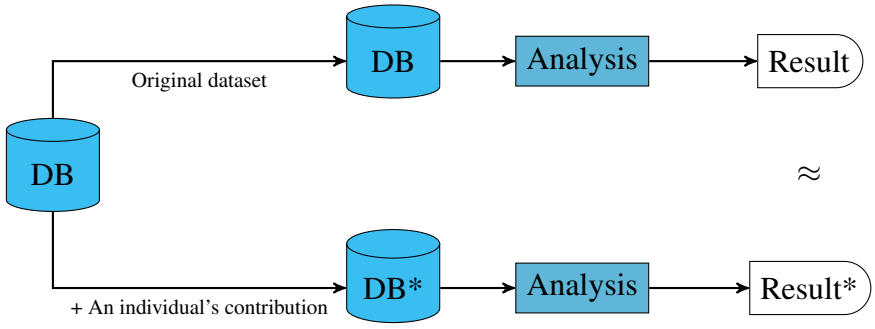

Figure 4.1: Analysis results should not differ significantly if an individual's data are added or removed when differentially private queries are used.

Differential privacy has potential for protection against all three aforementioned attack approaches but is susceptible to implementation flaws that can enable linking and inference attacks. If the used queries are not monitored by the system implementing differential privacy, an attacker could use a combination of discrete queries to link the results or to deduce the values of omitted properties. However, due to its potential as a tool for anonymous data analysis without the disclosure of the raw data, differential privacy should be capitalised.

T-closeness, on the other hand, anonymises the data by generating equivalence classes from the dataset where each class must contain at least l discrete values for each attribute,

other than the equivalent attribute, in the equivalence class. Additionally, the distributions of these attributes in each class should be close to their distributions in the entire dataset. [41, p. 18] This protects individuals from being vulnerable to being singled out and prevents an attacker from performing inference attacks with an absolute certainty of success. However, due to the inherently smaller sizes of the equivalence classes, linking multiple data points to the same subject is easier.

4.1.2 Challenges with anonymisation and pseudonymisation

Re-identification attacks are a major threat against anonymisation and pseudonymisation. By definition, pseudonymisation is more vulnerable to this type of attack due to the inherent linkability of the data subjects. The amount of external data an attacker would need to achieve this re-identification simply depends on the level of pseudonymisation. If, on the other hand, the data are anonymised, an attacker should not be able to re-identify the subjects. However, there are many cases where this can be done due to the difficulty of anonymising data.

For data to be useful to a data processor, they should contain more information than noise. As long as data entries are linkable to a subject source, an attacker could infer information about the said source by correlating the dataset with external data. Thus, for anonymisation to be effective, each of the entries of a dataset should be indistinguishable from the others.

This has been discussed previously e.g. by Narayanan and Shmatikov [43], Elliot et al. [44], and Ohm [45]. Algorithms used for re-identification use a large number of personal properties, with high granularity, variety, and stability, enabling re-identification of a subject whenever a sufficient amount of data is available [43, p. 26]. One challenge related to this issue is the difficulty of determining which types of data could disclose the identity of an individual [44, p. 205]. Additionally, Ohm states that it is *"naïve to assume that the adversary will be unable to find the particular piece of data needed to*

unlock anonymised data" [45, p. 1724], emphasising the importance of the potential of an attacker to gain access to an arbitrary amount of data, which will inevitably lead to re-identification as per the previous.

These issues make anonymisation models such as release-and-forget [45, p. 1751] not viable in the context of smart cities. Due to the inherently identifiable nature of the collected data, it is challenging, if not impossible, to anonymise them to the extent that re-identification would not remain a threat in the present or in the future. Thus, the data collected should remain in the possession of the data controller for their entire retention period. During the retention period, effective anonymity could be achieved using the aforementioned differential privacy methods. Finally, after the data are no longer required or relevant, they should be deleted instead of anonymised and released. The potential for negative side effects this has to research that could be done using the data is mitigated by differentially private access to them during their retention.

4.1.3 Recommendations

Given the previous discussion on privacy concerns related to the citizens' forced trust in the responsible and non-invasive data collection performed by a smart city, the following are recommendations on methods and approaches that can be used to mitigate potential risks and increase the level of voluntary trust experienced by the said citizens. The methods and approaches cover the entire life cycle of the collected data from system design to data disposal.

PR1 **Quantify the required level of privacy.** In order to be able to determine whether the privacy goals have been met within the smart city and its data processing, as well as those of private affiliates, they should first be clearly defined. These requirements can then be compared with the level of privacy protection provided by the chosen technologies [30] to determine whether the requirements are fulfilled or found wanting. Additionally, each participating organisation should actively

communicate their specific requirements with the other entities in order to better coordinate and ensure the fulfilment of privacy requirements city-wide [30, p. 506].

PR2 **Implement privacy by design.** As described by Cavoukian [46], privacy by design places emphasis on, inter alia, preventing privacy issues before they can occur, allowing users to opt in into data collection instead of opting out, and avoiding the false dichotomy of privacy vs. security. Incorporating this methodology into the design, implementation, and operation of a smart city is crucial for the preservation of its residents' privacy.

One major aspect of privacy by design is user-centricity of the privacy settings, options, and notices [46]. User trust can be improved by clearly informing them about any and all types of collection of personal data. Additionally, in any used systems that support e.g. personalisation, the citizens should be able to freely choose their participation in said processes, as well as be provided with the privacy-preserving settings enabled by default. These factors, together with transparency, contribute to converting the experience of forced trust towards voluntary trust.

PR3 **Evaluate privacy threats using available models.** Privacy threat models, such as LINDDUN [47], or risk assessment guidelines, such as that of the ENISA [48], can be used to gain a comprehensive picture of the threats and risks posed e.g. by the data flows and disclosure. These processes are especially important for proactive and preventative protection of the data, and thus compatible with privacy by design.

Attention should also be paid to the components used within the deployed devices and systems. If, for example, a manufacturer is known to produce, or have produced, components vulnerable to attacks, especially remote, that could jeopardise the confidentiality of processed and stored data, the users' privacy is also threatened. In these cases, the use of such components should be reconsidered, or sufficient additional precautions taken to protect from the known threats.

Awareness of all of the potential threats and risks associated with the chosen

design and implementation of the used systems is necessary in order to sufficiently protect the citizens' personal data. Due to the complex structures of smart cities, as well as device and system interoperability requirements, these types of evaluation are necessary. User trust can additionally be gained through e.g. privacy audits as well as through the use of devices with a security or privacy certification, such as the recently launched IoT label of the National Cyber Security Centre Finland (NCSC-FI) [49].

PR4 **Minimise the mandatory amount of personal data collected.** As per the article 5(1) of the GDPR [4], the collected personal data should be limited to what is necessary for the operation of a smart city. This protects the citizens' privacy during the regular operation of the city as well as after potential data breaches. Additionally, collecting a minimal amount of data, and disposing of it as per last recommendation, helps mitigate the risks of them being misused. This, in turn, increases the amount of trust enjoyed by the city.

The necessity of data minimisation can be seen by considering the dataset available during the lifetime of an individual resident of a smart city. These data include records from education and healthcare, location and consumption data, as well as general public records. Unless the retention period of non-critical information is limited, it is possible to misuse the dataset for in-depth profiling of the citizens.

Additional data collection could be introduced e.g. through personal opt-in. Each citizen could decide whether they want to participate by opting into expanding the coverage of existing, or introducing new instances of, data collection. This could be achieved for example with an online service where the citizens could control the flow of their own data. This example is expanded on in the discussion of citizen participation in the section 4.4.

PR5 **Perform data analysis with differentially private methods.** Minimising the effect each individual citizens' data have on the results, while being able to perform

meaningful analysis on the effectively anonymised data is beneficial both for the subjects, since they cannot be singled out, and for the parties wishing to utilise the data. This enables their use for e.g. operation and development of the smart city and could be used as a data source for research without compromising the residents' privacy.

However, the used methods, such as ε-differentially private SQL engines, should be resistant to the potential issues mentioned in 4.1.1. The level of threat these issues could pose depends on the range of potential users of the datasets, as well as their exploitability. If, for example, an attacker could use a combination of queries to infer information about a specific data subject or a group of subjects, they could automate the attack and systematically extract identifiable information.

PR6 **Dispose of data at the end of their retention period.** Due to the inherent difficulties of irreversibly anonymising data, and a significant risk of re-identification with a sufficiently large set of external data, as discussed in 4.1.2, releasing the collected data, even after anonymisation, threatens the citizens' privacy. Thus, the deletion of data is preferable to their release.

PR7 **Inform the citizens about the privacy risks of smart devices.** The ever-growing smart device market allows a plethora of devices with a varying quality of design and security to be available for purchase to consumers. Their use cases can range from general convenience to home security. Their marketing often omits verifiable claims about the security of the devices themselves, potentially endangering their owners' and others' privacy. It is then important to provide simple, clear, and easily accessible information to the citizens about the potential privacy threats posed by consumer-grade smart devices. Additionally, the use of products with e.g. the IoT certification of NCSC-FI should be recommended.

4.2 Data security and data protection

As has been earlier mentioned, data collection has a major role in the operation and development of a smart city. Consequently, the said data should be protected against threats including unauthorised access, eavesdropping, data corruption, and disclosure. Additionally, their processing should be monitored and restricted in order to prevent potential cases of unauthorised or non-consensual use.

Technical and theoretical aspects of data security are discussed in subsection 4.2.1. Required and recommended protective measures are considered in various states and contexts of data. The utilisation of the data is discussed in 4.2.2 as well as the influence the citizens have on the allowed use cases and data access limitations.

4.2.1 Security

The data, e.g. from infrastructural sensors, smart meters, and smart devices, associated with smart cities should remain confidential and have their integrity protected throughout their lifetime, from generation, through transit and retention, to deletion. The citizens should be able to trust the chosen implementation of a smart city to keep their data secure. An uncompromised security is a pre-requisite for their privacy. This subsection covers a number of important issues and solutions related to the handling of data during their retention period.

Sufficient measures should be taken to ensure this security and privacy of the data whether they are in transit, at rest, or in process. Data are in the state of transit when they are transmitted between or within systems. While in transit, they are vulnerable to, inter alia, eavesdropping, replay, and man in the middle (MitM) attacks. Without sufficient measures to ensure confidentiality, an attacker could capture the data during transmission and, depending on their nature, use them e.g. for profiling or corporate espionage. Additionally, if the transmission crosses national borders, it could be subjected to wiretapping

e.g. by intelligence agencies, potentially compromising the citizens' privacy.

In the case of the citizens, such sniffing attacks mainly affect the aforementioned devices in smart homes, such as home appliances and meters, cars with an in-built Internet connection, as well as mobile devices. Additionally, public cameras, when used beyond e.g. motion or body count detection, could have their feeds, if left open, eavesdropped. Similarly, security cameras sold for home use could reveal e.g. the identities and daily schedules of neighbourhoods, as discussed in section 4.1.

To protect the data traffic from eavesdropping attacks, the devices should protect their confidentiality by encrypting the data. The number of available cryptographic primitives is limited by device-specific resource constrains. Nevertheless, whenever possible the confidentiality of the transmissions should be protected. In smaller devices, symmetric cryptography could be more efficient due to e.g. smaller key size and available efficient hardware implementations [50, p. 22]. In these cases, the used keys should be generated initially using e.g. elliptic curve -based key exchange protocols in order to avoid risks caused by using a permanent device-specific key. Additionally, the implementations should be made resilient against side-channel attacks such as timing attacks to further protect the devices against key extraction.

The generation of cryptographic keys can be too resource-intensive e.g. in the case of small implanted medical devices. In these cases, to protect the medical data, development of lightweight algorithms and protocols is essential. Ideally, the measurements themselves could be utilised in these algorithms. One such approach is proposed by Sanaz [51, p. 42–46] in her dissertation on end-to-end security of medical IoT. In the architecture proposed and studied in the thesis, keys are generated based on the patient's measured electrocardiogram features, thus using the gathered biometric data in its own encryption.

Thus, in the absence of sufficiently lightweight yet secure key derivation methods, resource-limited devices should communicate only with a limited set of authorised parties and using a limited set of allowed transactions, for allowing arbitrary entities to freely

interact with a device connected e.g. to the Wi-Fi of a smart home or the public sensor network could compromise the other devices in the network. An example solution for smart homes is the use of a lightweight blockchain proposed by Dorri et al. [52], which would also enable neighbouring homes to securely exchange information.

Even with the use of a whitelist of supported parties a device can communicate with, an attacker could attempt to impersonate one of them to be able to listen to the communication or gain access to the device. To prevent these scenarios, the used devices, as well as the hubs, gateways, and other whitelisted systems, should be able to prove their authenticity. This could be done by using device-specific fingerprints, provided e.g. by physical unclonable functions (PUFs). PUFs take advantage of the unique imperfections and physical properties of the silicon in each manufactured device [53, p. 10]. With PUF-enabled device authentication, it would be virtually impossible for an attacker to duplicate the physical properties of a given device in order to impersonate them.

In addition to confidentiality, the integrity of the transmitted data must be confirmed by the receiver. This requires the generation of digests from the transmitted data, e.g. with keyed-hash message authentication codes (HMACs). HMAC calculation could be done with a hardware implementation of authenticated encryption, in the case of resource-limited devices, or in software. By checking the authenticity of the messages before further processing them, the system can be protected against data falsification or manipulation. Additionally, by using nonces in each sent transmission, they are protected against replay attacks, where an attacker captures a message to replay it later.

Besides the more passive protection methods, such as encryption and integrity checks, the smart city should be actively protected against intrusions and other network-based attacks. Intrusion detection systems and firewalls are recommended to fulfil this requirement. IDSs should be used to determine anomalous traffic in the network and prevent potentially malicious actions on hosts. On the other hand, firewalls can be used to restrict access of external devices and machines e.g. to the infrastructural sensor network of the

smart city. These tools can also, combined, protect the city from harmful attacks against the information infrastructure, such as DoS or compromised devices.

One approach, proposed by Sen et al. [54, p. 521], is a security model where the network protection is distributed between multiple layers: the smart devices collecting the data, a data scrutiny layer, and the servers processing the data. The devices run secure software that attempts to protect them from malware. The scrutiny layer, on the other hand, filters the communications between the smart network and the server to prevent malicious traffic from reaching the server, and potentially infecting it. Finally, the server verifies the data passing through it to detect corruption attempts.

This type of multilayer security, or defence-in-depth, aids in ensuring the systems, e.g. the smart network, remain secure even if some of the security precautions fail or are compromised. Additionally, it lowers the probability of these faults causing further faults in the system, whether directly, for example due to a dependency, or indirectly, such as allowing an attacker target other components. As such, it also acts as a mitigating factor against the cascading effects of system vulnerabilities described in subsection 3.2.2.

It is useful to outline and model the data flows within and from the concerned systems. These flows should be classified based e.g. on their sensitivity, and the lifespan of the transmitted data. Sensitivity deals with the level of confidentiality or privacy that should be achieved for the transmission to be considered secure. The lifespan of the data means the amount of time they remain relevant for processing. Data with a longer lifespan thus require better security.

Akin to data in transit, when at rest, i.e. stored for example in a database or locally on a device, the data should remain secure against attempts against their confidentiality and integrity, and unauthorised access. Additionally, if they are stored in a foreign country, whether by choice or due to the used services, the local applicable laws, including privacy protection and cases when the confidentiality of the data could be compromised, must be considered.

Confidentiality and integrity can be protected at rest similarly to in transit. The increased available resources, however, increase the number of viable solutions, such as increased key sizes and slower HMAC functions. Additionally, keeping logs on events such as data addition, modification, and deletion is vital to ensure the integrity of stored data. Accurate logs are also a significant defence in detecting cases of unauthorised access to the data.

However, care must be taken to ensure the logging process complies with the GDPR. The additional restrictions on the storage of personal data can limit the amount of information that are allowed to be stored significantly if the citizens' consent is not received for their collection. Logging and processing for the operation of public authorities have some exceptions, e.g. in article 6(1) [4], as well as for the prevention of fraud, but in general personal data should not be logged.

Protection of the data while they are processed is a greater challenge in comparison. With the aforementioned methods of ensuring confidentiality, the data are not usable as-is for e.g. analysis. In order to use them, they would first have to be decrypted, which has the potential of compromising the data if done on untrusted systems.

Trusted computing should then be used in the processing. The data owners, i.e. in a smart city the citizens, should be able to trust their personal information is securely processed and retain their confidentiality and integrity. This could be achieved with e.g. trusted platform modules (TPMs) or technologies similar to the Software Guard Extensions (SGX) by Intel. Alternatively, eventually data could be processed using cryptographic primitives that support data analysis, such as homomorphic encryption (HE) [55] or functional encryption (FE) [56].

TPMs are secure processors that, when added to a system, can be used to, for example, generate and store cryptographic keys, protect the system from tampering, and attest the integrity of the system. They can be used to determine the state of the host machine, by deriving cryptographic digests e.g. from its firmware, connected peripherals, and installed

software. These digests are then securely stored on the modules and used as a reference to detect changes in the system. If such changes are detected, during its start-up or during operation, the TPM will halt its operation. This process could also be performed remotely, allowing for remote attestation.

SGX enable suitable hosts to be used as secure remote computing platforms. They provide isolated, encrypted environments, enclaves, each of which are assigned their own regions in the system memory. Additionally, before uploading and potentially exposing information, a user of the SGX can request a digest of the current state of the module in order to verify its contents, thus preventing e.g. a hostile host from inserting malicious software. An SGX-type approach, regardless of the manufacturer, would then be a viable option for the processing of sensitive information like the citizens' data.

While TPMs and SGX are well-suited for processing tasks, which require trustworthy platforms and systems due to the nature of the handled data, they can be vulnerable to a number of attacks e.g. due to the processor architecture used in the host machine. Two recent examples are the timing and lattice attacks against TPMs [57] and speculative execution attacks against SGX [58]. The former exploited timing information of the processor, when it generates signatures, to recover used private keys. The latter exploits speculative execution of modern Intel processors and leaks in-flight data from various buffers. As mentioned in subsection 4.1.3, these types of vulnerabilities threaten the citizens' privacy, if left unpatched, and should be included in the threat and risk analyses.

Homomorphic encryption and functional encryption allow computation on encrypted data, forgoing their decryption. In HE the computations are performed on the encrypted data and the results remain encrypted [55, p. 1–2]. The amount of supported operations depends on the level of homomorphism of the algorithm, ranging from simply addition and subtraction to arbitrary operations in fully homomorphic encryption. Thus, HE can be used by a data owner to e.g. outsource analysis to external cloud services as confidentiality is never compromised. However, few of the currently available HE algorithms are efficient

enough to be considered viable for general use and thus further research and development is required.

On the other hand, FE allows the data owner to generate a function that, given different secret keys and the encrypted data, outputs decrypted analytics results based on the design of the scheme [56, p. 1]. The authority responsible for setting up the scheme can then also determine and define the types of computations that can be performed on the data. This feature is similar to the differential privacy discussed in subsection 4.1.1 in that it enables the production of analyses based on datasets without revealing information about any single data subject. While the field of functional encryption is still relatively young, e.g. the EU has co-funded the Functional Encryption Technologies -project [59] to develop FE systems for ICT.

TPMs, SGX, HE, FE, IDSs, and firewalls, inter alia, are thus a versatile selection of tools for a smart city. The capability of ensuring the trustworthiness and integrity of the used systems before performing computations or analytics is essential to retain the citizens' trust in their smart city. Alternatively, being able to securely perform analyses despite potentially untrusted systems through the use of homomorphic encryption further ensures the confidentiality of the data. Additionally, functional encryption provides a polymorphous method for disclosing selected statistics of the data in a privacy-preserving manner. Finally, guaranteeing the integrity and availability of the core infrastructure of the smart city protects the city from harmful side effects of corrupted and missing data.

4.2.2 Data utilisation and access management

Smart city data can originate from multiple sources, as discussed in 3.3. To recapitulate, their sources include personal devices, smart homes, inbuilt sensors in buildings and bridges, infrastructural sensors such as traffic and smart grid, and industry. Additional data can be gathered, inter alia, from education, with virtual learning environments, and healthcare, with worn and implanted sensors and medical IoT devices.

Some of these data, such as those from structures, infrastructure, or industry, can be utilised to optimise the operation of the smart city without introducing any risks to the citizens, assuming e.g. smart traffic sensors are not able to produce personally identifiable information. However, the remaining sources produce highly personal information such as daily location history or biometric data. Processing these types of data requires a thorough data protection impact assessment, as discussed in subsection 2.5.2. Additionally, the citizens should be made knowledgeable about all processing involving sensitive data.

Smart healthcare is an example of a service that can benefit from IoT and sensor networks and their capacity for generating and processing vast amounts of medical data. One of the most useful yet potentially dangerous application of medical IoT is the automation of medication, such as insulin or asthma medication, to safely administer appropriate doses when required. The used data are intrinsically sensitive, and thus should be protected throughout their lifespan within the system.

The potential for harm in badly designed medical IoT was exemplified by the recent cases of insulin pump [60] and pacemaker [61] vulnerabilities that could be exploited lethally. Ensuring the confidentiality, integrity, and availability of these devices and the data the process, should then be possible and practical before widespread adoption of medical IoT devices. Unfortunately, the currently available suite of security solutions applicable to implanted and wearable medical sensors and devices alike is limited, as discussed in 4.2.1.

Upholding transparency is important in the design of the data processing of a smart city. The data subjects should be able to know, at will, the extent to which their information is used, as discussed later in 4.4.1. Additionally, they should be able to object to expansion of the utilisation of their data. Finally, similar principles should also naturally apply to controlling the access to any non-anonymised data. This type of transparency was also included as the sixth principle of privacy by design [46] discussed in the privacy recommendations of subsection 4.1.3.

When designing the data processing of a smart city, the distribution of processing responsibilities between the private and public sectors should be a point of interest. Given the exemptions to the GDPR discussed in 2.5.2, there are potential concerns regarding misuse and disclosure of personal data. Depending on the severity of the impact such incidents could have on the subject and given the current data protection act [17], some aspects of the data management responsibility of the smart city should be outsourced to the private sector.

Such outsourcing itself introduces new risks for the citizens' privacy and data protection. For example, if the benefits a private party would receive from data abuse were greater than the potential penalties, the risk of misuse is higher. Thus, the responsibilities and permissions of these external service providers should be clearly defined to mitigate, if not eliminate, these risks. However, were a private party to breach the data protection act, they would be held accountable and fined as per article 83 of the GDPR [4]. A public authority, on the other hand, would not be subjected to administrative fines, and thus poses a greater risk when handling sensitive data, as this does not provide motivation for complying with the act. As such, a balance should be found for the distribution of the processing of sensitive personal data between the public and private sectors.

Eventually the expansion of services provided by the smart city might require the collection of new types of data or increasing the range of applications for existing data. In both cases the citizens should be informed about these plans ahead of time in order to adhere to the principle of transparency. In the former aforementioned case, the citizens should be able to monitor the usage of their data and, if possible without obstructing necessary city functions, opt out.

In the latter case, i.e. use of the readily available non-anonymised data in new contexts, the potential side effects on citizens should be thoroughly assessed. This applies whether such expansion is considered by the city or some other public authority as long as it requires the use of the residents' personal data. If privacy or data protection is-

sues are identified, these issues should be resolved before the process continues. These precautions help to pre-emptively avoid potential data misuse issues such as a form of a ”privilege escalation attack” described below.

In this context a privilege escalation attack refers to a, from the citizens' point of view, harmful situation where available information is allowed to be used in a context it was not originally collected for, potentially leading to e.g. their right to privacy [62] being compromised. This compromise could result in e.g. excessively comprehensive dataset or tracking capability of an individual or a group of individuals. Two examples of such cases are the recently introduced permission for the Finnish police and customs to use real-time video feed for facial recognition using biometrics available in the national person register [13], and the decision to create an EU-wide biometrics database, Common Identity Repository, which makes the biometric data of both EU and non-EU citizens easily searchable [63].

In these ”attacks” the given parties gained escalated access and utilisation privileges to the personal data of subjects. Such developments could then be seen as attacks against the privacy and freedoms of individuals, as the affected individuals' privacy rights have been undermined without prior notice or a chance to influence the outcome. Additionally, they can have a significantly negative effect on the level of trust enjoyed by the parties in the future.

4.2.3 Recommendations

In order to ensure the protection of the confidentiality and integrity of the data, and the privacy rights of the citizens, the following approaches are recommended based on the previous discussions on data security and protection. These approaches cover technical solutions as well as policies that collectively aim to minimise the risks related to any personal data handled by the city.

DR1 **Utilise trusted computing and platforms when possible.** While their use is not feasible in e.g. most of the used sensors and consumer-grade products, the use of trusted platforms, combined with clearly informing the citizens about this aspect of the smart city, in systems responsible for handling data encourages the citizens to trust their data to be processed using trustworthy equipment. TPMs and SGX, among other applicable and available technologies, can be used to ensure the used systems have not been tampered with, do not contain any malicious software, as well as securely store and generate cryptographic keys and run software remotely.

DR2 **Test the chosen security systems thoroughly before deployment.** Systems purchased from vendors for use in smart cities are often not tested [64]. Affected systems include networked devices such as smart traffic sensors and power meters. Additionally, some vendors refuse to sell their products, for testing purposes, to security researchers [64]. Due to potential security flaws e.g. in data confidentiality mechanisms, it is important for the cities to subject the systems, whether locally developed or bought from vendors, to testing in order to identify potentially severe security flaws.

DR3 **Take advantage of cryptographic primitives which support data analytics.** These techniques, such as HE and FE, enable secure processing and handling of data even without hardware that can be trusted to be uncompromised. Providing data processors only with data encrypted with HE protects the said information while still enabling their processing. Thus, it can be ensured that only the data controller has access to the processed, as well as raw, data. On the other hand, if the results of given analyses are wished, or required, to be published, FE allows the extraction of clearly specified results from the dataset without revealing any of the source information.

Currently the most applicable HE algorithms are still only somewhat homomorphic, as fully homomorphic, i.e. those that support arbitrary operations, solutions

are computationally demanding or produce too much noise to the results [55, p. 2]. Thus, their use cases are limited but among them are the secure processing of medical and financial data [55, p. 2]. Additionally, FE shows promise and, e.g. through the FENTEC project [59], feasible practical solutions should be available within the next decade.

DR4 **Distribute smart network protection onto multiple layers.** Implementing network security on all applicable levels between the sensors and the data analytics and processing centres should be prioritised over relying on a monolithic solution. As this can require a notable amount of resources, it is not suitable e.g. to resource-constrained sensors. However, on applicable sensors, their gateways, and the smart network this defence-in-depth approach can be used to improve the overall robustness of the smart city. Additionally, some of the resources of these components could be used to process the data ”in-flight”, i.e. between their origin and the processing centres. This reduces the amount of data that has to be transmitted, lowering the required data transfer capacity of the network.

DR5 **Monitor the network and data to detect and prevent attacks.** As smart cities are strongly dependent on the proper function and data reliability of their sensor networks, the city-operated information networks should be appropriately protected against external threats. Swift and dependable detection of occurring network- and host-based attacks is then a requirement for a smart city to prevent the compromise of its data, and thus operational input, flow, with potential to damage e.g. infrastructure or healthcare services.

DR6 **Take applicable data privacy and protection laws into account when data are stored or processed abroad.** The respective laws vary between countries, thus providing varying levels of protection from arbitrary access, inspection, and interception. Even international regulations such as the GDPR allow for differences in state-specific implementations, e.g. the possibility of the states to opt out of fining

public authorities for violations provided by GDPR.

As a consequence, whenever third-party services are used, the effects of the laws applicable to the chosen service provider on the data provided by the smart city should be closely scrutinised. From the point of view of the data subjects it is recommended to keep the data close to their source, and thus domestic data processors should be preferred unless the protection provided abroad is notably stronger. Additionally, if the data are transmitted via a country that actively performs deep packet inspection on traffic passing through it, the aforementioned gain in protection should also account for this added confidentiality risk.

DR7 **Balance data processing responsibilities between the public and private sector to maximise data protection.** The citizens' data protection could be improved by pairing the processing tasks and the respectively required data into groups by increasing level of sensitivity of information. These groups could then be separately evaluated to determine whether each task poses a notable risk to the data subject, and thus would require the added incentive for protection from the threat of an administrative fine as per the GDPR. The processing tasks identified to require it could then be allocated to trusted private third-party service providers.

DR8 **Follow the principle of least privilege.** A simple yet effective method to reduce risks related to misuse and disclosure of personal data is the minimisation of access and usage rights granted to those data. As such, these rights should be limited to the minimum set required to perform a task. Additionally, these tasks should be justified e.g. by their necessity for the function of the city or the consent of the owner of the data.

DR9 **Require the consent of the relevant data subjects before expanding the use cases of or access rights to personal data.** In addition to the principle of least privilege, in order to avoid potential abuse of gathered data in the future, they should be protected with a requirement of informed consent from the affected citizens.

This approach is important especially when personally identifiable information, e.g. biometrics, or medical or financial data, are processed. If, however, the data are anonymised before their utilisation, this recommendation does not apply.

4.3 System reliability, safety, and redundancy

Reliability engineering is a field that focuses on the dependability, as well as failure risks, of systems through the analysis of the reliabilities of their components. The reliability of a subsystem can be measured e.g. with the mean time before its failure. The minimisation of these risks is the main goal of reliability engineering. The dependencies of unwanted events and expected function of components on previous events or components can be displayed using e.g. fault tree diagrams or dependency diagrams.

In some cases, the reliability is not as important as another similar, but somewhat incompatible, property: safety. Safety engineering, similar to reliability engineering, analyses the failure risks of systems and aims to prevent safety issues even at the cost of reliability. Both of them, however, cover the effects and functionality of the systems on hardware- and software-level.

As societies develop towards more interconnectivity and dependence on technology, the reliability, and in some cases safety, of these technologies becomes increasingly important. Smart infrastructure, smart healthcare, and smart homes, inter alia, must be capable of functioning if the used systems suffer from a technical or software failure. A dumb mode of operation should always be available for maintaining basic functionalities in case such malfunctions occur.

The infrastructure, such as transportation, ICT, and mains grids and networks, of a smart city acts as its operational backbone and basis on which its services are built. Thus, their continuous function should be ensured; otherwise the city could grind to a halt. Transport, information, and communication networks affect, when partially or entirely

disabled, the function of the city considerably due to their central role in the collection of data.

Smart traffic, for instance, relies on a steady feed of environmental measurements related to vehicular and pedestrian traffic. If this data feed were to malfunction, without a functional dumb backup system, e.g. periodic switching of the traffic lights, the transit system could stop or, in a worse case, cause lethal accidents. A simple example of a fault tree diagram in the case of the data feed of smart traffic lights is shown in figure 4.2.

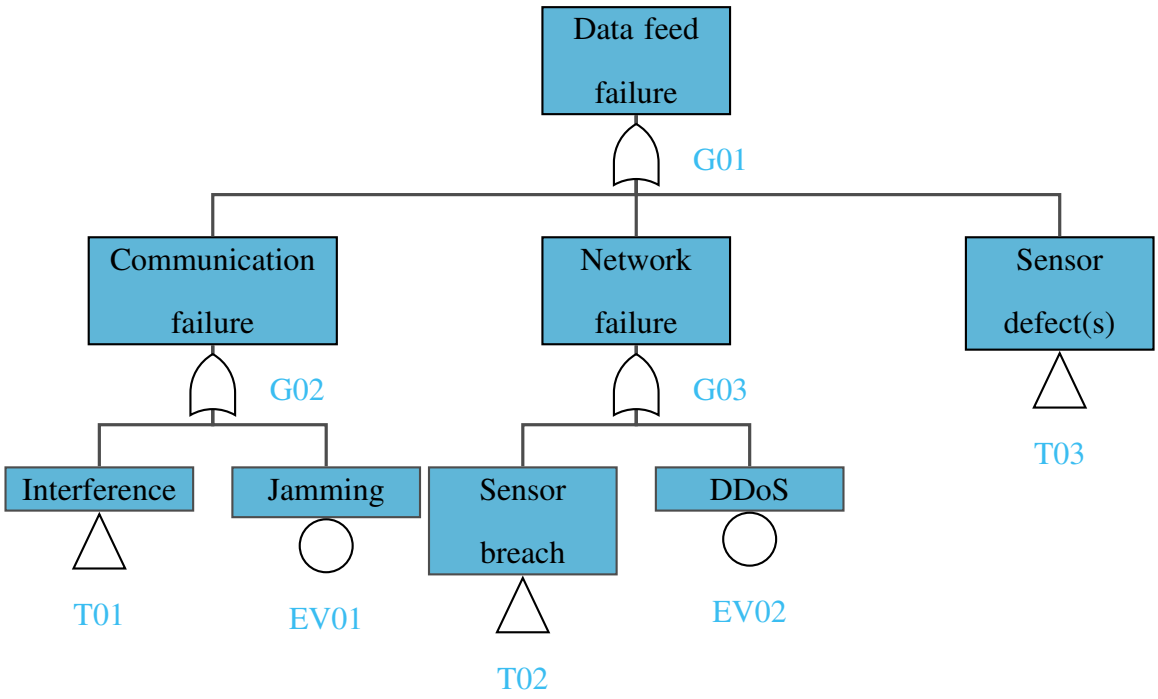

Figure 4.2: A non-exhaustive fault tree diagram of the data feed of smart traffic lights.

In the fault tree diagram, the events leading to fault states progress from bottom to the top. External fault trees used as input are marked with triangles; independent events are displayed as circles. In the diagram, a data feed failure occurs if any of the three immediately preceding events occur. In this example, a communication failure could occur due to signal interference, whether accidental or deliberate, or a jamming attack. Interference could have multiple causes and thus has its own separate fault tree diagram. In comparison, a jamming attack is a single event that is caused by an attacker and is thus

shown as a simple event. Similar reasoning applies to network failures and sensor defects. Sensor breaches can have multiple causes, e.g. key leakage through side-channel attacks, just as there are multiple ways for the sensors to malfunction. Thus, they are represented as the outputs of other fault trees.

Similar to traffic and infrastructure, healthcare can benefit from e.g. wearable smart sensors in receiving accurate and real-time data from patients, both inside and outside of the medical facilities, as discussed in 3.3.1. These benefits include reduced unnecessary appointments, pre-emptive treatments, and more efficient patient healthcare inside hospitals. As such, the smart healthcare equipment serve a complementary role along with the regular equipment and procedures.

Inaccurate and imprecise measurements, e.g. due to noise or systematic error, received from smart medical sensors, and consequently processed without checking the correctness of these data, could lead to incorrect, unnecessary, and potentially harmful treatments. Additionally, if the devices communicate wirelessly on a busy band, interference could also prevent the transmission. If, on the other hand, a device shares credentials with identical devices, e.g. because the manufacturer reuses default credentials, or it can be impersonated by an attacker after analysing captured packets, the reliability and safety of the medical accuracy of the used system is compromised.

Another case where both reliability and safety have to be considered are the smart homes. If, for example, a central hub is used to monitor and control the smart devices in a smart home, due to its central role in the home, the owner of the hub should be able to expect it to operate reliably for extended periods of time. Additionally, safety-related devices, such as smart locks and IP cameras, should not cause safety issues or prevent authorised access to the home during power outages.

Because the citizens' influence on the critical systems utilised by the smart city is limited, it is important that they can be trusted not to have detrimental effects on the citizens' lives whenever they malfunction. Thus, internally developed or custom-made

systems should incorporate reliability and safety requirements, set by the smart city, into their development process. Whenever externally produced, e.g. consumer-grade, products are used, they should be required to fulfil the same set of requirements.

These requirements should cover both physical and digital reliability and safety. Since, in many cases, they are used to process personal data, potential for exposure of such information due to or during failure states should be prevented. This could be achieved e.g. physically through the use of secure processors and by ensuring the implementations of security solutions, such as those discussed in 4.1 or 4.2, are not vulnerable to known attacks.

Sometimes ensuring reliability requires the introduction of redundancy. For example, systems, such as smart traffic, heavily dependent on a steady data feed could be severely impacted by unexpected downtime caused by e.g. mechanical failures or an external attack. In these cases, the use of e.g. backup or parallel systems aids in the prevention of outages. A superficial dependency graph for smart traffic light control is shown below in figure 4.3.

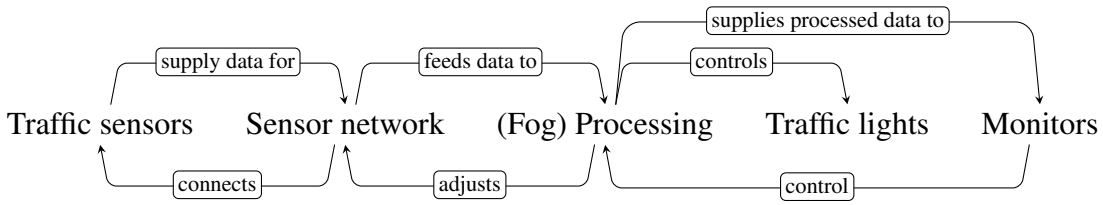

Figure 4.3: An example of a dependency graph for data feed of smart traffic.

Another suitable example is guaranteeing a steady power supply to healthcare facilities, such as hospitals. In order to maximise the availability and benefits of smart healthcare, as well as to prevent casualties, redundant power sources should be utilised. Viable precautions include the potential to use multiple power companies as suppliers if they use distinct power sources, and multiple connections to the power grid in case connection is lost due to natural causes. Additionally, local backup power sources, such as generators or solar panels, should be able to provide sufficient power to maintain critical operations.

An alternative approach to these analyses is to cover the data-flow of the systems as opposed to e.g. their mechanical or processal reliability. As with the others, data-flow reliability and safety can be assessed, and critical bottlenecks alleviated or altogether removed.

4.3.1 Recommendations

The reliance of smart cities on information and communications technology highlights the requirement to pre-emptively prevent, as well as reactively promptly recover from, failure states encountered during the operation of their central systems. As such, the following recommendations focus on three main phases of the development of the city. They are the preliminary requirements defined during design, and the continuous mitigation of reliability and safety risks through iterative development.

RR1 **Set and enforce safety and reliability requirements.** Due to the variation in the tasks and responsibilities of smart systems used in a smart city, context-dependent sets of requirements should be defined. For example, healthcare, infrastructure, and housing each have distinct focuses, such as monitoring health as compared to air quality, and thus, albeit with some overlap in the requirements, do not benefit from all of the requirements set for other contexts. These requirements should undergo periodic review to ensure they remain effective.

Additionally, they should be transparent and accessible to the citizens e.g. as a list of guarantees from the city to its residents. This allows the citizens to personally verify, and consequently trust, the chosen requirements and, if applicable, voice their concerns and thoughts as a part of the iterative development of the city, as discussed in 3.3.3, 3.3.2, and 4.4.2.

RR2 **Identify reliability and safety bottlenecks e.g. through fault and dependency analyses.** Fault tree and dependence diagrams, as shown in the previous section, can be used to analyse known failure states by examining the event chains required

for them to occur, or to analyse the dependence relationships of subsystems to determine weak spots. These tools can be useful in determining the weakest links of the systems and in mitigation of potential weaknesses if the diagrams are made thoroughly.

The discovered weak points could be e.g. single components or subsystems which are prone to malfunction but necessary for the entire system to function, or the failure state of a subsystem that is likely to lead to an undesirable safety risk. These states could be reached, inter alia, through component wear, malfunction, compromise, or as a side effect of a natural disaster. As each event is closely bound to a specific set of subsystems or components, the combination of these analyses can be used to directly identify high priority ”bottlenecks” of reliability and safety.

It is important to note that these bottlenecks are not always single components or subsystems but could entail multiple, especially if a failure causes a cascade of further failures. These fault chains could be identified e.g. through the combined use of the aforementioned fault tree and dependency diagrams.

This recommendation also applies to the data flows utilised in the systems. Their interruption, corruption, or falsification should be protected against. If this is not accomplished, and e.g. a data feed is injected with falsified information, further processing and, inter alia, automated decision-making are compromised.

RR3 **Use fail-safes and redundant systems to alleviate the identified bottlenecks.** Critical infrastructural systems, services, and security-related functions, especially without redundancy, can significantly hinder or even halt the operation of other systems important for a smart city during an outage. It is then advisable to introduce enough redundancy to the previously identified bottlenecks to reduce the probabilities of these risks. However, redundancy inherently incurs additional costs to development and implementation. Thus, it is more efficient to focus on the critical paths of operation. Additionally, wherever redundancy is not desired e.g. due to

resource constraints or operational overhead, such as in relevant software or small smart devices, fail-safes should be used to prevent large-scale system failure during malfunctions.

4.4 Avoidance

Perhaps the most directly observable effect of forced trust on the citizens of a smart city is their willingness to participate in and adapt to the changes brought on by the city becoming smart. As discussed in the subsection 2.2.2, the citizens could be willing to participate, accepting, for example due to their personal interest or because they deem the available benefits to be greater than the perceived potential issues the changes could bring. Alternatively, they could attempt to avoid participation to some of the features of the smart city. The extreme form of this reaction is to resist the smart city project altogether, deliberately attempting to e.g. provide falsified information, sabotage the systems, or spread disinformation about the project in order to gain support.

The latter two reactions are foreseeable especially in situations where these changes are abrupt, the citizens have not been previously informed, have not been able to successfully voice their concerns, or these concerns have been ignored. Additionally, if the introduced changes require the citizens to possess technological expertise beyond their current skills, or they struggle to adapt to or learn to use new technologies, some form of avoidance is a likely outcome.

The development processes should then take the end-users, as agents and subjects of systems and services, into account instead of focusing solely on the technical details. In practice this means concentrating the development efforts on their needs, such as by identifying services that improve their quality and ease of life. Thus, as mentioned in subsection 2.5.3, no technological solutions or advancements introduced with a goal to create a smart city should make tasks more complicated or difficult. For example, if some

services are moved online after being offered at a physical location, the accessibility, availability, and ease of use of these services should at least remain the same, or ideally improve.

Smart cities are by design heavily data-reliant, and thus require cooperation from their residents. Data, and metadata, collected, derived, and inferred from the citizens either directly or indirectly can be seen to be reliable, and generally applicable, if enough citizens choose to provide them or, if this is obligatory, the data are realistic. Ascertaining this is central if they are used to further develop, inter alia, the infrastructure, transit, or governance systems and services as they affect the entire population of the city.

Methods available to combat avoidance of systems and services of smart cities include transparency in the operation and decision-making of the city, capability of the residents to influence them, providing motivation e.g. by showing the benefits of using the systems, as well as providing them accessible advice on their use. Transparency and citizen influence are further discussed in subsections 4.4.1 and 4.4.2, respectively.

Improving the motivation of the citizens to use the services made available by the smart city will help reduce their indifference towards these services e.g. in cases where they are seen as unnecessary. This requires clear and unambiguous communication about the proposed and developed features. Showcasing quality of life improvements enabled by, for example, new online services or more efficient public transit and healthcare is a good method of informing the users of aspects they might not have been previously aware of. As a side effect, it can also hinder the spread of misinformation, especially the aforementioned official information is available both electronically and physically.

Finally, the citizens cannot be assumed to possess the required skills and experience to utilise e.g. technical apparatus as they were intended to be used. This could lead to accidental misuses with negative side effects, such as getting locked out of a smart home after changing their default master password. It is important to provide accessible and readily available information channels in order to enable the citizens to learn how to use

these services.

4.4.1 Transparency

Transparency is of utmost importance whenever personal data are processed, as was previously briefly discussed in 4.1.3. The design of such processes should abide by the principle of transparency as a fundamental part of data protection; the data subjects should always be aware of how, where, and by whom their information is used. As such, similar requirements apply to the relevant policy decisions made by the city as well as the public authorities allowed to handle the data. Transparency can be a strong tool for building trust in the authorities. Additionally, if the citizens are able to understand the systems and services they use, it is easier for them to trust these as well.

One approach to providing transparency in data processing is a hub akin to that proposed in the MyData model [21, p. 5]. The hub would allow the citizens to monitor the collection, retention, and processing of their personal data, by the smart city, throughout their lifetime. This hub would also serve as each citizen's personal control panel where they can opt in to and out of additional voluntary processing, such as the use of location data to improve the availability of public transit, or toggle their consent with regard to their data, e.g. medical, being shared between services. The hub could then also be used as an access point for the citizens to their data, improving the GDPR compliance of the system.

Additionally, connecting other relevant public services to the hub would improve the efficiency of their use, as it would serve as a single interface between the citizens and the services. Since this would require cooperation across multiple national public offices, it is out of the scope of a single city but could be advantageous if used in multiple smart cities.

4.4.2 Possibility to influence

In order to minimise the negative impacts forced trust has on the smart city implementations, the users, i.e. the citizens, should be able to influence their development. This mitigates one of the fundamental aspects of forced trust: the citizens' inability to choose or affect the information systems chosen by the public authorities. Naturally, in certain cases such as smart healthcare, energy, or infrastructure the allowed influence is limited due to e.g. safety, sustainability, or efficiency. However, whenever their personal information are used, or their regular activities or behaviour potentially limited, their concerns should be heard if shared between a sufficient portion of the population.

An example vector for citizen participation would be a platform, available e.g. online and smart devices, through which citizens could put forward suggestions related to the smart city, vote on them, and discuss them. This would improve the accessibility and ease of contributing to the development of one's own city, especially for people who are unable to attend e.g. meetings physically and would be beneficial to the goal of iterative city development. Additionally, gamifying this type of a platform could also help in its levels of adoption and engagement.

Providing the citizens means of influencing the decision-making process of the ISs of their city is not enough if they are not made aware of this capability and how to take advantage of it. Political apathy, a prevailing perception of citizen participation having no actual effect on the end results of e.g. policies, can hinder the motivation of people to take part in such processes. These mindsets could be caused e.g. by prior experiences of concerns being overlooked, especially if they were shared by a large number of people.

One example of such a case is the copyright reform of the EU, finalised in 2019, which faced opposition due to its potential to result in e.g. preventive censorship through automated filters and limits on research, as well as the support it received from extensive lobbying [65]. In the end, a petition signed by four million citizens [66] was ignored by the European Parliament after the reform was secured through a background deal between

France and Germany [67]. These types of political manoeuvres can quell the willingness of later engagement in citizens.

Albeit it is challenging to solve these issues at the aforementioned larger scale, it is easier to improve the effectiveness of citizen participation on local and city levels. Inclusion of citizens in some sections of the development can help build their trust and has the potential to lower the cost of the iterative development of the smart city as the focus can be placed on features that are needed. Another benefit resulting from this is the personal investment of the participating citizens, encouraging them to use the final services and systems.

4.4.3 Recommendations

Risks of the avoidance and resistance reactions can be mitigated by ensuring the previous concerns, i.e. privacy, data security and protection, and reliability, are addressed. Additionally, the following recommendations discuss potential methods for improving the level of citizen participation, and thus reducing avoidance.

AR1 **Motivate the citizens to adopt and utilise the features provided by the smart city.** This can be achieved e.g. through information campaigns. They should try to cover the major reasons for avoidance, e.g. derived from polls or interviews. As such, this approach is both proactive and reactive, as the reactions of the citizens cannot be fully predicted prior to the implementation of the smart city.

Citizens could be concerned about, inter alia, the technological or utility aspects of the implementations. For those concerned about their privacy, or the security of their data, the relevant safeguards and approaches taken to protect these aspects should be clearly explained, without resorting to technical jargon. On the other hand, in cases where the benefits of participating over non-participation have not been made salient, focus should be on the personal benefits gained from the city-level improvements enabled by citizen participation.

AR2 **Provide a hub for the citizens for monitoring their data.** This hub could a service provided e.g. by the city, or a trusted third-party service provider. This platform should equip the citizens with the capabilities to monitor the utilisation and access histories, by both public authorities and private entities, of their data. This log should also enumerate the grounds on which the data were accessed, e.g. for obligatory or voluntary processing.

Additionally, the hub should provide its users the capability to control their consent, and level of consent, to different forms of voluntary data processing. The available dimensions for control should include at least the identities of the authorised processors, and the purposes for which the data are processed. The types of processing one can opt into could include participation into tests of new public services, or enhancement of existing ones, or services provided by the private sector. In the latter case, it should also be made clear whether the respective entities monetise the data received from the citizens.

If made available online as well as integrated into smart home hubs, this platform would provide the citizens an accessible method of controlling their data. Further incentives for participation could be introduced through some level of gamification of the user experience, e.g. with a graph displaying quantifiable benefits accrued.

AR3 **Provide a platform for citizen participation.** In order to sufficiently support participation in the iterative development of the smart city, this platform should enable the citizens to e.g. raise suggestions on potential areas of development, discuss them, and show support for initiatives they agree with. While each citizen would have a personal account to this platform, in order to preserve at least a modicum of their privacy, they should also be able to use pseudonyms. Additionally, assuming the previously described data monitoring and control hub is in use, the functionalities described in this recommendation could be integrated into the same platform to

further centralise the smart city activities and lower the threshold for participation.

This platform could also be used as a communication channel between the city and its residents. Thus, official information regarding, for example, emergencies, accidents, or traffic rearrangements would be able to spread effectively.

AR4 **Provide accessible training for citizens.** The ever-developing set of features and functionalities offered by smart devices, be they for home, work, or public utilities, can be challenging to grasp for some citizens. As such, it is recommended to make necessary training available, accessible, and unambiguous e.g. in written form as manuals, and hands-on workshops. The latter example should be utilised especially in the cases of smart home devices.

AR5 **Disclose security breaches as soon as possible after they are discovered and their causes are resolved.** Attempting to repudiate incidents such as these will cause more damage to the citizens' trust when such an attempt is eventually disclosed. Instead, while their trust can initially decline due to the knowledge, the transparency will benefit the city in the long term as it will be able to display its capability of learning from past incidents and trustworthiness as a data controller.

Chapter 5

Smart city of Salo

The town of Salo, located in southwest Finland, has a notable history of development and manufacture of ICT. Perhaps the most prominent example is the Nokia mobile phone manufacturing, research, and development centre that operated in Salo until 2015. Recently, in 2018, Salo began a smart city project, aiming to become a smart city within the following decade.

This chapter covers the details of the smart city of Salo -project. Its major focus areas and goals are examined in section 5.1. These foci and their applicable concerns are discussed in section 5.2. Additionally, suitable recommendations regarding privacy, data protection and security, system redundancy and reliability, and avoidance are mapped onto these identified issues.

5.1 Project description

Salo is cooperating with the town of Somero, Lounea Oy, the University of Turku, Turku university of applied sciences, and Salo Region Vocational College to study and develop the smart city concept for small and medium-size towns and cities. The vision of the project is to utilise digitisation in knowledge-based management, as well as the development of the internal processes and mobility of the city. As a result, the public sector

should be able to operate their services at a lower cost. Additionally, the objectives of the project include

- collection of, sharing of, and managing with knowledge,
- real-time and predictive situation information to support management and decision-making,
- transparent and justifiable decision-making,
- incorporating cyber security and citizen trust, and
- easing and developing mobility. [68]

The smart city concept used in the project is comprised of eight aspects: smart governance, smart education, smart healthcare, smart building, smart mobility, smart infrastructure, smart technology, smart energy, and smart citizen [69]. These aspects are illustrated below in figure 5.1. Three of them are initially focused on: education, energy, and mobility.

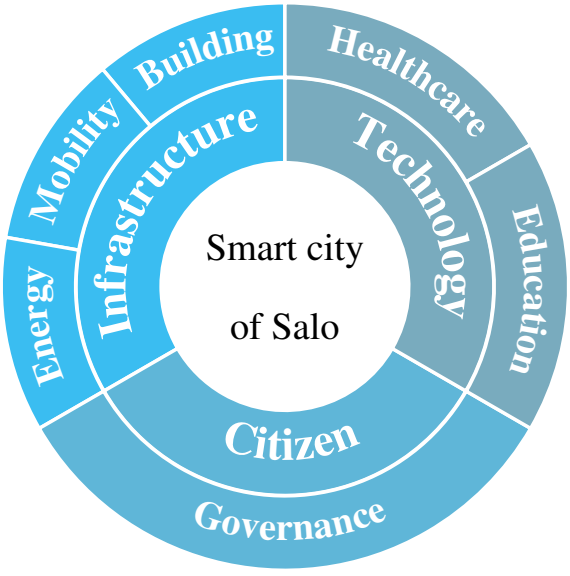

Figure 5.1: Main areas of focus in the Smart city of Salo -project.

Education is developed in cooperation with universities to discover and develop technologies and methods for teaching and learning. Resource consumption will be minimised through the combined use of smart energy, infrastructure, and technologies. Finally, due to the large geographical size and sparse population, Salo requires cost-effective and available modes of transport for its citizens. [69]

The planned digitisation takes advantage of the higher availability of relevant data to ensure the smart systems are fed up-to-date, accurate, and reliable information [70]. This could be used, for example, to implement a mobile application that provides information about the city, e.g. its utilities and functions [71].

Finally, the project is intended to result in a smart city concept that is scalable to towns and cities of varying sizes and could be productised into a business. This product would supply such communities with the framework, including the infrastructure, cyber security, and digitised services, required to establish a citizen-oriented smart city. [70], [71]

5.2 Addressing primary concerns

As the Salo smart city project is still in its preliminary phase, the amount of concrete, planned systems and solutions is very limited. Thus, the following consideration is based on the features and plans publicly available, as described in the previous section. The tangible plans from the description are knowledge-based management, an application for information sharing and communication, transparency of government, and incorporation of cyber security and citizen trust. For these aspects, the applicability of each of the primary concerns covered in chapter 4 are discussed, as well as their suitable recommendations and their fulfilment.

5.2.1 Knowledge-based management

Salo aims to digitise and productise the services provided by the town to enable knowledge-based management. This would allow them to produce predictable, standardised, homogeneous, and reproducible services, both in terms of their quality and cost. Additionally, the data should be reusable and, as a result, retained for a set period of time. As the consumed data are sensitive information related to the city, they should also be adequately protected. [70]

The range of necessary precautions, with regard to privacy and security, depends on the types of data used in the management. If they are purely operational or all identifiable data are sufficiently anonymised, the citizens' privacy is not threatened if their confidentiality is compromised. This also reduces, but does not abolish, the impact on their trust.

However, if the information used by the city includes e.g. pseudonymised or directly identifiable data, the affected citizens are likely to have an adverse reaction as a result of compromises. Based on the severity of the incident, this can range, as depicted in figure 2.1 of section 2.1, from the citizens becoming untrusting towards the city as an operator of the systems to them developing distrust. In the latter case, avoidance and resistance are notable potential consequences.

Based on these considerations, the recommendations PR4-PR6, DR3, and AR5 are applicable to knowledge-based management. The privacy recommendations apply on the condition that personal information of the citizens is involved in the operation of the services. In these cases, following the aforementioned recommendations will help to pro-actively protect their privacy, both during normal operation and during incidents. If suitable technologies are available, DR3 will benefit the services via their ability to ensure the confidentiality of the data while still enabling their analysis. Finally, as absolute security is never attainable, it is imperative to remain transparent in the cases of breaches, as per AR5, to ensure citizen trust after the incidents are resolved.

5.2.2 Smart city application

One of the projects under development is an application for the town of Salo to utilise for the sharing of information related to the town and events, and as a communication channel, as well as to provide the citizens with situational data e.g. about the availability of parking space [71]. Such an application could be further expanded to a citizen participation platform, or a hub, as described in the recommendations AR2 and AR3.

This application would ideally be developed both as an online service and for smart devices. The information available through the application could be targeted at multiple different focus groups, such as tourists and residents. This would enable its use as an information channel to e.g. improve awareness on the use of provided services, as in AR4, or on the mitigation of risks related to smart devices, as covered by PR7.

If the application is developed to provide the citizens access to critical information related to e.g. the operation of the smart city or incidents that could affect the citizens, or to become a central hub for services and data control, the reliability of associated systems has to be ensured. In these cases, the reliability of used components and software should be analysed, e.g. with the methods suggested in RR2, and tested. If necessary, the continuous availability of, for example, emergency information should be ensured during network outages with redundant backup systems, such as SMS, as discussed in RR3. Additionally, if the role of the application in the smart city grows to involve the handling of personal data, the considerations regarding their necessity and security covered in the following subsections 5.2.3 and 5.2.4 apply.

5.2.3 Transparency and justifiability

The fourth of the listed objectives of the smart city project is the introduction of more transparency to decision-making and communicating the justifications of these decisions better to the citizens [68]. If fulfilled properly, increased transparency and justifiability will lower the likelihood of user avoidance. These objectives are an important part of

building trust towards the city whether the citizens' personal information is used or not, as nonetheless a smart city project will require a notable amount of funding.

Transparency should be emphasised during the operation of the services to enable the citizens to trust but verify the city to perform their purported services and tasks. Justifiability, on the other hand, is especially important during the design and development of the city. The responsible public authorities should be able to reason the decisions and choices made for, inter alia, the systems, applications, and types of data collection.

The citizens should always remain knowledgeable about where their data are processed and stored, and thus DR6 is recommended. Additionally, informing the users about any extensions to access or utilisation of their data, as well as consent if they are personal, is an important factor of operational transparency. This process will also allow the city to justify this increase in privileges, potentially increasing the number of consenting citizens. Thus, DR9 is suitable for these objectives.

Data minimisation, PR4, can also benefit the justifiability of the approaches and systems used by the city, as the identification of the minimal set of information required for operation should be justified. Additionally, the citizens should be able to monitor the data usage, as their owners, e.g. through a hub as per AR2. Finally, akin to the knowledge-based management, transparency requires the disclosure of any breaches, as discussed in AR5, that compromise personal information.

5.2.4 Security and trust

Reaching a sufficient level of security is important to ensure a continuous operation of the smart city as well as the confidentiality and integrity of the utilised data. However, if the use of the services or systems, as a consequence, becomes complicated, their users could be motivated to bypass the security solutions in order to ease their use, as was discussed in 2.5.3. Nevertheless, if the city is capable of demonstrating the security of these systems, especially if they can be made inherently safe, the users are more likely to trust them even

in the case of operator mishaps.

As previously discussed, minimising the amount of data collected reduces the privacy risks of their owners, but it also reduces the amount of information that the systems must keep secured. If they are additionally disposed of at the end of their retention period, the burden of privacy protection and security systems is further reduced. Thus, PR4 and PR6 benefit the security objective as well as that of trust, as potential infringements of the right to privacy can severely impact the citizens' trust.

Thorough evaluation of potential security risks must be done in order to determine the necessary solutions to achieve the set requirements. Ideally, they are implemented with the philosophy of defence-in-depth to ensure the protection of the systems if one of them malfunction or is breached. These recommendations are covered in DR2 and DR4.

User trust can be further strengthened in the design phase by incorporating privacy in the entirety of the smart city, as discussed in PR2, and balancing the data processing responsibilities between different parties, both in terms of identity such as public or private as well as location, as covered by DR6 and DR7. Finally, giving the citizens agency, as in DR9, with regard to the usage of their data, e.g. with the previously discussed hubs of recommendation AR2.

Chapter 6

Conclusion

Based on the literature review of section 2.2, forced trust was defined as a situation where a truster is forced to trust a trustee without substantial opportunity to influence their behaviour. The trustee could be, inter alia, in the form of a service or an individual. Thus, the concept of forced trust can be applied in the context of smart cities, as the only alternative to using the information systems and services related to the cities can in some cases be a decrease in the truster's quality of life. If these systems are deeply ingrained into the daily lives of the citizens of a smart city, such as detection of pedestrians and vehicles in traffic using cameras, avoiding their use will inevitably make the concerned citizens' lives more difficult.

Due to the complicated trust landscape related to smart cities, the citizens are either in direct or indirect forced trust with multiple parties including national and international governments, and service providers. Due to this trust network, the initial, and developing, user trust towards the systems could be affected by regulations and the outcomes of prior public information system projects. Based on these factors, and the discussion on the technologies that enable smart cities in section 3.2, the foremost domains of concern related to smart city implementations were found to be the risks posed to the citizens' privacy, the level of security and protection of their data, the reliability of the systems, and the potential for the populace to avoid or resist the use of the implemented solutions.

Privacy concerns translated to the potential of the citizens' personal data to be, for example, misused or disclosed. Such misuses include identification of data subjects, excessive data collection, and long retention periods. On the other hand, the sensors, systems, and software used to collect and process these data can be subject to security and data protection flaws. Furthermore, mismanaged access rights can expose this information to unauthorised parties. Additionally, lacklustre reliability and safety of the used systems, especially if cyber-physical, can have direct detrimental effects on e.g. their users or bystanders. Examples of such threats include smart traffic control and healthcare systems.

As the residents of smart cities are forced to trust their city to ensure sufficient protection of their information, accessibility and availability of critical systems, and transparency of operation. If the citizens begin to perceive incidents, such as those described above, to be likely to occur, or if they are realised, they are more likely to avoid the usage of the affected systems. In extreme cases of avoidance, a citizen could react by resisting them, e.g. via attempts of disrupting or disabling these systems. Smart city implementations should then take these concerns into consideration in order to prevent these adverse reactions.

The four tangible plans of the Salo smart city -project discussed in detail in chapter 5, knowledge-based management, smart city application, transparency and justifiability, and cyber security and citizen trust, are based on the objective of the project to digitise the services of Salo in order to homogenise them both in terms of quality and cost. With an increased amount of digital and ICT-based systems, it is important to ensure the users' forced trust to these systems does not affect them negatively. As a result of the discussion in the chapter, the among recommendations most applicable to the Salo project, out of those suggested in chapter 4, were the minimisation of personal data collection, their disposal at the end of their retention period, and a system for the citizens to control the flow of their data. Together, these approaches provide the citizens agency, and consequently increase their trust, in the smart city, and encourage participation in its development.

6.1 Fulfilment of thesis objectives

Below, the thesis objectives set in the introductory section 1.2 are reviewed and their fulfilment evaluated. The evaluation consists of references to relevant sections of this thesis, where each of the objectives are discussed or resolved, and, if necessary, a brief summary of the results. A more detailed review of this thesis can be found at the beginning of this chapter.

O1 What is forced trust and how does it affect and relate to smart city projects?

Definition 2.3.1 for forced trust was found in section 2.3, covering most of the scenarios and uses for the term found in the literature review of section 2.2. The applicability of the definition to the context of smart cities was displayed with the corollary 2.3.2.

The trust relationships between the citizens and the other parties relevant in smart city implementations were discussed in section 2.4. Factors affecting their trust towards said implementations were covered in section 2.5, focusing on factors influencing the initial trust, and chapter 4, where implementation- and operation-specific factors were discussed.

O2 What are the main concerns related to the design and operation of smart cities for their citizens?

In this thesis, four major categories of concern related to smart cities, from the point of view of their residents, were identified: privacy protection, data protection and security, reliability, and avoidance. These concerns were discussed in detail in chapter 4.

O3 How can the concerns identified in O2 be resolved to minimise the potential negative impacts related to forced trust?

Recommendations for approaches that help mitigate the main causes for negative impacts of forced trust, i.e. incidents involving privacy or security violations, or

reliability issues, as well as the effects of these impacts, i.e. user avoidance, were given in chapter 4. These recommendations are applicable, depending on the recommendation, in one or more of the following phases of smart city projects: design, development, implementation, and operation.

O4 How can the approaches of O3 be applied to the Salo smart city project?

The aforementioned recommendations were mapped onto the planned aspects of the smart city of Salo in section 5.2. The discussed aspects were based on the description of the project given in section 5.1.

As a conclusion, this thesis successfully fulfilled the set objectives. However, the moderately low number of practical examples or available detail in the plans and strategies of the smart city of Salo project hindered the thoroughness of the application of recommendations given in chapter 4.

6.2 Potential for future work

Further study should be done on the scope and nature of forced trust in relation to information systems, e.g. with case studies or from purely theoretical point of view, in order to more accurately understand its effects. The currently available literature on the subject is, as mentioned in 2.3, extremely limited and thus limits the deliberation on its practical influence on those in a forced trust relationship with a party or a service.

Additionally, in-depth research and development of methods and technology for privacy-preserving data analysis is important for smart cities. These include privacy-enhancing technologies, such as applications of differential privacy discussed in section 4.1, as well as data monitoring and control mechanisms, such as the hubs described in 4.4.

References

[1] S. Marsh and M. R. Dibben. Trust, Untrust, Distrust and Mistrust – An Exploration of the Dark(er) Side. In *Third International Conference on Trust Management (iTrust)*, pages 17–33, Paris, France, 2005. Springer Berlin.

[2] A. Hakkala, O. I. Heimo, S. Hyrynsalmi, and K. K. Kimppa. Security, Privacy'); Drop Table Users; - and Forced Trust in the Information Age?: When Trusting an Information System is Not Optional and Why It Matters. *ACM SIGCAS Computers and Society*, 47(4):68–80, 2018.

[3] A. Pfitzmann and M. Köhntopp. Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology. In *Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability*, pages 1–9, Berkeley, United States, 2000. Springer Berlin.

[4] The European Parliament and the Council of the European Union. General Data Protection Regulation (2016/679). Available online at `https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679`, 2016. Accessed 2019-10-24.

[5] B. Schneier. *Liars and Outliers: Enabling the Trust That Society Needs to Thrive*. John Wiley & Sons, Incorporated, Somerset, United States, 2012.

[6] Oxford English Dictionary. *trust, n.* In *OED Online*. Oxford University Press, 2015. Available online at https://oed.com/view/Entry/207004?rskey=CbNm79&result=1. Accessed 2019-09-20.

[7] A. Hakkala. *On Security and Privacy for Networked Information Society: Observations and Solutions for Security Engineering and Trust Building in Advanced Societal Processes*. PhD thesis, University of Turku, Turku, Finland, 2017.

[8] S. Madhisetty and M.-A. Williams. The Role of Trust and Control in Managing Privacy When Photos and Videos Are Stored or Shared. In *Proceedings of the Future Technologies Conference (FTC) 2018*, volume 2, pages 127–140, Vancouver, Canada, 2019. Springer International Publishing.

[9] A. Ledeneva. The Genealogy of Krugovaya Poruka: Forced Trust as a Feature of Russian Political Culture. In *Trust and Democratic Transition in Post-Communist Europe*, chapter 5, pages 85–108. British Academy, Oxford, United Kingdom, 2004.

[10] G. Hosking. Trust and Distrust in the USSR: An Overview. *The Slavonic and East European Review*, 91(1):1–25, 2013.

[11] A. Tikhomirov. The Regime of Forced Trust: Making and Breaking Emotional Bonds between People and State in Soviet Russia, 1917–1941. *The Slavonic and East European Review*, 91(1):78–118, 2013.

[12] The Parliament of Finland. Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018). In Finnish. Available online at https://www.finlex.fi/fi/laki/ajantasa/2018/20181054, 2018. Accessed 2019-11-13.

[13] Y. Hjelt. Poliisi ja Tulli saivat oikeuden automaattiseen kasvojen tunnistamiseen ihmisvirrasta – lupa on, mutta laitteet puuttuvat. YLE. In Finnish. Available online at https://yle.fi/uutiset/3-10815487, 2019. Accessed 2019-10-25.

[14] Finnish Security Intelligence Service. Ten questions on civilian intelligence legislation. Available online at https://www.supo.fi/intelligence/intelligence_legislation, 2019. Accessed 2019-11-13.

[15] European Commission. It's your data – take control. Available online at https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf, 2018. Accessed 2019-10-24.

[16] European Commission. The GDPR: new opportunities, new obligations. Available online at https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf, 2018. Accessed 2019-10-24.

[17] The Parliament of Finland. Data Protection Act (1050/2018). Available online at https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf, 2018. Accessed 2019-10-24.

[18] The Parliament of Finland. Eduskunnan vastaus EV 108/2018. In Finnish. Available online at https://www.eduskunta.fi/FI/vaski/EduskunnanVastaus/Sivut/EV_108+2018.aspx, 2018. Accessed 2019-10-25.

[19] T. Kuukkanen. Kolmen lääkärin tyly arvio 600 miljoonan euron jättijärjestelmästä: Edelleen täysin keskeneräinen, ei pitäisi laajentaa muualle. YLE. In Finnish. Available online at https://yle.fi/uutiset/3-10700107, 2019. Accessed 2019-11-21.

[20] STT, P. Kosonen, and S. Hirvonen. HS: Apotti-järjestelmästä on paljastunut potilaiden tietosuojan vaarantava ongelma. YLE. In Finnish. Available online at https://yle.fi/uutiset/3-10891042, 2019. Accessed 2019-09-04.

[21] A. Poikola, K. Kuikkaniemi, and H. Honko. MyData – A Nordic Model for human-centered personal data management and processing. The Ministry of Transport and Communications of Finland. White paper. Available online at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf, 2018. Accessed 2020-03-06.

[22] M. Deakin and H. Al Waer. From intelligent to smart cities. *Intelligent Buildings International*, 3(3):140–152, 2011.

[23] S. Singh. Smart Cities – A $1.5 Trillion Market Opportunity. Forbes. Available online at https://www.forbes.com/sites/sarwantsingh/2014/06/19/smart-cities-a-1-5-trillion-market-opportunity/#2feab3f86053, 2014. Accessed 2020-01-22.

[24] IEEE Smart Cities. What makes a city smart? Available online at https://smartcities.ieee.org/images/files/pdf/IEEE_Smart_Cities-_Flyer_Nov_2017.pdf, 2017. Accessed 2020-01-22.

[25] A. Liñán Colina, A. Vives, A. Bagula, M. Zennaro, and E. Pietrosemoli. *IoT in five Days*. E-Book, 2016. Revision 1.1. Available online at https://github.com/marcozennaro/IPv6-WSN-book/releases/.

[26] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund. Formal security analysis of LoRaWAN. *Computer Networks*, 148:328 – 339, 2019.

[27] 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*, 7(2):612–625, 2016.

[28] M. Vanhoef and F. Piessens. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In *Proceedings of the 24th ACM SIGSAC Conference on Computer and*

Communications Security (CCS), pages 1313–1328, Dallas, United States, 2017. ACM.

[29] MITRE. 2019 CWE Top 25 Most Dangerous Software Errors. Available online at https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html, 2019. Accessed 2020-01-27.

[30] T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah. Security and privacy challenges in smart cities. *Sustainable Cities and Society*, 39:499–507, 2018.

[31] E. Gasiorowski-Denis. The future of farming. *ISOfocus*, 122:6–11, 2017.

[32] W. Castelnovo. Co-production Makes Cities Smarter: Citizens' Participation in Smart City Initiatives. In *Co-production in the Public Sector: Experiences and Challenges*, chapter 7, pages 97–117. Springer International Publishing, 2016.

[33] Amsterdam Economic Board. Amsterdam Smart City. Available online at https://amsterdamsmartcity.com/, 2019. Accessed 2020-02-03.

[34] Vienna City Administration. Smart City Wien: Framework Strategy. Available online at https://smartcity.wien.gv.at/site/files/2016/12/SC_LF_Kern_ENG_2016_WEB_Einzel.pdf, 2016. Accessed 2020-02-03.

[35] G. Greenwald and E. MacAskill. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. Available online at https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, 2013. Accessed 2019-11-23.

[36] M. Day, G. Turner, and N. Drozdiak. Amazon Workers Are Listening to What You Tell Alexa. Bloomberg. Available online at https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio, 2019. Accessed 2019-11-29.

[37] Security Research Labs. Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping. Available online at https://srlabs.de/bites/smart-spies/, 2019. Accessed 2019-11-29.

[38] K. Cox. Uploaded Ring footage reportedly provides location to the square inch. Ars Technica. Available online at https://arstechnica.com/tech-policy/2019/12/ring-used-parties-swag-to-build-700-police-partnerships-report-finds/, 2019. Accessed 2020-01-09.

[39] K. Cox. Police can get your Ring doorbell footage without a warrant, report says. Ars Technica. Available online at https://arstechnica.com/tech-policy/2019/08/police-can-get-your-ring-doorbell-footage-without-a-warrant-report-says/, 2019. Accessed 2020-01-09.

[40] S. Biddle. Amazon's Ring Planned Neighborhood "Watch Lists" Built on Facial Recognition. The Intercept. Available online at https://theintercept.com/2019/11/26/amazon-ring-home-security-facial-recognition/, 2019. Accessed 2020-01-09.

[41] Article 29 Data Protection Working Party. Opinion 05/2014 on Anonymisation Techniques. Available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, 2014. Accessed 2019-12-04.

[42] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating Noise to Sensitivity in Private Data Analysis. In *Third Theory of Cryptography Conference*, pages 265–284, New York, United States, 2006. Springer Berlin.

[43] A. Narayanan and V. Shmatikov. Myths and fallacies of "personally identifiable information". *Communications of the ACM*, 53(6):24–26, 2010.

[44] M. Elliot, K. O'Hara, C. Raab, C. M. O'Keefe, E. Mackey, C. Dibben, H. Gowans, K. Purdam, and K. McCullagh. Functional anonymisation: Personal data and the data environment. *Computer Law & Security Review*, 34(2):204–221, 2018.

[45] P. Ohm. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, 57:1701–1777, 2010.

[46] A. Cavoukian. Privacy by Design: The 7 Foundational Principles. Available online at `https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf`, 2009. Accessed 2019-12-12.

[47] K. Wuyts. *Privacy Threats in Software Architectures*. PhD thesis, KU Leuven, Heverlee, Belgium, 2015.

[48] ENISA. Handbook on Security of Personal Data Processing. Available online at `https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/at_download/fullReport`, 2017. Accessed 2019-12-12.

[49] Traficom. Tietoturvamerkki. In Finnish. Available online at `https://tietoturvamerkki.fi`, 2019. Accessed 2019-12-12.

[50] ENISA. Algorithms, key size and parameters report – 2014. Available online at `https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014/at_download/fullReport`, 2014. Accessed 2020-01-09.

[51] S. Rahimi Moosavi. *Towards End-to-End Security in Internet of Things based Healthcare*. PhD thesis, University of Turku, Turku, Finland, 2019.

[52] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Con-*

ference on Pervasive Computing and Communications Workshops (PerCom Workshops), pages 618–623, Kona, United States, 2017. IEEE.

[53] G. E. Suh and S. Devadas. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In *Proceedings of the 44th Annual Design Automation Conference*, pages 9–14, San Diego, United States, 2007. ACM.

[54] M. Sen, A. Dutt, S. Agarwal, and A. Nath. Issues of Privacy and Security in the Role of Software in Smart Cities. In *Proceedings of the 2013 International Conference on Communication Systems and Network Technologies*, pages 518–523, Gwalior, India, 2013. IEEE Computer Society.

[55] K. Lauter, M. Naehrig, and V. Vaikuntanathan. Can Homomorphic Encryption Be Practical? In *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, pages 113–124, Chicago, United States, 2011. ACM.

[56] D. Boneh, A. Sahai, and B. Waters. Functional Encryption: Definitions and Challenges. In *Third Theory of Cryptography Conference*, pages 253–273, New York, United States, 2011. Springer Berlin.

[57] D. Moghimi, B. Sunar, T. Eisenbarth, and N. Heninger. TPM-FAIL: TPM meets Timing and Lattice Attacks. To appear in *29th USENIX Security Symposium (USENIX Security 20)*, 17 pages, Boston, United States, 2020. USENIX Association.

[58] S. van Schaik, A. Milburn, S. Österlund, P. Frigo, G. Maisuradze, K. Razavi, H. Bos, and C. Giuffrida. RIDL: Rogue In-flight Data Load. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 88–105, San Francisco, United States, 2019. IEEE.

[59] FENTEC. FENTEC Project: Increasing Trustworthiness of ICT solutions developing Functional Encryption. Horizon 2020. Press release. Available online at `http://fentec.eu/sites/default/files/fentec/public/`

content-files/article/FENTEC_PR_1.pdf, 2018. Accessed 2019-12-19.

[60] L. H. Newman. These Hackers Made an App That Kills to Prove a Point. Wired. Available online at https://www.wired.com/story/medtronic-insulin-pump-hack-app/, 2019. Accessed 2020-01-09.

[61] L. H. Newman. A New Pacemaker Hack Puts Malware Directly on the Device. Wired. Available online at https://www.wired.com/story/pacemaker-hack-malware-black-hat/, 2018. Accessed 2020-01-09.

[62] United Nations. The Universal Declaration of Human Rights. Available online at https://www.un.org/en/universal-declaration-human-rights/index.html, 1948. Accessed 2019-12-23.

[63] C. Cimpanu. EU votes to create gigantic biometrics database. ZDNet. Available online at https://www.zdnet.com/article/eu-votes-to-create-gigantic-biometrics-database/, 2019. Accessed 2019-12-23.

[64] N. Kobie. Why smart cities need to get wise to security – and fast. The Guardian. Available online at https://www.theguardian.com/technology/2015/may/13/smart-cities-internet-things-security-cesar-cerrudo-ioactive-labs, 2015. Accessed 2020-01-20.

[65] Corporate Europe Observatory. Copyright Directive: how competing big business lobbies drowned out critical voices. Available online at https://corporateeurope.org/en/2018/12/copyright-directive-how-competing-big-business-lobbies-drowned-out-critical-voices, 2018. Accessed 2020-01-14.

[66] C. Doctorow. Four million Europeans' signatures opposing Article 13 have been delivered to the European Parliament. Electronic Frontier Foundation. Avail-

able online at https://www.eff.org/deeplinks/2018/12/four-million-europeans-signatures-opposing-article-13-have-been-delivered-european, 2018. Accessed 2020-01-14.

[67] C. Doctorow. As the German Government Abandons Small Businesses, the Worst Parts of the EU Copyright Directive Come Roaring Back, Made Even Worse. Electronic Frontier Foundation. Available online at https://www.eff.org/deeplinks/2019/01/german-government-abandons-small-businesses-worst-parts-eu-copyright-directive, 2019. Accessed 2020-01-14.

[68] City of Salo. Salo - Älykäs kaupunki. In Finnish. Available online at https://www.salo.fi/kaupunkijahallinto/strategiajatalous/strategiajavisio/saloalykaskaupunki/. Accessed 2020-02-04.

[69] City of Salo. Invest in Salo. In Finnish. Available online at http://www.saloon.fi/attachements/2015-10-29T09-37-31164.pdf, 2015. Accessed 2020-02-05.

[70] City of Salo. Tiedolla johtaminen. In Finnish. Available online at https://salo.fi/kaupunkijahallinto/strategiajatalous/strategiajavisio/saloalykaskaupunki/tiedollajohtaminen/. Accessed 2020-02-05.

[71] P. Nisula. Salon, Someron, ja Lounea Oy:n tavoitteena älykkäät yhteisöt. In Finnish. Available online at https://www.salo.fi/kaupunkijahallinto/strategiajatalous/strategiajavisio/saloalykaskaupunki/49984.aspx. Accessed 2020-02-05.