Lappeenranta-Lahti University of Technology LUT

School of Engineering Science

Software Engineering

Master’s Programme in Software Engineering and Digital Transformation

Bachelor’s Thesis

**Erik Taavila**

# WEARABLE TECHNOLOGY AS PART OF ACCESS CONTROL

Examiner: Associate Professor Ari Happonen

# TIIVISTELMÄ

Lappeenrannan-Lahden teknillinen yliopisto LUT
School of Engineering Science
Tietotekniikan koulutusohjelma
Master's Programme in Software Engineering and Digital Transformation
Erik Taavila

**Wearable Technology as part of Access Control**

Kandidaatintyö 2020

59 sivua, 17 kuvaa, 1 liite

Työn tarkastaja: Associate Professor Ari Happonen

Hakusanat: puettava teknologia, pääsynhallinta, sähköinen kulunvalvonta, riskien hallinta, omaisuuden suojaaminen, IoT, esineiden internet, tietoturva
Keywords: wearable technology, access control, electronic locking systems, risk management, asset protection, IoT, Internet of Things, information security

Työssä katselmoidaan puettavan teknologian suhdetta pääsynhallintaan ja sähköisiin kulunvalvontajärjestelmiin riskienhallinnan ja omaisuuden suojaamisen näkökulmista. Tutkittavan kuuden pääsynhallinnan teknologian soveltuvuutta analysoidaan viiden yleisen pääsynhallinnan toimintaympäristön käyttötapauksiin. Käyttötapauksien avulla analysoidaan mitä lisähyötyjä puettava teknologia voi tuoda pääsynhallintaan, mitä erityisiä riskejä puettava teknologia tuo mukanaan pääsynhallintaan sekä mitä asioita on syytä erityisesti huomioida käytettäessä puettavaa teknologiaa pääsynhallinnassa. Analysoidun valossa, puettavan teknologian pääsynhallinnan hyötyjä saadaan etenkin monimutkaisemmissa pääsynhallinnan tilanteissa sekä pääsynhallintaan yhdistyessä muita toiminteita kuten maksusuorituksia. Työn tunnistamat riskit ja siten huomiota ansaitsevat osa-alueet ovat puettavan teknologian ja asioiden internetin epäkypsyys, tietoturvaongelmat sekä yksityisyyden suojaan liittyvä lainsäädännön lisääntyminen.

# ABSTRACT

Lappeenranta-Lahti University of Technology LUT
School of Engineering Science
Software Engineering
Master's Programme in Software Engineering and Digital Transformation
Erik Taavila

**Wearable Technology as part of Access Control**

Bachelor’s Thesis 2020

59 pages, 17 figures, 1 appendix
Examiner: Associate Professor Ari Happonen

Keywords: wearable technology, access control, electronic locking systems, risk management, asset protection, IoT, Internet of Things, information security

Thesis reviews the relationship of wearable technology to the electronic access control in the context of risk management and asset and property protection. Thesis analyzes the suitability of six access control technologies to five common use cases of access control situations. Use cases were used to analyze the benefits of implementing wearable technology to access control, what risks are introduced and what considerations should be made when implementing wearable technology to access control. In the light of the analysis, most benefits in using wearables for access control are in complex access control situations and where access control is intertwined with other functions such as payments. Recognized risks and issues to consider when combining wearable technology to access control are the immaturity of wearable technology and internet of things, related information security problems and increasing regulation for data protection.

## ACKNOWLEDGEMENTS

Research was started by topical research of reference materials during 2013. The deeper review of the materials was intended to happen already in 2014. The thesis work however took longer than originally planned due to author's personal and professional circumstances. The added benefit of the extension in the timeline provided professional growth to happen while working full-time in information security domain. The other side effect was that technologies that were just on the horizon in 2014 have now matured and the timeline provides very interesting thought patterns about technological advancements and their actual speed compared to the marketing pitches. The structure of the work does not support opening these insights in this thesis but could be an interesting study topic for someone to analyze these patterns from emergence to maturity. Interestingly the concerns that were present already in 2014 regarding the information security of connected devices have not disappeared or gotten remediated but the discussion in information security forums shows that the issues are only now, six years later starting to be understood. Also, now regulators have started to be interested in this type of technology and in 2018 California state issued one of the first connected technology related regulation. It was still quite simple and only gave direction to further regulation that is almost certain to be needed for the industry to start building more sturdy and secure devices especially for consumer markets.

Special thanks for the support on this thesis go to the examiner Ari Happonen who seemingly never lost faith of me completing this thesis. In the final phase of concluding the thesis work, he gave professional feedback and guidance on the intermediate work versions, he also managed to do it by coaching me into realizing my issues by pointing to the right direction. Thank you, Ari!

Equally big supporter was my beloved wife Jenni, who stood by my side all those years and raised our two adorable daughters with me at the same time. Thanks for the early morning coffee cups and hugs to get me through the work. I love you, my family!

# TABLE OF CONTENTS

**1 INTRODUCTION ........................................................................................ 4**

1.1 GOALS AND DELIMITATIONS ........................................................................ 5

1.2 STRUCTURE OF THE THESIS ......................................................................... 6

**2 RESEARCH METHODS ............................................................................. 7**

2.1 ANALYZING REFERENCES AND MATERIAL .................................................... 7

2.2 STRUCTURING AND FOCUSING RESEARCH ................................................... 7

**3 WEARABLE TECHNOLOGY ...................................................................... 8**

3.1 TYPES OF STUDIES AND MATERIALS AVAILABLE .......................................... 8

3.2 TECHNOLOGY MAGAZINE ARTICLES ............................................................ 8

3.3 ANALYST REPORTS ON WEARABLE TECHNOLOGY ....................................... 8

3.4 BRIEF INTRODUCTION TO WEARABLE TECHNOLOGY AND ITS ORIGINS ............ 9

**4 RISK MANAGEMENT .............................................................................. 12**

4.1 DEFINITIONS .............................................................................................. 12

4.2 RISK CLASSIFICATIONS .............................................................................. 14

4.3 ACCESS CONTROL IN RELATION TO RISK MANAGEMENT ............................. 16

**5 PROTECTING PROPERTY AND ASSETS .................................................... 17**

5.1 PROPERTY AND ASSETS .............................................................................. 17

5.2 RISKS AND THEIR MITIGATIONS POSSIBILITIES TO PROPERTY AND ASSETS ........ 17

5.3 ACCESS CONTROL ON PROPERTY AND ASSETS .............................................. 18

**6 ELECTRONIC ACCESS CONTROL AND WEARABLES .................................. 19**

6.1 DEFINITION OF ELECTRONIC ACCESS CONTROL ........................................... 19

6.2 COMPARISON OF ELECTRONIC AND TRADITIONAL ACCESS CONTROL ............ 19

6.3 COMPONENTS OF ELECTRONIC ACCESS CONTROL SOLUTION ........................ 20

6.4 ALARMS, INTRUSION DETECTION AND ELECTRONIC ACCESS CONTROL ............ 20

6.5 SPECIFIC RISKS AND CONSIDERATIONS WITH ELECTRONIC ACCESS CONTROL ........ 20

6.6 WEARABLES IN ELECTRONIC ACCESS CONTROL ........................................... 21

**7 USE CASE ANALYSIS FOR ACCESS CONTROL ........................................... 22**

7.1 USE CASES SELECTION AND REVIEW MODEL ........................................................ 22

7.2 ACCESS TECHNOLOGIES REVIEWED FOR USE CASES SELECTION ............................ 23

7.3 USE CASE 1: HOTEL ROOM AND GENERAL ACCESS FOR TENANTS AND STAFF ........ 25

*7.3.1 Definition of the use case, characterization, and protection targets ............... 25*

*7.3.2 Comparison of access technologies for the use case ....................................... 25*

*7.3.3 Learnings from the use case ............................................................................. 27*

7.4 USE CASE 2: PRIVATE HOME AND RELATED AREA DOORS ...................................... 27

*7.4.1 Definition of the use case, characterization, and protection targets ............... 27*

*7.4.2 Comparison of access technologies for the use case ....................................... 28*

*7.4.3 Learnings from the use case ............................................................................. 30*

7.5 USE CASE 3: OFFICE BUILDING DOORS, FLOORS, AND MAINTENANCE SPACES ....... 31

*7.5.1 Definition of the use case, characterization and protection targets ................ 31*

*7.5.2 Comparison of access technologies for the use case ....................................... 32*

*7.5.3 Learnings from the use case ............................................................................. 34*

7.6 USE CASE 4: UNLOCKING AND LOCKING CITY BIKES / AD-HOC RENTAL CARS ....... 34

*7.6.1 Definition of the use case, characterization and protection targets ................ 34*

*7.6.2 Comparison of access technologies for the use case ....................................... 35*

*7.6.3 Learnings from the use case ............................................................................. 36*

7.7 USE CASE 5: PUBLIC SERVICE ACCESS FOR NURSING AND EMERGENCY SERVICES . 37

*7.7.1 Definition of the use case, characterization and protection targets ................ 37*

*7.7.2 Comparison of access technologies for the use case ....................................... 38*

*7.7.3 Learnings from the use case ............................................................................. 40*

7.8 OVERALL LEARNINGS FROM THE ANALYSIS USE CASES ........................................ 40

7.9 CURRENT MARKET SITUATION FOR WEARABLES USE IN ACCESS CONTROL ............ 42

**8 CONCLUSIONS ......................................................................................... 43**

8.1 FURTHER STUDIES AND FUTURE OF WEARABLES AS PART OF ACCESS CONTROL .... 44

**REFERENCES ........................................................................................... 46**

**APPENDICES**

# LIST OF SYMBOLS AND ABBREVIATIONS

| | |
|---|---|
| AI | Artificial Intelligence |
| IoT | Internet of Things |
| M2M | Machine to Machine |
| MaaS | Mobility-as-a-Service |
| MEMS | Microelectromechanical System |
| ML | Machine Learning |
| NFC | Near-Field Communication |
| PII | Personally Identifiable Information |
| PIN | Personal Identification Number |
| RFID | Radio-Frequency Identification |

# 1 INTRODUCTION

The world as we live in is filled with physical places, things, and assets. It has been further extended by a layer of digital places, things and assets and this extension is growing fast because of digitalization even in traditional businesses such as manufacturing [1, 2]. This development is not just happening but becoming a necessity for business success [3]. These places, things and assets usually come with a reason of existence and are of value to people, organizations, and nations. When there is value there is a risk of for example compromise, misuse, loss, or damage. Sometimes the risks when realized can additionally result to further compromise, misuse, loss, damages or even casualties.

The process on considering these risks is called risk management [4] [5]. Several books have been written on the risk management and its multiple subdomains studying the intricacies of the value of assets, the varying threats to the assets, their identification, and mechanisms on addressing these risks. Addressing risks is formally called risk treatment. One specific risk treatment to risks related assets is generically called *access control* [6]. The control usually defines the ways to protect an asset from being accessed by unauthorized entities and allow the access to the asset by authorized entities. Access control commonly is accompanied with a larger set or superset of controls called physical and environmental controls. Physical and environmental controls address a larger set of risks to the asset being protected [7]. Basic examples of physical and environmental controls include protection from forces of nature (for e.g. rain, fire, and earthquakes), technical system failures (for e.g. loss of power, power surges and network connectivity losses).

Access control risk treatment originates from early history of mankind. The basic access control mechanisms include processes and technology for e.g. hiding assets, guarding, walls, fences, gates, doors, windows, locks, and keys, authorized and unauthorized entity lists and passwords. In the modern world these basic principles are still valid but have evolved further with technological advancements – for example strong authentication, electronic locks, and an alarm system. Since wider adoption of mobile phones computing has become more and more ubiquitous. The development of technology solutions into more power efficient, smaller, and computationally more powerful has then opened some new opportunities to embed such equipment into clothes and jewelry – commonly now referred also as wearable technology. Wearable technology (later just wearables) as a term is somewhat loosely defined but can be described as almost any electronic device that can be worn as from functional purposes or from aesthetic reasons or both. Another wave of electronics which goes hand in hand with wearables is Machine to Machine communications (M2M) also known as Internet of Things (IoT). This trending cumulates from very much from same technical advancements as wearables – improvements on power efficiency and computing power as well as cost reduction. While the two technical worlds go on their own ways, they seem to be on a collision course too. As ‘things’ get connected to the internet then also the wearables can be used to get information from them or manipulate them (like using a smartwatch turn on house lighting).

When the two areas collide, there is one especially interesting point of convergence – access control, let that be virtual or physical in nature. If one has electronic house with electronic doors and electronic ambience controlling, then one can quickly see the logic on handling the access control to the house and why not also the access to family photo collection similarly with the wearables one is anyway carrying. The wearables mixed with electronic access control hence are an interesting area of research and application to mitigate risks to assets. Depending on the application of these techniques they can also introduce different and totally new risks to the assets being protected.

## 1.1 Goals and delimitations

This research studies combinability of electronic access control and wearable technology in the context of risk management, asset protection and access control generally. They are introduced first separately to create a picture into the domain of access control and wearable technology. These are then studied together to provide insights into how they could be used as combined applications. The reference study parts of this work review risk management, asset protection, electronic access management and wearable technology. These sections cover the aspects from background point of view and bring the focus on matters related to the other sections. They cover some of the assets, risks associated to these assets and the risk treatment options available. They try then to highlight the various considerations for asset protection design and how these considerations vary in different use cases.

Research questions in this Bachelor’s thesis are: “Where does wearable technology bring additional benefits to the electronic access control use cases?”, “What are the most typical new risks that using wearable technology introduces to traditional access control use cases?” and finally, “What considerations should be taken when using wearable technology in electronic access control use cases?” Research scope is outlined to focus on certain example use case scenarios to simplify the very complex and developing technology area. The research comparisons are collected into initial comparison tables. The tables are not to be viewed as comprehensive list of considerations. The research will call for further studies to developing domain of wearable technology. Further studies to provide more comprehensive list of use cases and their specific consideration angles could be needed. The report will not go very deeply into the technical solutions – there are other literature available on those including the previously mentioned power and cost savings [8, 9, 10]. It will also not focus too much on the Internet of Things paradigms but will explain more the features making wearables provide additional aspects for access control and tries to highlight situations where they do not fit for the purpose.

## 1.2 Structure of the thesis

First part of the report focuses on previous studies and will cover other available studies and literature about wearables, Internet of Things, Machine to Machine communications, risk management and asset protection and especially access control solutions using wearables. It will not go into depth of the topics but tries to highlight the relevant points from those areas and to introduce the studies for interested reader. Section about research methods explains how the research for this report will be conducted and what benefits the selected methods provide and where they leave matters craving for further analysis. The methods will be chosen to accommodate the recent nature of some of the trends that the report focuses on – especially the wearables. Next sections of the report will provide a broad overview on the risk management, asset protection, access control and wearable technology. They are studied separately to create a picture into the domain of access control and wearable technology. Main section of the report will combine the domains together. The section utilizes set of use cases to consider applicability of using wearable technology as part of electronic access control to protect assets. Final part of the report will provide the results of the report, offer conclusions, and propose further studies. It will then summarize the whole report.

# 2 RESEARCH METHODS

## 2.1 Analyzing references and material

The research will present resources to study on the suitability of wearable technology for access control purposes. The suitability will not be analyzed solely from the access control integration point of view, but bigger viewpoint shall be sought as technology rarely solves things on its own – the pieces are formed from complexity of society, culture and technology together. Constructing the background into the individual domains, use cases and the risks within the research is done in a way to cover multiple references. Multiple references are used to reduce the risk of research errors [11]. The preceding studies of other touching topics will be reviewed and interfaces towards the research focus points will be analyzed from chronological point-of-view and from relevance point-of-view.

## 2.2 Structuring and focusing research

The research will be mainly based on literature review and analytical conclusions based on it in the form of use cases. Use case examples are developed during the research based on the materials and practical day-to-day situations. The results are discussed individually and then prepared in a comparison table format showing different use scenarios and then cross-matching those with different technical solutions. Such scenarios would include homes fitted with electronic doors, a workplace, and a large manufacturing unit such as a dry dock. Technical solutions will cover for example common proximity cards, smartphones, and smart watches, – for comparison there will be traditional solution in the form of traditional keys and locks. The key aim in the research is to capture essential concepts around wearable technology, model use case scenarios for using wearables for access control and then weigh those sample cases from their strengths and weaknesses from multiple angles such as social interest, technical feasibility and practicality, security, privacy and concerns of physical harm. The research is set to answer the question whether the wearable technology is really the answer for the age-old dilemmas of lost keys, key management, and access maintenance for various places. Research is done in a way to focus more into the joint usage of all things larger than their value individually added up.

# 3 WEARABLE TECHNOLOGY

## 3.1 Types of studies and materials available

There are plentiful of studies [12], technology papers [13], commercial products available about wearable technology [14], augmented reality [15], Internet-of-Things [16], human bodily enhancements, access controls, wireless communications, electronic keys and key management. The reference materials were searched focusing on author own professional interests focusing on security related from own bookshelf, O’Reilly’s online library, university scientific research databases, relevant organization provided materials, public media, technology magazine articles and wearable technology vendor product and service descriptions.

## 3.2 Technology magazine articles

There are plentiful of case examples of various key tokens and device-based access controls. Wired magazine is one of the go-to technology trendsetter journals that predicts the available tools in near future nicely. The articles also cover the touching concepts such as Internet-of-Things. There are for example articles about Wearable fashion technology [17], Cisco’s Internet of everything: The connected home [18], the third wave of computing [19] and NFC ring jewel that can be used as access token [20].

## 3.3 Analyst reports on Wearable technology

Gartner Technology Research [21] as one of the world’s leading researchers of technology also covers Wearables in their reports. There are reports talking about top trending technologies on a yearly basis [22] and then there are more specific reports about wearables [23]. Deloitte has produced also reports citing the future trends for wearable computing [24]. These and more of analyst reports provide the real-life considerations and timeline for the research topic. Also, technology provider own laboratories are providing analysis reports [15].

## 3.4 Brief introduction to wearable technology and its origins

Since wider adoption of mobile phones computing has become more and more ubiquitous. The development of technology solutions into more power efficient, smaller, and computationally more powerful has then opened some new opportunities to embed such equipment into clothes and jewelry – commonly now referred also as wearable technology.

One of the first wearable technology experiment from 50's was used to calculate roulette table probabilities was not really industrialized and had to be built onto the user even several times per use occasion [25]. MIT Tin Lizzy [26] based experimental wearable system (Remus Wearable Computer) [27] running Linux late 90's was just a smaller PC wrapped on the user. These devices did not majorly penetrate the markets. More modern versions of these devices such as Europad's Zypad [28] and Samsung's Gear Fit [29] still had their challenges but now in 2020 there are many wearable solutions from ruggedized Microsoft Hololens2 [30], to Wearable rings by nfcring [31] and Smartwatches by Apple [32] and many others [33].

Wearable technology (later just wearables) as a term is somewhat loosely defined but can be described as almost any electronic device that can be worn as from functional purposes or from aesthetic reasons or both [12]. Another wave of electronics which goes hand in hand with wearables is Machine to Machine communications (M2M) also known as Internet of Things (IoT). This trending cumulates from very much from same technical advancements as wearables – improvements on power efficiency and computing power as well as cost reduction.

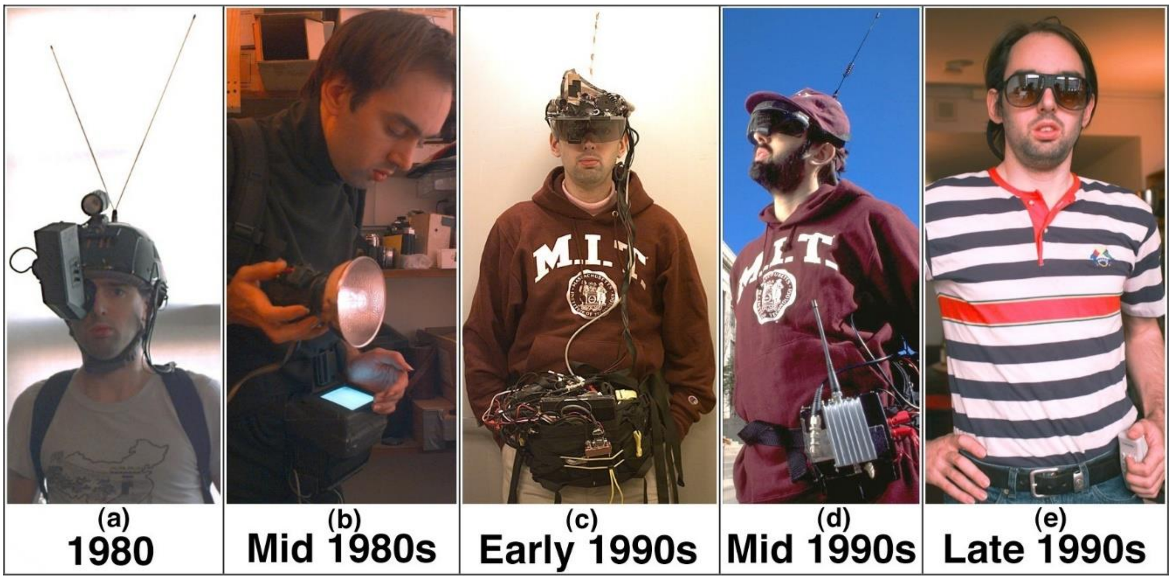


**Fig. 1.** Evolution of wearable computers in 1980s to 1990s. [34]

While the two technical worlds go on their own ways, they seem to be on a collision course too. As ‘things’ get connected to the internet then also the wearables can be used to get information from them or manipulate them (like using a smartwatch turn on house lighting). When the two areas collide, there is one especially interesting point of convergence – access control, let that be virtual or physical in nature. If one has electronic house with electronic doors and electronic ambience controlling, then one can quickly see the logic on handling

**Fig. 2.** Modern smart watch. [35]

the access control to the house and why not also the access to family photo collection similarly with the wearables one is anyway carrying.

By combining the two technology domains of wearable technology and M2M we get introduced to on- and in-body sensors and enhancements. The simplest form is a smartphone in the pocket to remind about calendar events and store contact information enhancing our memory. The available options are more numerous to count here but they include at least smart watches, eye enhancements, augmented reality addons, organ transplants, exoskeletons, body sensors and communication equipment.

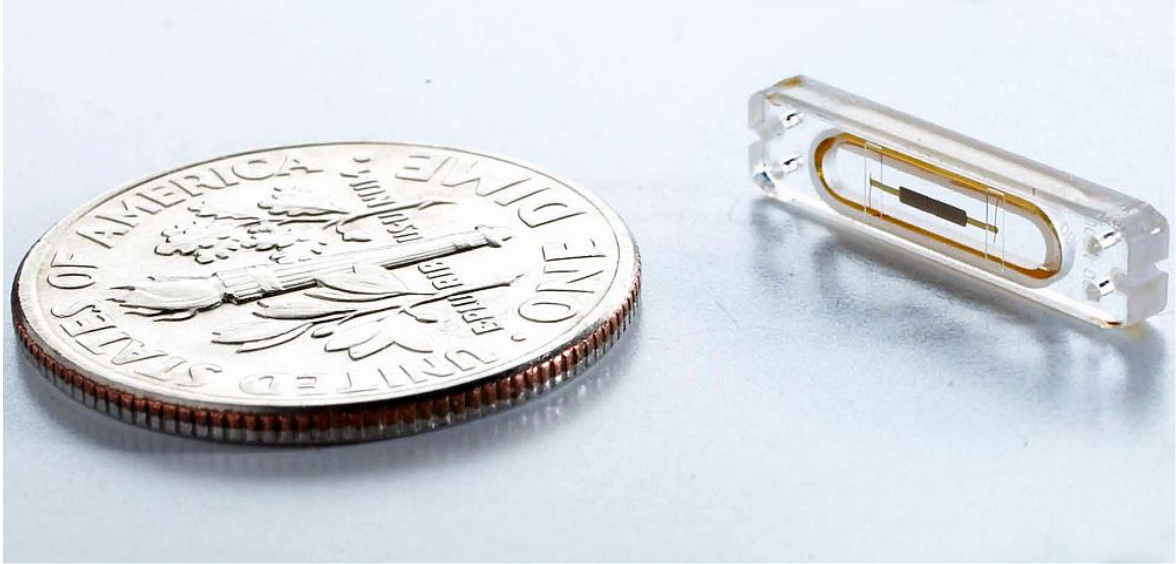


**Fig. 3.** Tiny Microelectromechanical system (MEMS) sensor that can be inserted to a human body for detecting heart failures. [36]

As the wearable computing becomes us and simultaneously the Internet-of-Things world embraces us then the likelihood that they need to interact is very high. This includes the access control into the world of connected equipment. As the connected devices, homes and even people (via sensors and enhancements) enable interaction of the digital world and the physical realm they require consideration for the risks associated. Additionally, the digital world enabled assets might be facing also different kind of risks than their fully analogous predecessors.

# 4 RISK MANAGEMENT

This section introduces basic concepts of risk management. As access control is a specific risk treatment to risks related assets it is fundamental to comprehend basics on the risk management concepts. In practical implementations where access control would be considered it would not be a separate topic but would be part of larger risk management framework looking into more holistically to the organizations, people and assets that might be under a threat and require consideration of protection. This chapter presents basic definitions and risk management process based on existing literature. The chapter is concluded in the relationship of access control to the overall risk management. New technology can both resolve some previous issues and mitigate risks, and it can introduce some new ones. It is useful to comprehend this and consider the risks overall before taking new technology into use.

## 4.1 Definitions

Multiple sources [4] [5] defines the risk via the characteristics of uncertainty of an event and the presence of possibility of adverse outcome. Furthermore, the possibility of adverse outcome is defined via the presence of a threat, vulnerability, and consequence.

Threat refers to basically things that can exploit a vulnerability either intentionally or accidentally. Such an exploit would then result into a consequence to the protected asset. [4] General categories of threats:

- natural or unnatural events that can take place in related circumstances, such events include rainfall, earthquake, lightning storm, power outage of electric grid
- person, organization, or nation that has the capability to take specific actions or make mistakes,
  - such actors could include for example bank teller, criminal organization, or a nation state
  - specific actions that could be considered include for example account transaction, theft of a car or a missile attack

Vulnerability refers to weaknesses or holes in the protection efforts for an asset. [4] Such weaknesses could be for example missing process step, leaking roof, broken fence, open gate, unfortified military base.

Consequences again are adverse outcomes that could take place onto an asset impacting their value. Assets are usually people, organizations, property – such as buildings, vehicles and goods and information or digital assets. Adverse outcomes that could occur onto such assets include events such as loss, damage, destruction, death, injury, unavailability, inaccessibility, compromise, and manipulation. There can be direct adverse impacts (primary) and indirect adverse impacts (secondary). The directness does not necessarily reflect the amount of impact. Example the loss of a key (low value asset) is the direct impact of the event of losing the key the indirect impacts could result into a misuse of the key by a thief, costs of renewing locking mechanisms or inability to access an asset such as a car. Risk can then be quantified by the likelihood of threat and value of or possible damages to an asset.

Risk management is the process of applying repeatable model and care to consider assets, relevant threats, vulnerabilities, possible consequences, and decisions on how the risks should be treated. The process can take many forms [4] [5] but usually includes at least the following phases

1) Discovery of Assets
2) Threat assessment
3) Vulnerability assessment
4) Risk or impact assessment
5) Risk treatment options analysis
6) Decisions on risk treatments and their application

The very definition of risk highlights the uncertainty and therefore a risk management comes with its own uncertainties. Valuation of an adverse impact to an asset can only sometimes be accurately assessed due to possible indirect impacts that can result as well. Likelihood of an adverse impact can only sometimes be scientifically calculated, in situations where the likelihood is certain the risk turns into a known issue. While the inaccuracies are at the very nature of risk management there are still ways to describe the picture of total risks and their usual worst-case impacts. This is very important analysis phase as the calculated expected damage determines the reasonable efforts to consider as treatments to a risk.

Looking at the risks can be done by looking at likelihood of an event, and the impact of the event as derived from the original work of defining risk by William Lowrance in 1976 where he defined the risk as “"a measure of probability and severity of harm" [5], since then there have been developed other more complex versions of this same basic concept [4, 5]. Depending on the amount of threats, vulnerabilities, consequences and probability calculation finesse the actual calculation process can be much more complicated [37]. Depending on the needs the process can be done as a one-time-event or be developed into a more continual process that reiterates the phases [5]. As an outcome of the risk treatments the general situation changes it would be advisable to apply the more continuous or repeated application of the risk management to stay aware of the current remedial risk [5].

## 4.2 Risk classifications

Risk management in any significantly more complex environment can quickly result into a myriad of identified risks and their parameters of threats, vulnerabilities, and consequences. When the complexity is not managed further the process of risk management can become inefficient. The mechanisms of classifying, rating and prioritization can assist in the complexity management. While there are many ways to categorize and classify risks (see examples in below list) one building a risk management approach should consider the classification schemes from at least two angles: what are the common ways to identify risks and what are the common ways to address or mitigate them within the organization. This approach can make it easier for the organization to both recognize the risks and group them for possible mitigations [5].

Risks and their characteristics can be categorized multiple ways. For example, based on

1) the impact type they can cause (impact type)
2) the damage amount they can cause (damage amount)
3) the likelihood how they can occur (likelihood based)
4) the threats they result from (threat based)
5) the vulnerability they exploit (vulnerability based)

6) the way to mitigate (mitigation type based)

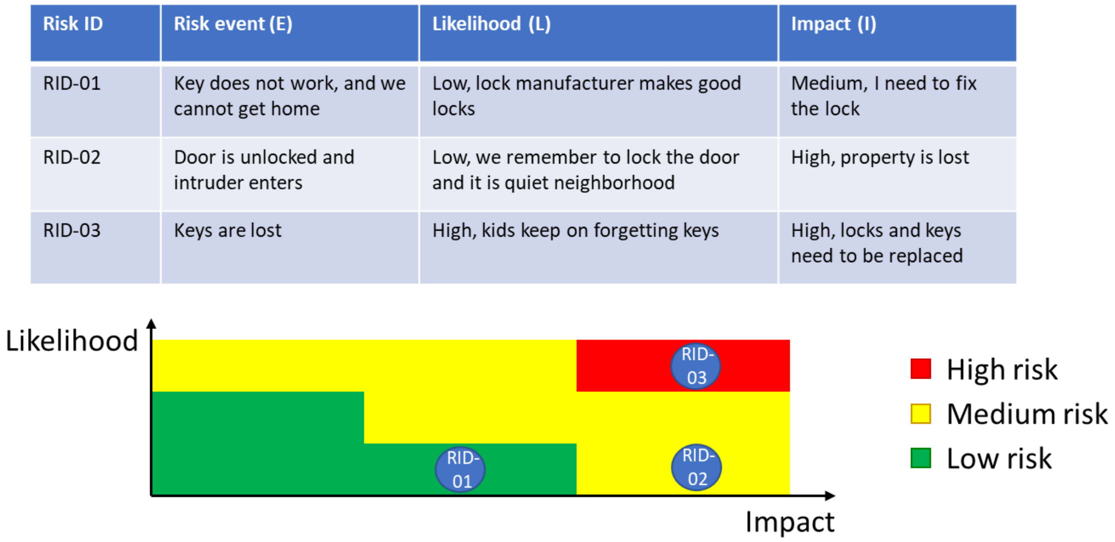
7) the efforts to mitigate (mitigation effort based)

8) the assets they apply to (asset based)

9) the asset owner (asset owner based)

10) the combinations of the above examples

Very common classification scheme is graphical visualization format where the risk has been defined as a set R= {E, L, I}. The definition of the set here is derived from Kaplan’s “The Words of Risk Analysis” [37]. E is the event of something to happen, and very commonly it is an event of adverse effects to the target of risk assessment. L is the likelihood or probability of the events occurrence, and I is the impact of the event. The risks are place on graphical layout to visualize them for the analyzer and audience. See Fig. 4. for simplified example risk assessment for a home access control situation with 3 events, their assessed likelihood and impact in a chart format, then visualized on a risk graphics. The analysis then could proceed with considering risk management options for the risks. In the example the deduction could be to switch to electronic locks that lock automatically with keys embedded to smartphones. The proposed treatment here mitigates RID-02 and RID-03 and potentially RID-01 but it could introduce the risks RID-04 electronic lock does not work due to battery failure and RID-05 doors get locked while fetching newspaper. As situations develop, risks change, and risk management might hence require an iterative and continuous process [5]



| Risk ID | Risk event (E) | Likelihood (L) | Impact (I) |
|---|---|---|---|
| RID-01 | Key does not work, and we cannot get home | Low, lock manufacturer makes good locks | Medium, I need to fix the lock |
| RID-02 | Door is unlocked and intruder enters | Low, we remember to lock the door and it is quiet neighborhood | High, property is lost |
| RID-03 | Keys are lost | High, kids keep on forgetting keys | High, locks and keys need to be replaced |

**Fig. 4.** Risk Assessment Chart example.

## 4.3 Access control in relation to risk management

Access control itself is a risk mitigation as it is purposed to limit the access to property, physical assets, intangible assets, or people to only those authorized to access them. There are however further risks that are associated to this mitigation where it is used. They can be commonly grouped into two main ones via the risk of destruction or temporary malfunction of the mitigation function either fall-backing to the situation of 1) fail-open or 2) fail-close.
1) Risk of the mitigation not functioning as intended (bypass by unauthorized person), and
2) risk of the mitigation limiting access beyond the needed for example limiting the access to the target from authorized person. Ultimately the access control failing as such is not usually the key concern of its own but it is the assets, property or personnel that the access control is protecting that become at risk of harm or exposure with a failing access control.

Depending on the application of the access control mitigation there should be a proper design in place to decide on which access control mechanisms should be in fail-open or fail-close modes. For example passage way doors would be required to fail-open or fail-safe to allow people to evacuate a burning building or vehicle while an already sealed bank vault would remain sealed even if the bank building would be on fire or under a fire alarm to mitigate the risk of robbers misusing the fire alarm system.

Access control systems themselves can be very simple such as a locked door and a matching keys to unlock it (for example garage) to a complex multi-zoned facility with multitude of different users and access needs to areas, rooms, storage units or equipment and data (for example airport). Depending on the risks associated to the property, asset or people being protected by using access control there is a usually a need to carry out system design for the access control. In many cases such designs are a combination of other designs and plans and might be even under regulations regarding building standards and for example fire safety. [38]

# 5 PROTECTING PROPERTY AND ASSETS

This section introduces basic concepts of property and assets protection. The definitions and protection needs are briefly discussed. Next risk to assets and property and mitigation possibilities are described in basic terms. Finally, the relation of access control to property and assets protection is reviewed.

## 5.1 Property and assets

Property and assets are an integral part of modern society. They can come in many forms of physical or intangible assets. They are what enable the members of the society to live and survive on daily basis. Very basic example is housing that protects from the forces of nature and predators. Others could be utilities such as heat or energy that provides warmth to the housing and water that is essential for life. Necessary knowledge, manpower, equipment, material, and infrastructure to manufacture and maintain everything needed for a modern society to function on day to day basis are hence worth protecting from disruptions and other harm. Many services and goods while not perhaps essential to life on immediate basis such as art still possess value to societies and are worth protecting from loss and destruction.

## 5.2 Risks and their mitigations possibilities to property and assets

Risks can come in many forms like described in chapter 4.1. There are also then many forms of risk management that can be considered and the related mitigations for the risks. To look at individual mitigations that might be relevant for a protection for particular property or assets one needs to put these into context and consider them equally or at least in balance to the threats being looked at. It would not make sense to invest all available resource into the flood prevention in an area prone to just drought or it would not make sense to invest into state of the art burglary protection to protect grain whereas the rodents are the most likely source of damage to the crops. For the benefit of this report we will limit the considerations here only to the access control mitigation [4, 39].

## 5.3 Access control on property and assets

Access control can happen in multiple ways for a property or an asset. It would be first of all deterring controls to keep asset undetectable for general pass-by audience and for the more direct intruder announce the asset to belong to someone else and make it initially harder to gain access for the property or an asset. For example, a datacenter could be hidden from plain sight from the street and not have big signage giving away its whereabouts or nature. If one would stumble on such a site still it would be fenced and gated off making it hard to access without determination and resource [4, 39].

Secondarily the access control could be preventative to require certain procedure to gain access to a property or an asset. The datacenter would be having locked gates and doors making it difficult to access without keys and authorization. Finally, the access control could be detective control allowing certain access but either leaving a trace of access or having then other access limiting counter measures in place after a detection would happen. An authorized person might be getting into the data center but a security guard could be monitoring the activities of the person and a theft of equipment could be stopped by the guard even if the equipment itself would not be protected withing the datacenter.

# 6 ELECTRONIC ACCESS CONTROL AND WEARABLES

This section introduces basic concepts of electronic access controls and related terminology. It first compares electronic access control to traditional access control. Next components of an electronic access control system are listed, then electronic alarm and intrusion detection technologies relationship to access control is discussed briefly. Finally, the chapter concludes in specific risks related to electronic access control systems use and wearable technology utilization possibilities as part of electronic access control.

## 6.1 Definition of electronic access control

Electronic access control is a wide term but is in basics all access control solutions or complete access control systems either fully or partially supported by electronics. Usually the simplest example is electronically lockable and un-lockable door. Depending on the needs for the access control these electronics can be user operated with electronic keys, cards or tags or remotely operated by facility or security management as needed or automation and sensor based [38, 40, 6].

## 6.2 Comparison of electronic and traditional access control

Traditional access control is quite limited in functionality and operation. That usually being just fences, walls and analogously locked or physically jammed gates, doors, and windows. Traditional access control also covers the physical security guarding and possible physical alarms. A traditional access control solution or system can be sometimes enhanced with sensors (door open/closed, camera system) but still not changing the actual access control system into an electronic one. The main difference is hence the fact that in electronic access control solution or system the users of the system can gain access without physical keys. The most common reason to move into electronic access control is hence to replace the physical keys with the possibility to issue access to users without having to physically alter the lock-systems [38]. Depending on the various access needs for a property or set of assets it is still quite common that some rarely and limitedly accessed parts of the protected target are partially using analogous locks and keys due to the cost, regulation or other complexity of managing the entirety of the solution.

## 6.3 Components of electronic access control solution

Electronic access control system can be split into multiple components. The most common key components are:

1) The closing/locking/opening mechanism (usually locks, key readers, motors, needed power and direct control components).
2) The key (this can be a device, software, electronic radio transmitter, key card, password/PIN code or biometric characteristic, authorized license plate).
3) Control system to match users to keys and the keys to closing/locking/opening mechanisms [40].

## 6.4 Alarms, intrusion detection and electronic access control

Whilst the heavily evolving alarm and detection technology is quite often combined with electronic access systems it should be still considered separately. The developments in facial and video image recognition could open further doors to even move towards “keyless” access control which would recognize the users themselves and hence users themselves becoming the keys for such a system. In current maturity of these technologies such access control solutions are rarely used solely in any higher risk protection environments. Facial and image recognition technology is still already utilized successfully in some situations such as by utilizing virtual fences in video surveillance systems [41]. Another example is car parking to allow already invoiced parking customers to enter and exit the parking area by reading the vehicle license plate [42].

## 6.5 Specific risks and considerations with electronic access control

Electronic access control has key benefits that comes in form of electronic and often remotely managed access token credentialing, accounting, and access configuration. These same aspects are the key specific risks and consideration aspects when comparing electronic access control solutions to traditional access control solution. First risk is the use of electronics. They require power and can be susceptible to power surge damages or power outages. The consideration of power is fundamental when choosing electronic access control solution over a traditional. Second key consideration and risk is connectivity, integrations, and compatibility. Traditional access control is self-reliant while electronic access control is usually connected to its own other nodes, control system and potential remote management, it is also often supporting a number of technologies of which some or all might become obsolete during the life-cycle of the access control system itself. This connectedness adds into complexity of the system and especially systems which support multiple external integrations require extensive system testing and maintenance for all the supported features. Innovations, technological advancement and consumer electronics cheaper prices have started to open electronic access control markets also to consumer and everyday use cases [43]. As the technology is emergent there are risks that have realized already in some situations [16]. Access control technology is also IoT technology and should be considered against IoT security best practices [44]. Finally, the electronic access controls usually collect usage records. These records can become a register of personally identifiable information (PII). PII processing is regulated for example in United States and within European Union [45, 46]. Without the required focus on handling such records the access control system operator can violate privacy regulation even by mistake resulting to fines or other legal consequences.

## 6.6 Wearables in electronic access control

Wearable technology comes in many forms and as such can be utilized in various ways together with access control to provide additional functions like payment solutions, security by providing additional layers of authentication or by providing other user context to determine the authorization for access in specific circumstances and for example usability allowing for example the utilization of a ring on finger as an access token to an electronic lock. Wearables could also assist the electronic access control operator or guard work by providing additional capabilities such as augmented reality views to a building and its current users to a guard for better focusing the guarding rounds to zones with people [30, 47, 48].

# 7 USE CASE ANALYSIS FOR ACCESS CONTROL

In this chapter we introduce a concept of analyzing different access control technologies in different access control use cases. First the selection criteria for use cases and the analysis model is explained. It is followed by selection criteria explanation and descriptions of the chosen access technologies. The use case sections first describe the chosen use case and its specific bias for review criteria by analyzing the relations of the protected assets and property characteristics, users, access profile and protection target. The sections for use cases also review the access control technologies suitability for the use cases and finally conclude in learnings from each use case. The chapter then summarizes overall learnings between all use cases. This is done by comparing the use cases and access control technologies in a matrix table and by analyzing the access control technologies suitability for different kind of access control needs. As conclusion, the market situation and outlook for the selected access control technologies is discussed.

## 7.1 Use cases selection and review model

The use cases presented in this section were selected as common situations where access is being controlled to protect property, assets, and people. The use cases are reviewed individually to assess the various access technology suitability and possible additional benefits/downsides of using wearables in the use case situations. The use case specific risks of chosen technologies are also considered. For the review we adopt the system qualities as utilized in system design and testing for example by IBM: reliability, availability, and serviceability [49]. The aspect of usability was added as access control system has human-machine interaction present. The adaptation from the model is done to suit for the access control system specific characteristics also emphasizing the use case specific characteristics. Reliability is considered in terms of the technology function in the use case and by the match to the needed protection level. Availability is considered through the likely and common malfunction situations or other unavailability risk. Serviceability is viewed from first the angle of revocation and modification of accesses as well as the possible technical maintenance angle. Usability is viewed from the common use situations with the use case – access token addition, access granting and use of token by the user. Finally, security and privacy are derived from the usability quality. These domains are viewed and graded separately as they play a specific role in modern connected access solutions [12, 50]. Cost of acquisition and initial installation is omitted as all solutions have this cost it is considered in this study as carrying small enough cost difference that it is omitted from the review. The maintenance efforts, their costs and the equipment maintenance have been embedded into the grading of serviceability and usability.

For the characterization and security targets of each use case we utilize the model defined in Mary Lynn Garcia's book: Design and Evaluation of Physical Protection Systems [51]. In the model there are three parts to analyze: "Facility Characterization, Threat Definition and Target Identification". Using these as modelling patterns within the use cases, we will justify the grading bias for each use case review.

## 7.2 Access technologies reviewed for use cases selection

The selected access technologies are same for all use cases so their suitability in combination can be considered. The selected access technologies selection was done by choosing traditional access controls seen in daily basis throughout the society 1) traditional lock and key, and 2) Proximity cards. They were then accompanied with less common but utilized and technology considered as a secure identification 3) Biometrics based readers. Finally from the category of wearables 4) Smart phone app, 5) Smart watch and 6) Wearable ring / jewel were chosen as having existing market solutions for access control and to provide more deeper insight into the nuances within the wearable technology in the context of access control. The technologies do not refer to any specific vendor or protocol but are general approximations of actual solutions as defined later in more detail. There are more detailed specification documents for access control technologies such as the British Security Industry Association "Specifier's guide to access control systems" [52] and others [6, 38]

*Traditional lock and key* refers to a basic physical lock and key mechanism such as a rim, mortise or pin tumbler cylinder lock where the key and lock are physically configured to function together and in our selection here also allow certain configurations for universal and group keying. In Figure 5 the functionality of basic pin tumbler lock is explained. Figure 5 diagram (1) is showing an unengaged pin tumbler lock where pins are firmly down and preventing the lock from turning. Diagram (2) shows how wrong key when inserted will not line up the pins and still preventing the lock from turning. Diagram (3) is visualizing how the correct key lines up the two-part pins with the lock cylinder and in diagram (4) shows how the right key allows the lock to be turned and unlocked.

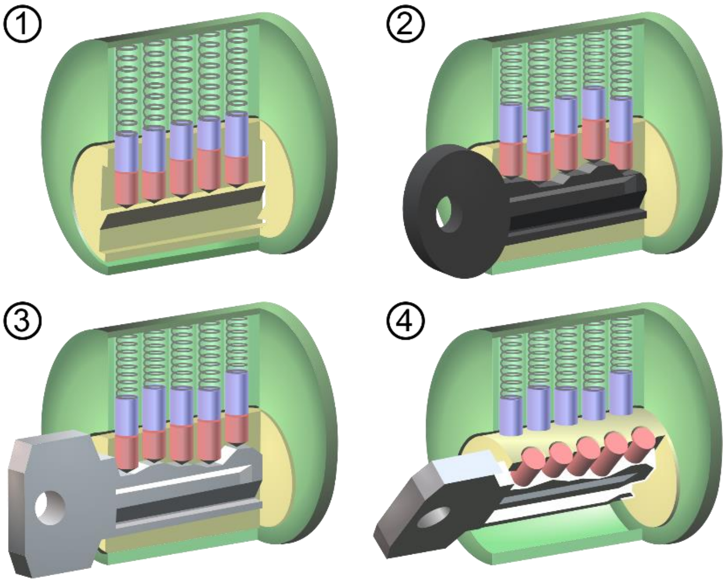


**Fig. 5.** Pin tumbler lock function illustration [53]

It is to be noted that the reviewed literature for access controls did not refer any more to the physical key-lock systems, as they do not support easy key replacement, revocation and integration to other security solutions such as alarms and access monitoring. *Proximity card* refers here to a proximity/connectionless card using wireless technology and related authentication protocols such as Near Field Communications (NFC) and HID iClass based on 3DES [13]. *Biometrics* refers to a biometrical characteristic recognition technology such as fingerprint reader [52]. Smart phone app refers to a solution where the smart phone NFC or Bluetooth antenna is used to interact with the reader and app is providing the authentication challenge response. Smart watch refers to a solution where the smart watch NFC or Bluetooth antenna is used to interact with the reader and the watch app is providing the authentication challenge response. Wearable ring / jewel refers in the following use cases to wearables generally smaller than smart watches and lacking a user interface beyond predefined functions thus requiring a companion equipment / software for mobile devices or workstations to reconfigure.

## 7.3 Use case 1: Hotel room and general access for tenants and staff

### 7.3.1 Definition of the use case, characterization, and protection targets

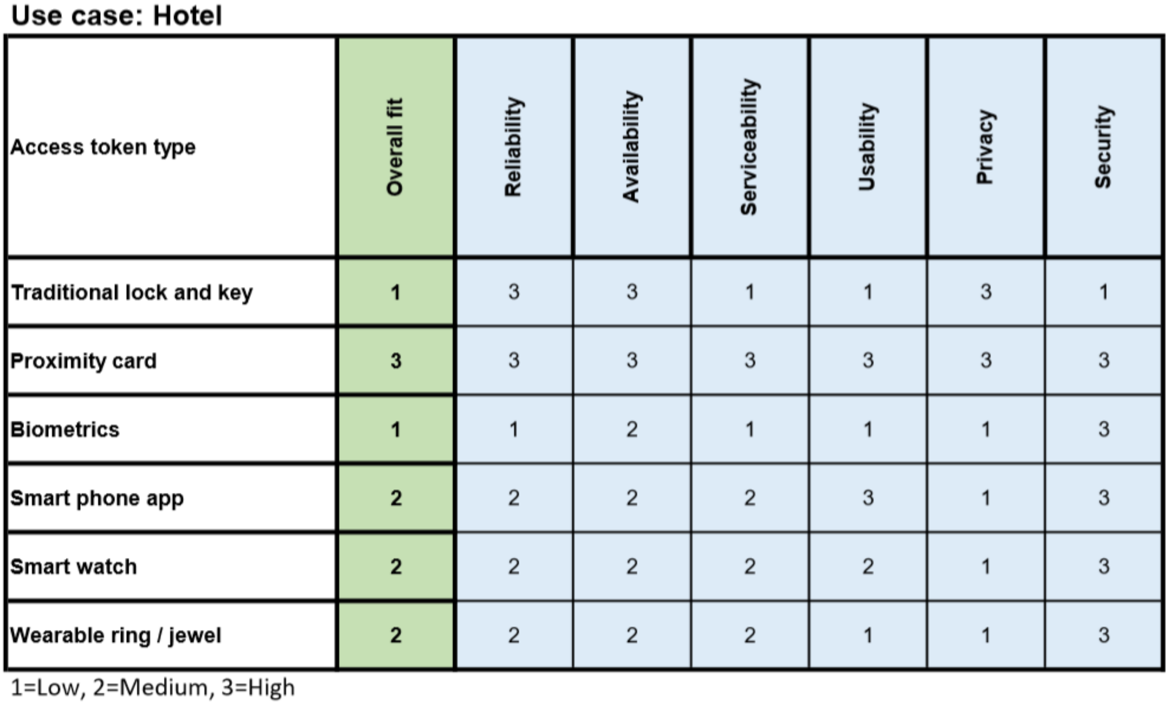
Hotel is a model of accommodation where the customers frequently change, usually even on daily basis. The tenants come from of all demographic, geographic, educational and ability groups. The common access situation is to enter the premises, be granted access to one or more hotel rooms. The other key access situation is the non-tenant allowed access areas such as building technical spaces, kitchens, storages, and closets where access with dedicated hotel personnel and maintenance staff. In usual situations the protection target is to protect the hotel rooms from unauthorized access to protect the hotel guests and their property. The hotel rooms also have hotel property and need to be accessible by the hotel personnel. Building other areas contain both property and building essential facility functions which must be protected for various reasons but mainly to ensure safety of building occupants. The amount of people using the access control system of a hotel on daily basis can be in hundreds and sets specific usability requirements for reliability, availability, serviceability, and usability. Also, privacy can be essential as many times the hotel visitors wish to keep their presence during and after the visit in limited knowledge.

### 7.3.2 Comparison of access technologies for the use case

All six access technologies were compared against the use case parameters and grades were collected into a table. The table is visible in the below figure 6. *Traditional lock and key* scored fairly on reliability, availability, and privacy, it is functional and well adopted technology. It how ever has clear downsides in the use case as a lost key cannot be replaced easily but requires a massive effort of rekeying complete parts of the building (assumption here is that the hotel building would have serialized keying to allow for cleaning crew, maintenance and room services to have reasonable amount of keys while working. Having every room separately keyed would ease the work of rekeying but means heavy keychains for the personnel. *Proximity card* is well adopted and easy to use, many hotels currently utilize such solution. Proximity card-based solutions are reliable, and keycards are quick to replace and or re-authorize to different access zones or rooms.

*Biometrics* solution that could be somewhat considered for a hotel setting would be fingerprint readers. This solution would offer good security but require longer time to enroll tenants into the hotel and come with reliability risks when tenants have wet, dirty, dry, or otherwise fingerprint changes during the visit. Also, the privacy is at increased risk as biometrics are considered as a sensitive personally identifiable information in many countries and regions [45, 46]. It could also require hence a fallback double solution to support for tenants not interested to utilize their fingerprints either from hygiene or privacy reasons.

*Smart phone app* is a reliable and functional solution also for hotel environments albeit it requires user skills, compatible smart phone and user willingness or interest to use their mobile device in this setting. *Smart watch* and *wearable ring / jewel* were considered to require additional user skills and further effort from both the enrollment process and use point of view. All wearable solutions come with a certain expectation to be only a secondary/optional access solution in a hotel setting and hence they would need additional fallback solution to go with them.



**Use case: Hotel**

| Access token type | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|
| Traditional lock and key | 1 | 3 | 3 | 1 | 1 | 3 | 1 |
| Proximity card | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| Biometrics | 1 | 1 | 2 | 1 | 1 | 1 | 3 |
| Smart phone app | 2 | 2 | 2 | 2 | 3 | 1 | 3 |
| Smart watch | 2 | 2 | 2 | 2 | 2 | 1 | 3 |
| Wearable ring / jewel | 2 | 2 | 2 | 2 | 1 | 1 | 3 |

1=Low, 2=Medium, 3=High

**Fig. 6.** Comparison chart of access technologies for ‘Hotel’ use case

### 7.3.3 Learnings from the use case

When looking at the use case table there are no major unexpected results. The traditional lock and key and biometrics do not seem like very potential choices for the use case. Proximity card is clear choice over the other technologies. Wearable solutions could be utilized in addition to the proximity but as only as supplementary basis as their overall adoption is still quite far from 100%. Statistics Finland has reported that only 10-20% of all Finnish citizens have used activity tracker or smart watch devices for sports. Ericsson Consumer labs report from 2016 did however report that consumers expect more functionality from their smart wearables beyond sports and activity tracking [15, 54]. It is very clear still that from all the demographics and backgrounds of hotel tenants there are still a large portion who do not have a suitable equipment nor knowledge and skills to operate them to their full effects. Adding to the challenges a hotel faces when considering the addition of wearables as access mechanism is the personnel skills and efficiency; increasing technical options and complexity with "any consumer device supported" can quickly add up to a sizeable additional investment from hotel operator point of view.

## 7.4 Use case 2: Private home and related area doors

### 7.4.1 Definition of the use case, characterization, and protection targets

Home is defined here as a form of continuous dwelling in a separate house of a shared dwelling such as a block of flats. A home is a place where the residents do not change very often, access zones are very simple and most of the times access is granted only to very closely known individuals with the possible consideration for renovation crew, cleaning services, delivery person or other service providers. Access zones in a home is usually just one – one can either get into the home or not. There can be additional zones needed for household valuables (a safe), dangerous items (weapons cabinet) or dangerous materials (medicine cabinet). The home or house can also have multiple buildings or building compartments where the access could be set separately like the garage, storage unit, basement. While the access setting is usually quite stable it does not mean that there could not be people with varying level of abilities living in the home such as elderly people, children, people with disabilities. In the use case analysis it is considered that the people using the home would be generally able to use the chosen technology and in special setting where disabilities or skills would be a clear issue the technology would just be disregarded. The overall usability or fit of the technologies and how they could potentially gain or lose share is considered in later chapters.

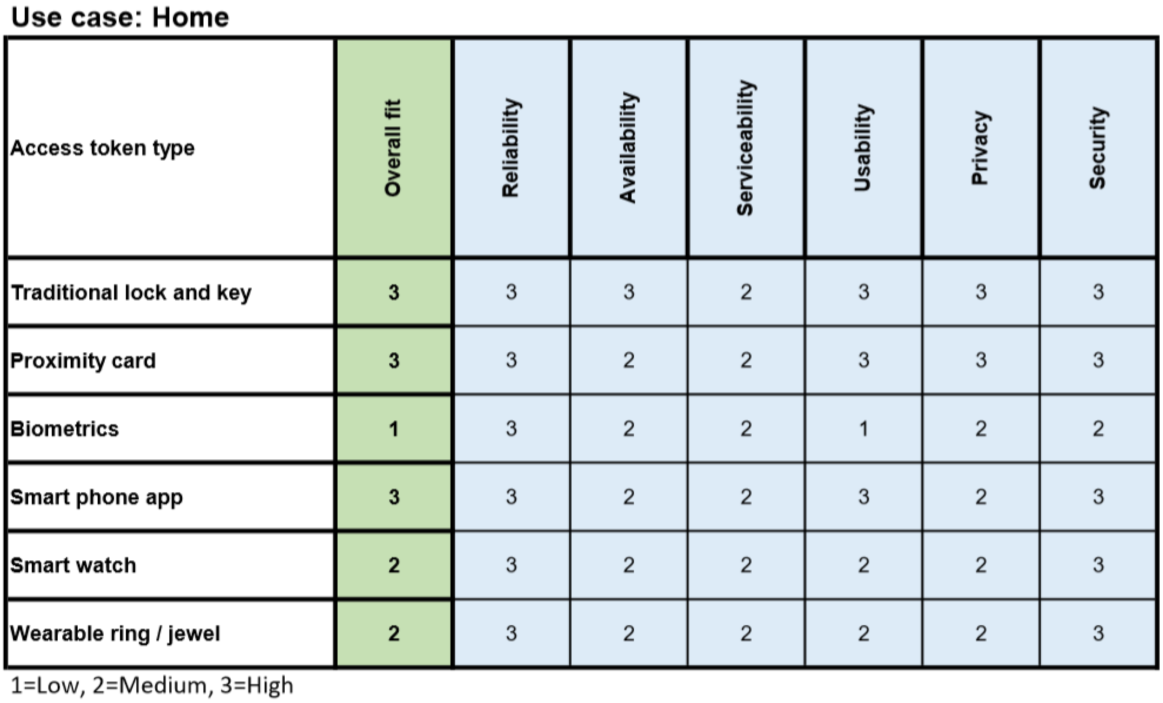
The protection target for a home is the people living in the home and their property. In some situations, the risk of unauthorized people entering to a home could also be a risk to the building itself whether it is owned by the same people that the home is. Burglars could break in and steal valuables and set the building on fire to cover their tracks, posing threat to possible other homes of the building and or at minimum cause additional property damage in addition to the theft. The reliability and availability of an access control must be adequate as housing is one of the very critical basic needs and if considering some special circumstances such as polar regions where it can be very cold outside or in warm areas where the immense heat could be a serious health risk if one cannot find shelter from their homes. Serviceability is a topic as usually the access control systems are maintained by the occupants of the home and should there be a malfunction there might be situations where the only way in is a break-in – to avoid the risk of needing to fallback to breaking in to a home one should consider having a fallback mechanism for some access control solutions. Privacy and security can be less of a topic for a home but must be adequate for the regional or area circumstances. A warzone requires different level of security for the doors and locks than a quiet suburban setting.

### 7.4.2 Comparison of access technologies for the use case

All six access technologies were compared against the use case parameters and grades were collected into a table. The table is visible in the below figure 7. *Traditional lock and key* scored well on all but serviceability and even there it is still ok. The downside of it is that in the a lost key cannot be replaced easily but requires an effort of rekeying, in shared buildings this can mean not just the home door but also parts of the building as well, such as shared lobby doors, garage and storage units. The risk of losing keys is lower than in some other settings as the keys are in constant use are a critical item for the occupants. *Proximity card* is well adopted and easy to use and many shared buildings already use this technology everywhere else but the home door itself due to the potential high costs of occupant lost keys and effort to replace / re-key the physical locks of common areas. Proximity card-based access is reliable and easy to use, however in a home setting the serviceability and availability might be an issue especially where the occupants are responsible for the maintenance of the solution like in the case of homeowners.

When looking at the *Biometrics* solution such as fingerprint readers, individual grades it looks quite suitable to a house at first glance – however the overall fit goes quite low due to the very common situations of needing to share keys to a home. Keys to a neighbor to get in and feed the pets or water the plants, keys for leasing the home for short periods of time. As biometrics cannot be handed over but require an enrollment process with the person present it might be quite unusable in most situations. Also, in home setting occupants regularly have wet, dirty, or dry hands or otherwise fingerprint changes over time increasing the risk of availability. Privacy can be a concern too as biometrics are considered as a sensitive personally identifiable information in many countries and regions [45, 46]. Depending on the reader setup the biometric data could be handled outside of the occupants' control.

*Smart phone app* is a reliable and functional solution also for home environments albeit it requires user skills, compatible smart phone and user willingness or interest to use their mobile device in this setting. *Smart watch* and *wearable ring / jewel* were considered to require additional user skills and further effort from both the enrollment process and use point of view. These four last solutions implementations were assumed only for homes where the homeowner or occupants have the skills to setup and use them. Hence the consideration was not done in a generalized setting. The later chapters will investigate the general usability in larger scale.



Use case: Home

| Access token type | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|
| Traditional lock and key | 3 | 3 | 3 | 2 | 3 | 3 | 3 |
| Proximity card | 3 | 3 | 2 | 2 | 3 | 3 | 3 |
| Biometrics | 1 | 3 | 2 | 2 | 1 | 2 | 2 |
| Smart phone app | 3 | 3 | 2 | 2 | 3 | 2 | 3 |
| Smart watch | 2 | 3 | 2 | 2 | 2 | 2 | 3 |
| Wearable ring / jewel | 2 | 3 | 2 | 2 | 2 | 2 | 3 |

1=Low, 2=Medium, 3=High

**Fig. 7.** Comparison chart of access technologies for 'Home' use case

### 7.4.3 Learnings from the use case

When looking at the use case table there are no major unexpected results. The traditional lock and key and proximity card-based solutions seem like the obvious choices for the use case. The wearable solutions could be utilized in addition to the proximity card. It is still quite early to consider the more technical solutions use on bigger scale as overall adoption of these in general is still fairly low [15, 54]. However, the usually stable access setting allows the time for longer or more complicated enrollments in a home use case and can make the technical options other benefits more and more appealing to home occupants. The relatively good sub-scores of biometrics were a somewhat interesting discovery however the overall suitability of it to a home use case was not an unexpected result.

## 7.5 Use case 3: Office building doors, floors, and maintenance spaces

### 7.5.1 Definition of the use case, characterization and protection targets

Office building as a location for managing accesses is at the same time complicated but relatively stable. Depending on the office use purposes it should be still considered that users of the office space whether they are regular users, visitors or building maintenance personnel - come from of most demographic, geographic, educational and ability groups. The common access scenarios are a fixed access zones for different organizations or organization departments, visitor access with the same fixed access zones or more narrowed down zones and finally the building maintenance and or other support personnel and guards access throughout the building. Within the zones there might still be a need to have additional access controls like locked cabinets, storages or data rooms and information security practices for equipment such as workstations, network devices and printers.

In usual situations the protection target is to protect the office occupying organization personnel, data and property from unauthorized access, destruction or theft. Some organizations can have also non-functional valuable property in the offices such as art or personnel personal belongings like wallets. In many situations, the risk of having unauthorized people within an office could also be a risk to the building itself whether it is owned by the same organization or not. Burglars could break in and steal organizational assets, destroy equipment and set the building on fire to cover their tracks, posing threat to possible other homes of the building and or at minimum cause additional property damage in addition to the theft.

The reliability and availability of an access control must be adequate as many times the office and the appearance of it is directly linked to the brand and reputation of the organization as well as the office and access to it could be critical to the organizations continuity. However as the continuity for an organization is a key risk there should be alternative locations for the business to continue operations for many other risks point of view as well (such as loss of building to a fire) that these countermeasures should also cover the mere issues of inaccessibility to a building for some days.

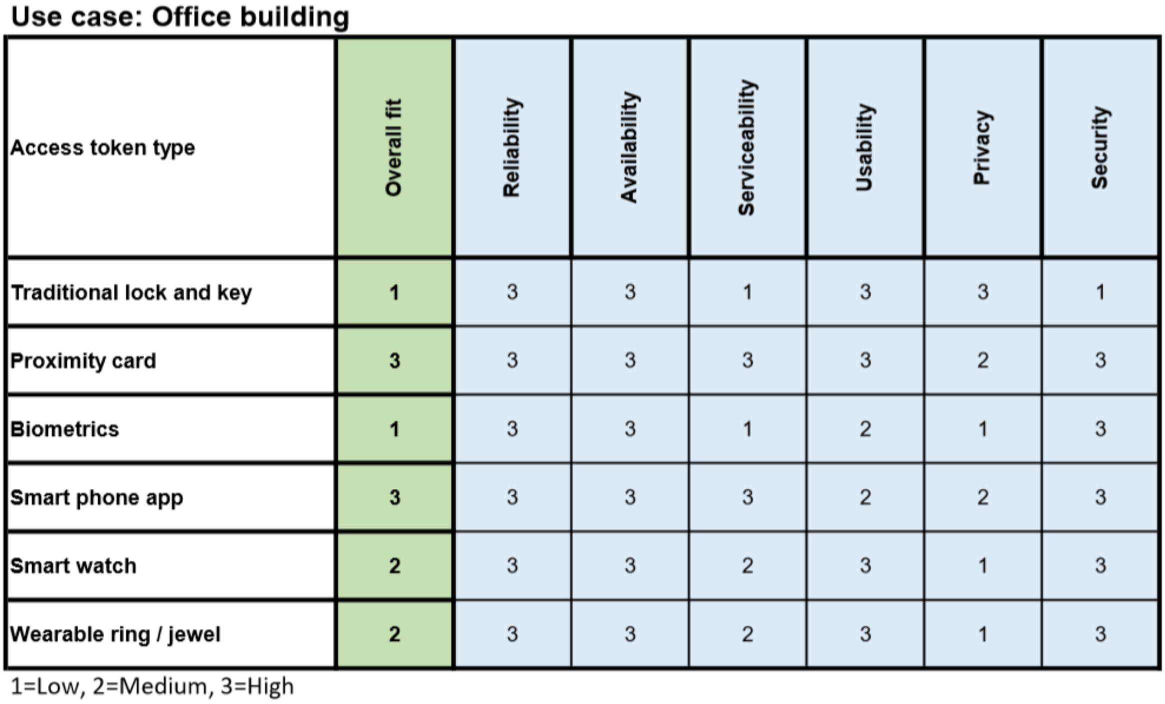
Office building other areas contain both property and building essential facility functions which must be protected for various reasons but mainly to ensure safety of building occupants. The amount of people using the access control system of an office on daily basis can be in hundreds and sets specific usability requirements for reliability, availability, serviceability and usability overall. Usability can be very critical factor also for security angle as dysfunctional access control systems tend to be bypassed by office user by jamming doors open if the access is not seen as very important or is seen as major obstacle for continuous fluent use of the office. Also, privacy can be essential as for many countries and regions there are special regulations in place for employee monitoring or limitations for it. Security can be less of a separation topic for an office building but must be adequate for the regional or area circumstances. A warzone requires different level of security for the doors and locks than a quiet suburban setting.

### 7.5.2 Comparison of access technologies for the use case

All six access technologies were compared against the use case parameters and grades were collected into a table. The table is visible in the below figure. 8. *Traditional lock and key* scored fairly on reliability, availability and privacy, it is functional and well adopted technology. It however has clear downsides in the use case as a lost key cannot be replaced easily but requires a massive effort of rekeying complete parts of the building (assumption here is that the office building would have serialized keying to allow for guards, maintenance and cleaning services to have reasonable amount of keys while working. Having every office zone separately keyed would ease the work of rekeying but means heavy keychains for the personnel. As keys are hold by their assigned users for long periods the risk of discovering loss of keys only after longer period is significant additional consideration for office buildings. *Proximity card* is well adopted and easy to use, many offices currently utilize such solution. Proximity card-based solutions are reliable, and keycards are quick to replace and or re-authorize to different access zones.

*Biometrics* solution that could be somewhat considered for a general office building setting would be fingerprint readers. This solution would offer good security and usually good reliability for office use. The privacy is at increased risk as biometrics are considered as a sensitive personally identifiable information in many countries and regions [45, 46]. It could also require hence a fallback double solution to support for office user organizations not interested to utilize their personnel fingerprints either from hygiene or privacy reasons.

*Smart phone app* is a reliable and technically functional solution also for office environments albeit it requires user skills, compatible smart phone and user willingness or interest to use their own mobile device in this setting or the organization to issue organizational equipment supporting the access technology. The mere possibility of such limitations might require a secondary access mechanism for users without wearable devices. *Smart watch* and *wearable ring / jewel* were considered to require additional user skills and further effort from both the enrollment process and use point of view. Many offices have multilayered access zoning and a smart phone might require cumbersome process to be used at every door depending on the chosen technique: reach out for a phone, unlock phone, locate app, unlock app and unlock the door. Also, office users might be carrying other things while moving across the office so needing to use a smart phone on the door could pose practical challenges even when used once. While the process could be quite ok for unique use, it will become quite unusable in daily use. The more easily accessible smart watches and wearable rings and jewels might not have the same complications though so were considered more usable in the office setting.



**Use case: Office building**

| Access token type | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|
| Traditional lock and key | 1 | 3 | 3 | 1 | 3 | 3 | 1 |
| Proximity card | 3 | 3 | 3 | 3 | 3 | 2 | 3 |
| Biometrics | 1 | 3 | 3 | 1 | 2 | 1 | 3 |
| Smart phone app | 3 | 3 | 3 | 3 | 2 | 2 | 3 |
| Smart watch | 2 | 3 | 3 | 2 | 3 | 1 | 3 |
| Wearable ring / jewel | 2 | 3 | 3 | 2 | 3 | 1 | 3 |

1=Low, 2=Medium, 3=High

**Fig. 8.** Comparison chart of access technologies for ‘Office building’ use case

### 7.5.3 Learnings from the use case

When looking at the use case table there are no major unexpected results. The traditional lock and key and biometrics do not seem like very potential choices for the use case. Proximity card is clear choice over the other technologies. Wearable solutions could be utilized in addition to the proximity but as only as supplementary basis as their overall adoption is still quite far from 100% [15, 54]. It is very clear still that many offices would have users from demographics and backgrounds that would struggle using or do not even have suitable equipment. The smart phone still raises to the list of usable solutions as many office users would be provided already with suitable equipment and there are major solution providers supporting this technology in a limited deployment setting. While smart watches and wearable rings and jewels could be more usable in the use case they could be harder to properly support and enroll as well as their overall availability to be in wide scale use make them still less suitable overall for the office use case.

## 7.6 Use case 4: Unlocking and locking city bikes / ad-hoc rental cars

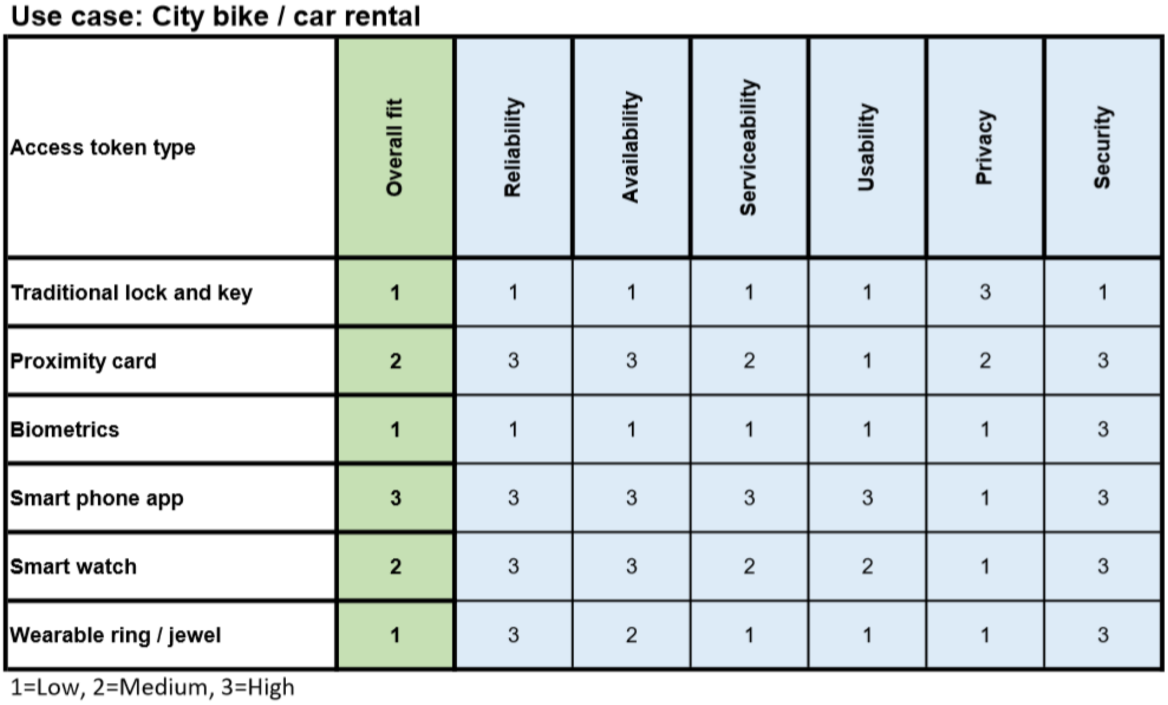
### 7.6.1 Definition of the use case, characterization and protection targets

City bike or ad-hoc car rental as a use case is quite different to the other use cases as in this one the access control is mobile or distributed widely. These services are commonly associated to be part of a Mobility-as-a-Service (MaaS) concept. In MaaS the main idea on such services are that users either do not possess the mobility solutions at all or travel around with so many different solutions that it becomes infeasible to own the solutions of fixate on just one of them [55, 56, 57]. These services can come in different forms but, in many cities, they have already been combined into mobility packages. Packages could include trips with taxi, use of city bike, allowance of car rental and mass transport tickets such as busses, metros and trains. Whether the user of these services is a regular one or a visiting ad-hoc user such as a tourist, the potential users come from of all demographic, geographic, educational and ability groups. The common use scenarios are the ticket purchase, rental payment or subscription payment and then accessing the chosen transport option whether that is just the consumption of the individual ticket or selecting the desired bike or car and then unlocking the locks / doors of it. The last step in the scenario is the possible return check procedures and locking the returned vehicle. While the focus is on the access control the special nature of the contracting that takes place at the same time is considered for usability part of the analysis.

The protection target within this use case is to protect the vehicles from loss and damage as well as ensure correct service charging from the users by disallowing unpaid use. With some transport mechanisms it is important to ensure the driver's eligibility for the vehicle as renting a vehicle to person without proper driver's license can be considered illegal in some countries and regions as well as might cause a risk to public safety to have larger vehicles at the hands of unexperienced driver. The amount of people using the vehicle access control system can be in hundreds on daily basis and sets specific usability requirements for reliability, availability, serviceability and usability. Also, privacy can be essential as many times the vehicle users wish to keep their whereabouts and use of vehicles during and after the ride in limited knowledge. Security is a key issue especially for more valuable vehicles like cars.

### 7.6.2 Comparison of access technologies for the use case

All six access technologies were compared against the use case parameters and grades were collected into a table. The table is visible in the below figure 9. *Traditional lock and key* were clearly unsuitable for the use case. It would be very hard to manage physical keys for all the cars and physical bikes for a geographically spread regions and ad-hoc usage, bike keys could be considered perhaps to be changed on seasonal basis with every one purchased a subscription having a key. Cars would not be feasible at all with a direct key use mechanism. If the physical keys would be stored nearby the vehicle in a separate key cabinet that is accessible with for example a smart phone that could be still considered but would still be prone to user errors and misuse. *Biometrics* solution is also seen as completely infeasible due to the requirements to have offline unlocking capabilities as well as reliably enroll ad-hoc users to the biometrics management system. The privacy would be a special concern as well as biometrics are classified as sensitive personally identifiable information in many countries and regions [45, 46]



Use case: City bike / car rental

| Access token type | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|
| Traditional lock and key | 1 | 1 | 1 | 1 | 1 | 3 | 1 |
| Proximity card | 2 | 3 | 3 | 2 | 1 | 2 | 3 |
| Biometrics | 1 | 1 | 1 | 1 | 1 | 1 | 3 |
| Smart phone app | 3 | 3 | 3 | 3 | 3 | 1 | 3 |
| Smart watch | 2 | 3 | 3 | 2 | 2 | 1 | 3 |
| Wearable ring / jewel | 1 | 3 | 2 | 1 | 1 | 1 | 3 |

1=Low, 2=Medium, 3=High

**Fig. 9.** Comparison chart of access technologies for ‘City bike / car rental’ use case

*Proximity card*-based solution would require the users to get a card from a separate enrollment location prior to ad-hoc use of the bikes making it less usable compared to solutions that could combine the purchase event and unlocking. When users have the proximity card with required funds or invoicing mechanism the proximity card-based solution would be very usable and convenient way to access the desired transport solutions. Smart phone app allows more complex application to support the user for usage or subscription payments as well as possible additional services such as locating transport options and vehicles to use. *Smart watch* and *wearable ring /jewel* as a convenient solution for actual vehicle use situations could be usable but will not function solely without the accompanying smart phone app or enrollment location capable of supporting the users with their chosen supported devices. This lowers their usability score in the use case.

### 7.6.3 Learnings from the use case

When looking at the use case table there are no major unexpected results. The traditional lock and key, biometrics and wearable rings / jewels do not seem like very potential choices for the use case. Proximity card might be a choice for users who are willing to get to a location to enroll for the card. Smart phone app is the obvious choice in this use case as it allows more complex application to support the user for usage or subscription payments as well as possible additional services such as locating transport options and vehicles to use. *Smart watch* and *wearable ring /jewel* could offer some additional convenience for actual use situations, but as they require additional enrollment they would be considered only by most active MaaS users. could be considered more user friendly but will not function solely without the accompanying smart phone app or enrollment locations capable of supporting the users with their chosen supported devices. Also the low overall adoption rates of these technologies do not support their wide scale use for the use case [15, 54].

## 7.7 Use case 5: Public service access for nursing and emergency services

### 7.7.1 Definition of the use case, characterization and protection targets

Public services in this use case refer to emergency response and nursing services offered to various locations and homes. In an emergency it is of upmost importance to reach the accident place or sick patient location in timely fashion – where lives are at stake then use of raw force can be considered to arrange access for emergency crews. However not all emergency crews are equipped to breach buildings nor in many cases it is well suited and hence emergency crews are waiting for building maintenance teams for access or spend additional time to seek out and access potential maintenance key storages. Nursing teams work in shifts to visit people needing care in their own homes and as teams change often a traditional key management is an additional burden and risk of keys getting lost or just left to wrong nurse is a real daily concern.

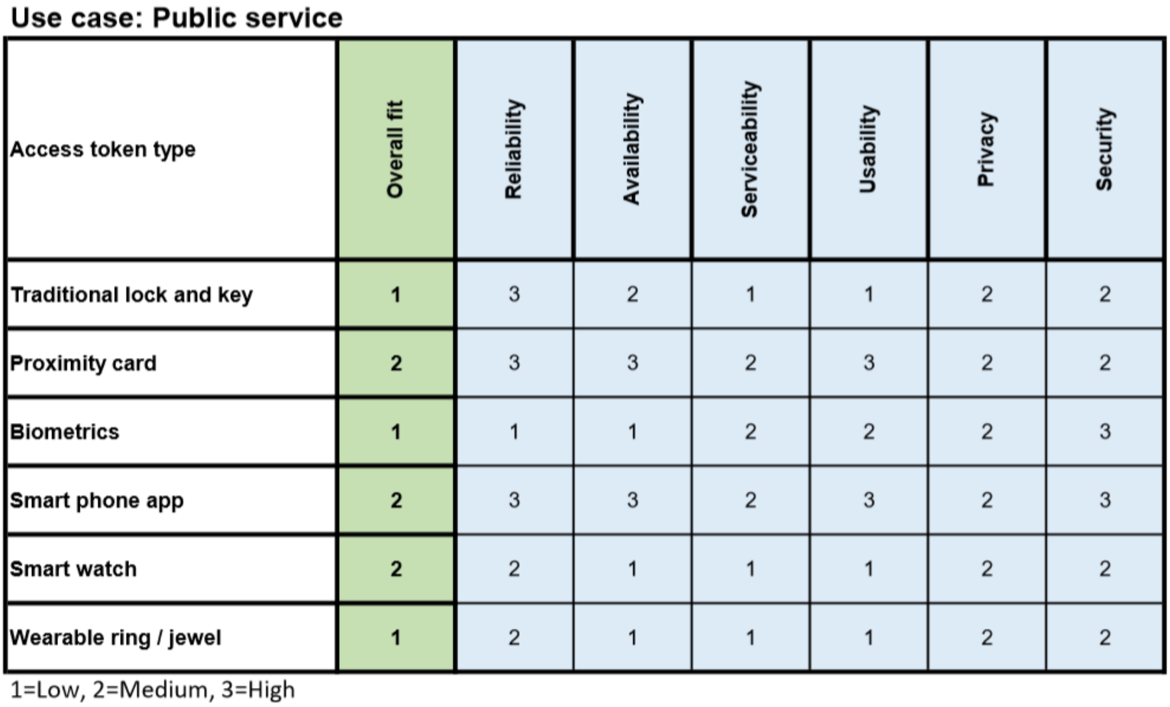
As the buildings and homes where the access might be needed can vary and for emergency teams it can literally be anywhere in this use case the key considerations is put onto the possibilities to spread the technology and access throughout large environments which can be office buildings, shops, manufacturing units, private homes and hotels. Demographically the users in the use case are primarily working age, well trained for their tools and fit, however the other user group for many of the access controlled doors and pathways is the daily users of these and they come from of most demographic, geographic, educational and ability groups. Here the protection target is a mix of all the individual access control use situations mainly to places where people can be sick or injured but on the contrary the reliability, availability and usability from nursing and emergency teams point of view take main precedence in the review. Security is a key concern from the point of view that if public service personnel have possibility to access homes and building when needed how is it controlled that they only use the access where needed. Privacy is a concern as well as the use case involves nursing sick and elderly people or taking care of injured people in emergencies and as health information is sensitive personally identifiable information in many countries and regions [45, 46]

### 7.7.2 Comparison of access technologies for the use case

All six access technologies were compared against the use case parameters and grades were collected into a table. The table is visible in the below figure 10. *Traditional lock and key* while reliable, secure and suitable to protect the privacy of both the users and property owners and users, is difficult to deploy in large scale so that all needed crews would have access to the relevant keys where needed. Proper shift and key planning and enough keys for smaller teams can still be a functional solution in small scale. Small scale use could be small home nursing teams. There are implementations of building wide master-key caches to which emergency crews have access to with their own dedicated master key. As these caches are small and sometimes located also within the building, they might not be found in emergency situations fast enough. Traditional keys with long periods of no usage carry also additional risk of being lost without being recognized. Additionally, the keys would need to be having wide accesses within buildings causing the situation in case of loss that the building needs to be rekeyed. *Proximity card*-based solution offer a good suitability, but the current technical solutions and access control ownership would often limit the use of the card to a building specific setup resulting to somewhat similar problems than with traditional keys. Proximity cards allow the access management usually remotely and a lost card can be revoked if lost. Enrollment of cards can be done before hands and required number of cards can be done relatively cost effectively.

*Biometrics* solution such as fingerprint readers could be considered for public service use, but reliability and availability can be an issue as emergency crews change often and use gloves or other protective gear. All personnel would need to be enrolled physically to the biometrics system and solution would need to be centrally managed to allow different buildings to be accessible with single biometrics enrollment. In practice this can be considered to be relatively infeasible and carry privacy concerns as fingerprints are sensitive personally identifiable information in many countries and regions [45, 46].

*Smart phone app* is a reliable and technically functional solution also for single building use cases but requires the organization to issue organizational equipment supporting the access technology. Smart phone app can offer good suitability, but the current technical solutions and access control ownership could make it hard to enroll the mobile devices to all buildings as needed without taking more holistic large-scale access control into use. Smart watch and wearable ring / jewel could offer for a skilled user additional usability in practical use on daily basis but are considered to require additional user skills and further effort from both the enrollment process and use point of view. On the other hand, small and hidden rings and jewels might be unusable to emergency crews with gear on, but regularly clothed home nurses could utilize these.



Use case: Public service

| Access token type | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|
| Traditional lock and key | 1 | 3 | 2 | 1 | 1 | 2 | 2 |
| Proximity card | 2 | 3 | 3 | 2 | 3 | 2 | 2 |
| Biometrics | 1 | 1 | 1 | 2 | 2 | 2 | 3 |
| Smart phone app | 2 | 3 | 3 | 2 | 3 | 2 | 3 |
| Smart watch | 2 | 2 | 1 | 1 | 1 | 2 | 2 |
| Wearable ring / jewel | 1 | 2 | 1 | 1 | 1 | 2 | 2 |

1=Low, 2=Medium, 3=High

**Fig. 10.** Comparison chart of access technologies for 'Public service' use case

### 7.7.3 Learnings from the use case

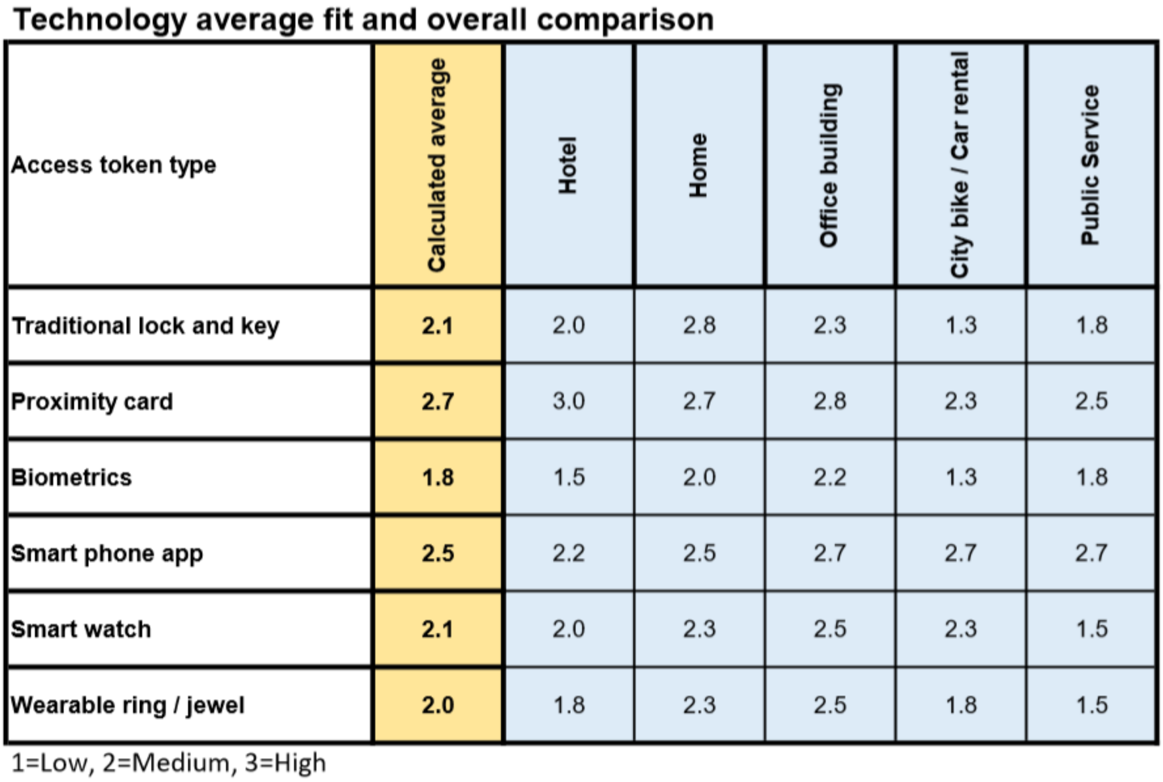
When looking at the use case table there are no major unexpected results. The traditional lock and key, biometrics and wearable rings / jewels do not seem like very potential choices for the use case. Proximity card, smart phones and smart watches might serve in the use case, but results are somewhat contradicting. There are already experiments for example in Finland where shared housing units are being equipped with smart phone app compatible access control systems enabling public services such as emergency crews and home nurses to enter the needed homes and premises with their work smart phone [58]. The public service user group is large there are specific requirements for cost, interoperability and usability. There are still hurdles in this progress as the solutions are tied to specific technology and suppliers with little or no compatibility. While most providers can support the chosen alarm or access control ecosystems they require specific connector equipment to be purchased for it – and there cannot be more than one system at once [59, 43, 58].

All wearables offer decent privacy and security in the use case. The main differences in availability, serviceability and usability side come from the additional complexity of possibly enrolling quite personal watches and rings into a work related access control system – this is a line-crossing consideration both from the employee and employer point of view that should be policed carefully from contract and legal point of view.

## 7.8 Overall learnings from the analysis use cases

All six access technologies were compared against the use cases in the previous chapters using parameters and grades. The technology specific results were composed into per technology tables and are available in Appendix 1. The average grades for each technology was calculated and were cross referenced with the use case. This table is visible in the below figure 11. *Traditional lock and key* scored well in use cases where the environment and users are more stable like home, small offices and smaller hotels and did not do well in public settings. Proximity card-based access control systems do not seem to have really any weak spots in terms of where they can be utilized based on the chart. Why the technology has not fully penetrated the whole market is a good question and might require further studies. *Biometrics* despite of its solid foundation of being tied to an individual and providing hence a very secure and authorization enforcing solutions scored rather poorly overall in the use case reviews.

*Wearables* on average scored very well, so on general note their utilization for access control use cases in the future as well are worth a consideration. The downsides that were noted was their still relatively low market penetration and challenges with certain user groups [15, 54]. From wearables the *smart phones* are clearly the most mature and more adopted solutions that are readily available from the market and outperformed the others. Even the *smaller equipment* could provide some usability benefits, they only appear to be useful as supporting device, and for various access control situations they need to be accompanied at least by a smart phone for ordering, payment and enrollment purposes.



Technology average fit and overall comparison

| Access token type | Calculated average | Hotel | Home | Office building | City bike / Car rental | Public Service |
|---|---|---|---|---|---|---|
| Traditional lock and key | 2.1 | 2.0 | 2.8 | 2.3 | 1.3 | 1.8 |
| Proximity card | 2.7 | 3.0 | 2.7 | 2.8 | 2.3 | 2.5 |
| Biometrics | 1.8 | 1.5 | 2.0 | 2.2 | 1.3 | 1.8 |
| Smart phone app | 2.5 | 2.2 | 2.5 | 2.7 | 2.7 | 2.7 |
| Smart watch | 2.1 | 2.0 | 2.3 | 2.5 | 2.3 | 1.5 |
| Wearable ring / jewel | 2.0 | 1.8 | 2.3 | 2.5 | 1.8 | 1.5 |

1=Low, 2=Medium, 3=High

**Fig. 11.** Comparison chart of access technologies for 'Hotel' use case

Finally, enrolling quite personal watches and rings into a work related or potentially insecure access control system require user and organizational education and policing from contractual and legal point of view.

## 7.9 Current market situation for wearables use in access control

Innovations, technological advancement and consumer electronics cheaper prices have started to open electronic access control markets also to consumer and everyday use cases. When looking at the available products and offerings the standardization work is quite immature especially considering more complex use cases of utilizing either the access control or related tokens across in different use cases. Some technologies are less cross-compatible and lack backwards compatibility or might be just for marketing purposes locked down to the vendor specific technology stack [59, 43, 13]. Consumer techniques that are more open to cross integration are starting to emerge, for example the widely used Apple ecosystem provides support via its Apple HomeKit developer toolkit [14, 43]. There have been early indication however that the emerging technology vendors have brought into the market either technologically immature or outright insecure solutions [16]. There is even a separate OWASP project for IoT security providing awareness as well as design and implementation pre-requisites for IoT devices and systems [44]. Some countries have started to even provide regulation or certifications for information secure devices. For example in United States State of California has issued specific regulation for connected devices and Finnish regulators are offering certification for devices meeting defined security criteria [60, 61].

Early adopters will likely face the need to swap in multiple occasions their chosen technologies to keep up with the development and in order to maintain secure solutions. While there are already available experiences in some projects [58] about larger scale access control systems able to function with single set of keys and support multiple different user groups, it is unlikely that key chains will converge into a single set of keys used everywhere. The main counteracting forces are that in large scale there will be incompatible legacy technology, users' adoption rate for skills and process, availability of supported technology from user side and the still very clear lack of unified technology stacks from vendors side.

# 8 CONCLUSIONS

This research studied the combinability of electronic access control and wearable technology in the context of risk management, asset protection and access control generally. The concepts were introduced first separately to create a picture into the domain of access control and wearable technology. These were then studied together using selected use cases.

Research question “Where does wearable technology bring additional benefits to the electronic access control use cases?” was discussed in the context of five different use cases and the benefits are becoming visible in the ongoing early projects utilizing wearable technology such as the home nursing access project in city of Lahti, Finland. The key benefits supplement the traditional electronic access control by adding additional functionality to coexist with the mere access such as combining access and work tracking or access and rental bike payment process. Wearables and other advanced electronic access control solutions could also alleviate the key and keycard management burden for some users who work in environments currently with scattered key management such as emergency, health care, cleaning, logistics, and security services. There is indication that for example smart phone-based access control solutions might be well suited to address this problem.

The second research question “What are the most typical new risks that using wearable technology introduces to traditional access control use cases?” was discussed together with the use cases and in addition in chapters 6.5, 6.6 and 7.8. The clear risks that were identified were related to choosing incompatible technologies causing monetary losses, immature emerging technology technical issues and security issues. There are also legal and misuse risks in using some of the solutions such as private equipment in another context. Using private equipment could in some cases could expose user content on the device to the access control provider acting maliciously. Another legal risk resides in projects where inadequate considerations is put for example to privacy issues, access control system logs can easily form up a private information register that is under special regulation. Privacy violations like that are likely to result into fines and other legal consequences. Finally, the Internet of things overall exposes equipment overall to the threats of internet and bad actors well beyond current exposure level of current access control systems.

The last research question “What considerations should be taken when using wearable technology in electronic access control use cases?” was discussed together with the use cases and in addition in chapters 6.5, 6.6 and 7.8. The key point is on spending the effort on ensuring technology selection total cost of ownership while making financial decisions and looking beyond marketing promises. Consideration for the legal topics in general when building shared access control solutions and especially privacy implications for use cases mixing private equipment to shared use cases.

## 8.1 Further studies and future of wearables as part of access control

Further studies and pilot projects building larger scale shared access control systems could be beneficial to allow better support for public servants like home nursing and emergency crews to access buildings easier and more efficiently than with traditional solutions for the benefit of their patients. IoT overall is just emerging and security researchers are predicting early IoT implementations to be a longer time concern as they become deeply intwined in the everyday lives making them hard to be fixed or replaced due to complex automation and integration setup. It could be worth hence building further standardization for the IoT devices with key consideration to the serviceability and replaceability throughout the access control solution life cycle.

Utilization of biometrics, artificial intelligence (AI), machine learning (ML) and user behavioral alarm and access systems could lower the need for access tokens or remove their need all together. Privacy concerns could make it quite hard to implement properly in environments that have very strict requirements / limitations use of biometrics/cameras – for example swimming pool lockers in dressing rooms are ill suited for camera-based access control. On the other hand, the wearables even if they would become unnecessary for the access control in principle, wearable sensors could still potentially enhance the dynamic access systems by providing more context to the mere video feed. For example a person carrying heart rate sensor could provide the heart rate to the access control system for more accurate identification and / or providing additional context, for example an elevated heart rate could indicate a distress of a person being coerced to provide access to intruders.

Additional ideas that were considered by the author as potential further analysis:

- wearable technology could be used also for requesting accesses on ad-hoc basis to areas where the access has not been previously granted
- wearables could be used to give route guidance within the building while the user passes near the access control points
- wearable technology could be used to see and the access logs, providing useful insight for a security guard doing his/her rounds
- wearable technology could be used to not just be polled about being present on a authentication point – it could also be used as part of the authentication chain (heartbeat sensor, facial recognition, fingerprint, voice recognition) leaving the actual access control devices plain and simple and putting more logic side to the equipment on the users themselves

# REFERENCES

1. H. Kortelainen, A. Happonen and S.-K. Kinnunen, "Fleet service generation—challenges in corporate asset management," *Lecture Notes in Mechanical Engineering,* vol. 4, pp. 373-380, 2016.
2. H. Kortelainen, A. Happonen and J. Hanski, "From asset provider to knowledge company—Transformation in the digital era," *Lecture Notes in Mechanical Engineering,* pp. 333-341, 2019.
3. A. Q. Stefania, H. M. Glauco, H. S. Jorge, M. G. Gilberto, A. C. M. Paulo and G. O. Maicon, "Servitization and performance: impacts on small and medium enterprises," *Journal of Business & Industrial Marketing,* vol. 35, no. 7, pp. 1237-1249, 2020.
4. G. Allen and R. Derr, Threat Assessment and Risk Analysis - An Applied Approach, Waltham: Elsevier, Butterworth-Heineman, 2016.
5. A. J. Dorofee, J. A. Walker, C. J. Alberts, R. P. Higuera, R. L. Murphy and R. C. Williams, Continuous Risk Management Guidebook, Pittsburgh: Carnegie Mellon University, 1996.
6. T. L. Norman, Electronic Access Control, Waltham, MA: Elsevier, Butterworth-Heinemann, 2012.
7. T. A. Ricks, B. E. Ricks and J. Dingle, *Physical security and safety: A Field Guide for the Practitioner,* Boca Raton: CRC Press, 2015.
8. K. Hartman, *Make: Wearable Electronics,* Maker Media Inc, 2014.
9. E. Sazonov, *Wearable Sensors,* San Diego: Academic Press, 2014.
10. G. Fortino, R. Gravina and S. Galzarano, *Wearable Computing,* Hoboken: John Wiley & Sons, 2018.
11. O. Nykänen, Toimivaa tekstiä - Opas tekniikasta kirjoittaville, Helsinki: Tekniikan Akateemisten Liitto TEK, 2002.
12. J. Lindström, "Security challenges for wearable computing," in *Proceedings / IFAWC : 4th International Forum on applied Wearable Computing 2007,* Tel Aviv, 2007.
13. P. Dzurenda, J. Hajny, V. Zeman and K. Vrba, "Modern physical access control systems and privacy protection," in *2015 38th International Conference on Telecommunications and Signal Processing (TSP),* Prague, 2015.
14. Apple Inc, "HomeKit," 2020. [Online]. Available: https://developer.apple.com/homekit/. [Accessed 1 July 2020].
15. Ericsson Consumer Lab, "Wearable technology and the IoT," June 2016. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/consumerlab/reports/wearable-technology-and-the-internet-of-things. [Accessed 24 June 2020].
16. A. Gilchrist, IoT Security Issues, Boston: Walter de Gruyter Inc, 2017.
17. T. Cheshire, "Chameleon clothing adapts to its environment," 6 February 2014. [Online]. Available: http://www.wired.co.uk/magazine/archive/2014/03/start/chameleon-clothing. [Accessed 22 May 2014].

18. Cisco, "Internet of Everything: The Connected Home," *Wired UK,* pp. 57-61, Mar 2014.

19. J. Medeiros, D. Russell and Hammersley, "What to Wear," *Wired UK,* pp. 117-132, Jan 2014.

20. T. Cheshire, "This NFC ring will be the key to your house," *Wired UK,* p. 28, Feb 2014.

21. Gartner Inc, "Technology Research | Gartner Inc.," 2014. [Online]. Available: http://www.gartner.com/technology/home.jsp. [Accessed 21 May 2014].

22. D. W. Cearley, "The Top 10 Technology Trends for 2012," 16 February 2012. [Online]. Available: https://www.gartner.com/doc/1926316?ref=SiteSearch&sthkw=wearable&fnl=search&srcId=1-3478922254. [Accessed 22 May 2014].

23. A. Velosa, "Internet of Things and Wearables: The Battleground," 3 December 2013. [Online]. Available: http://my.gartner.com/portal/server.pt?open=512&objID=202&mode=2&PageID=5553&showOriginalFeature=y&resId=2624618&fnl=search&srcId=1-3478922244. [Accessed 22 May 2014].

24. P. Lee, D. Stewart and C. Calugar-Pop, "Deloitte. Technology, Media and Telecommunications Predictions 2014," 2014. [Online]. Available: http://www.deloitte.com/assets/Dcom-Iceland/Local%20Assets/Documents/TMT%20Predictions%202014.pdf. [Accessed 25 May 2014].

25. D. Melanson, "Gaming the system: Edward Thorp and the wearable computer that beat Vegas," 18 September 2013. [Online]. Available: http://www.engadget.com/2013/09/18/edward-thorp-father-of-wearable-computing/. [Accessed 21 May 2014].

26. The Human Dynamics Lab at the MIT Media Laboratories, "Wearable Computing at the MIT Media Lab," MIT, 2014. [Online]. Available: http://www.media.mit.edu/wearables/. [Accessed 21 May 2014].

27. P. Ritsos, "Remus Wearable Computer on Behance," 2000. [Online]. Available: http://www.behance.net/gallery/Remus-Wearable-Computer/3609645. [Accessed 21 May 2014].

28. Eurotech, "Zypad WL1500 : Latest generation wrist-wearable computer Eurotech," 2014. [Online]. Available: http://www.eurotech.com/en/products/Zypad%20WL1500. [Accessed 21 May 2014].

29. Samsung, "Samsung Gear Fit," 2014. [Online]. Available: http://www.samsung.com/uk/consumer/mobile-devices/galaxy-gear/galaxy-gear/SM-R3500ZKABTU. [Accessed 21 May 2014].

30. Automation World, "Automation World 2019 edition," 2019. [Online]. Available: https://pmg-designer.s3.amazonaws.com/FreeDownloads/AW/AW-ConnectedTechnologiesImpactingIndustryToday2019.pdf?utm_source=Newsletters&utm_medium=PMG+Marketing&utm_term=20200626. [Accessed 1 July 2020].

31. McLear Ltd, "NFC Ring," 2020. [Online]. Available: https://store.nfcring.com/collections/all. [Accessed 1 July 2020].

32. Apple Inc, "The #1 smartwatch in the world. Times two.," 2020. [Online]. Available: https://www.apple.com/watch/. [Accessed 1 July 2020].

33. CES Consumer Technology Association, "Wearable Technology Summit 2020," January 2020. [Online]. Available: https://wearabletechnologysummit.com/. [Accessed 1 July 2020].

34. Glogger, "File:Wearcompevolution.jpg," 1 August 2004. [Online]. Available: https://commons.wikimedia.org/wiki/File:Wearcompevolution.jpg. [Accessed 21 June 2020].

35. energepic.com, "File:Smart watch.jpg," 13 June 2016. [Online]. Available: https://commons.wikimedia.org/wiki/File:Smart_watch.jpg. [Accessed 21 June 2020].

36. I. F. Press, "File:CardioMEMS wireless sensor with quarter.png," 29 August 2013. [Online]. Available: https://commons.wikimedia.org/wiki/File:CardioMEMS_wireless_sensor_with_quarter.png. [Accessed 21 June 2020].

37. S. Kaplan, "The Words of Risk Analysis," *Risk Analysis,* vol. 17, no. 4, pp. 407-417, 1997.

38. R. Hovinen, V. Kauppi, M. Leskinen, A. Vuorinen and V. Vironen, Kulunvalvonta- ja rikosilmoitinjärjestelmät, Tampere: Sähkötieto ry, 2007.

39. G. E. Rejda and M. J. McNamara, Principles of Risk Management and Insurance, Hagerstown: Pearson Education, 2014.

40. J. Konicek and K. Little, Security, ID Systems and Locks, Burlington: Elsevier, Butterworth-Heineman, 2009.

41. Axis Communications, "AXIS Fence Guard for Intrusion Detection," 2020. [Online]. Available: https://www.axis.com/en-fi/products/axis-fence-guard. [Accessed 1 July 2020].

42. Finnpark, "Finnpark pysäköintijärjestelmät," 2020. [Online]. Available: https://www.finnpark.fi/pysaekoeintijaerjestelmaet/referenssit#c73. [Accessed 1 July 2020].

43. PC Magazine, "The Best Smart Locks for 2020," 9 April 2020. [Online]. Available: https://uk.pcmag.com/smart-locks/77460/the-best-smart-locks. [Accessed 1 July 2020].

44. OWASP, "OWASP Internet of Things," 2020. [Online]. Available: https://owasp.org/www-project-internet-of-things/. [Accessed 1 July 2020].

45. European Union, "Document 02016R0679-20160504," 27 April 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504. [Accessed 7 July 2020].

46. United States State of California, "AB-375 Privacy: personal information: businesses.," 28 June 2018. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. [Accessed 7 July 2020].

47. D. Weinbach, "Mobile Devices Integral to Access Control," *Security Technology Executive,* vol. 2017, no. 1, pp. 38-40, February 2017.

48. P. Meharia and D. P. Agrawal, "The Human Key: Identification and Authentication in Wearable Devices Using Gait," *Journal of Information Privacy and Security*, vol. 2015, no. 11, pp. 80-96, 2015.

49. M. Mueller, L. C. Alves, W. Fischer, M. L. Fair and I. Modi, "RAS Strategy for IBM S/390 G5 and G6," *IBM Journal of Research and Development,* vol. 43, no. 5, pp. 875-888, 1999.

50. J. Lindström and C. Hanken, "Wearable Computing: Security Challenges, BYOD, Privacy, and Legal Aspects," in *Analyzing Security, Trust, and Crime in the Digital World*, 1 ed., Hershey, Information Science Reference, 2014, pp. 96-120.

51. M. L. Garcia , The design and evaluation of physical protection systems, 2nd ed., Burlington: Butterworth-Heineman, 2008.

52. British Security Industry Association, "A specifier's guide to access control systems," April 2016. [Online]. Available: https://www.bsia.co.uk/bsia-front/pdfs/132-specifiers-guide-access-control-systems[1].pdf. [Accessed 27 June 2020].

53. Crisco 1492, "File:Tumbler key lock explained in four steps.png," 29 September 2013. [Online]. Available: https://commons.wikimedia.org/wiki/File:Tumbler_key_lock_explained_in_four_steps.png. [Accessed 30 06 2020].

54. Statistics Finland, "Väestön tieto- ja viestintätekniikan käyttö," November 2019. [Online]. Available: http://www.stat.fi/til/sutivi/index.html. [Accessed 24 June 2020].

55. G. Smith, J. Sochor and M. Karlsson, "Mobility as a Service: Development scenarios and implications for public transport," *Research in Transportation Economics,* vol. 69, pp. 592-599, 2018.

56. C. Mulley, J. D. Nelson and S. Wright, "Community transport meets mobility as a service: On the road to a new a flexible future," *Research in Transportation Economics*, vol. 69, pp. 583-591, 2018.

57. H. Song, R. Srinivasan, T. Sookoor and S. Jeschke, Smart Cities: Foundations, Principles and Applications, Hoboken: John Wiley & Sons Inc, 2017.

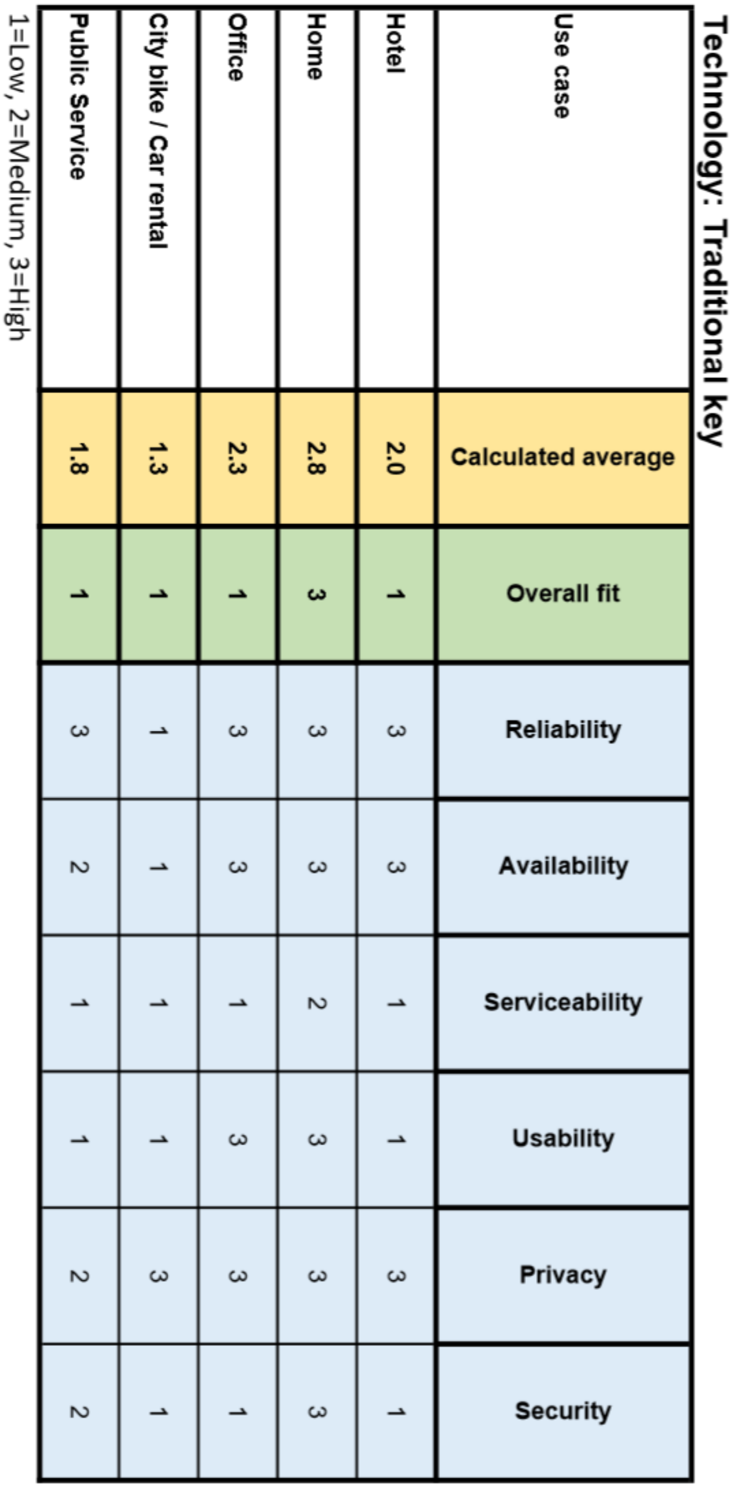
58. Lukoton Experience Oy, "Lukoton ratkaisut kotihoidolle," 2020. [Online]. Available: https://www.lukoton.com/index.php/kotihoito/. [Accessed 1 July 2020].

59. Verisure, "Älylukko - Valvo kotisi lukitusta helposti ja turvallisesti," 2020. [Online]. Available: https://www.verisure.fi/alykoti/alylukko.html. [Accessed 01 July 2020].

60. Government of Finland - Traficom, "Tietoturvamerkki," 2020. [Online]. Available: https://tietoturvamerkki.fi/. [Accessed 1 July 2020].

61. United States State of California, "SB-327 Information privacy: connected devices.," 28 September 2018. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327. [Accessed 1 July 2020].

# APPENDIX 1. Collection of tables of use case results per technology



Technology: Traditional key

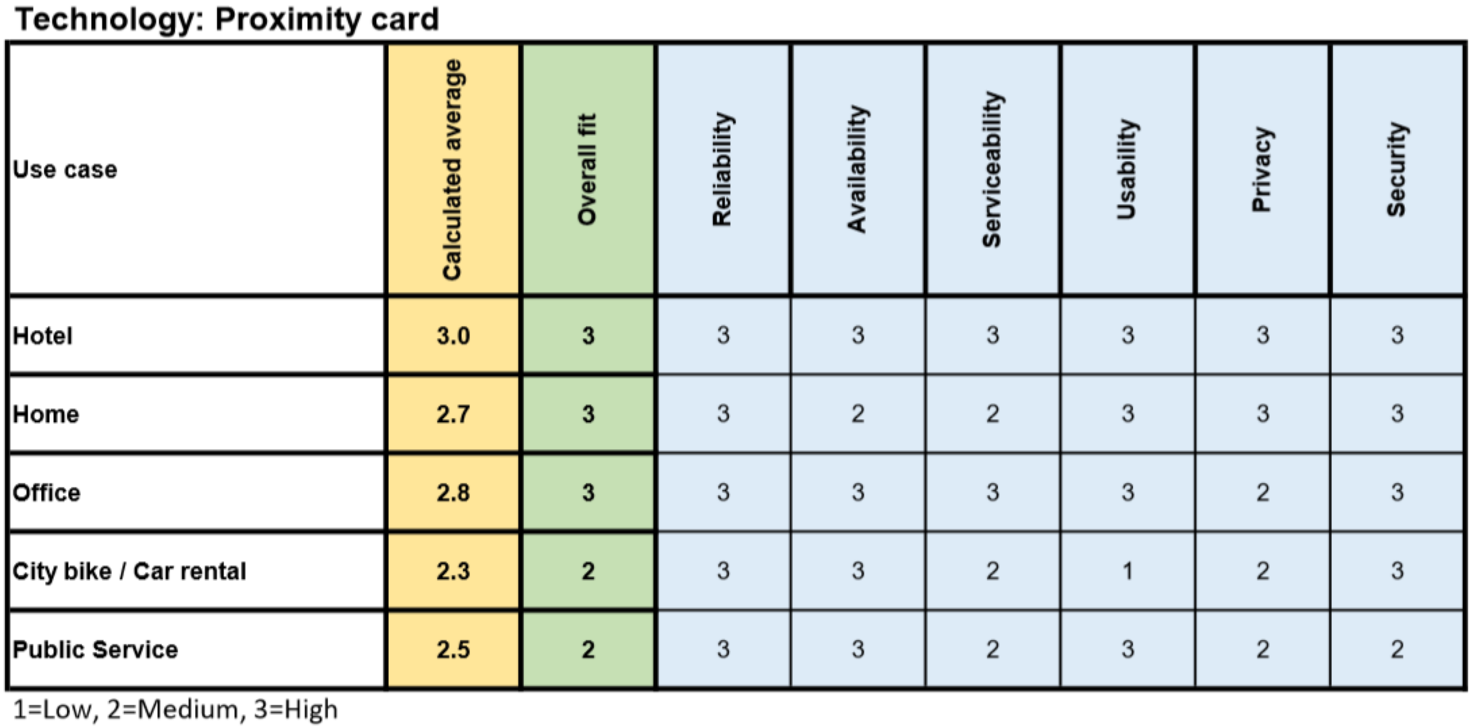
| Use case | Calculated average | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|---|
| Hotel | 2.0 | 1 | 3 | 3 | 1 | 1 | 3 | 1 |
| Home | 2.8 | 3 | 3 | 3 | 2 | 3 | 3 | 3 |
| Office | 2.3 | 1 | 3 | 3 | 1 | 3 | 3 | 1 |
| City bike / Car rental | 1.3 | 1 | 1 | 1 | 1 | 1 | 3 | 1 |
| Public Service | 1.8 | 1 | 3 | 2 | 1 | 1 | 2 | 2 |

1=Low, 2=Medium, 3=High

**Fig. 12.** Comparison chart of ‘Traditional lock and key’ access control technology suitability scoring against different access control use cases

(continues)

## APPENDIX 1. (continues)



Technology: Proximity card

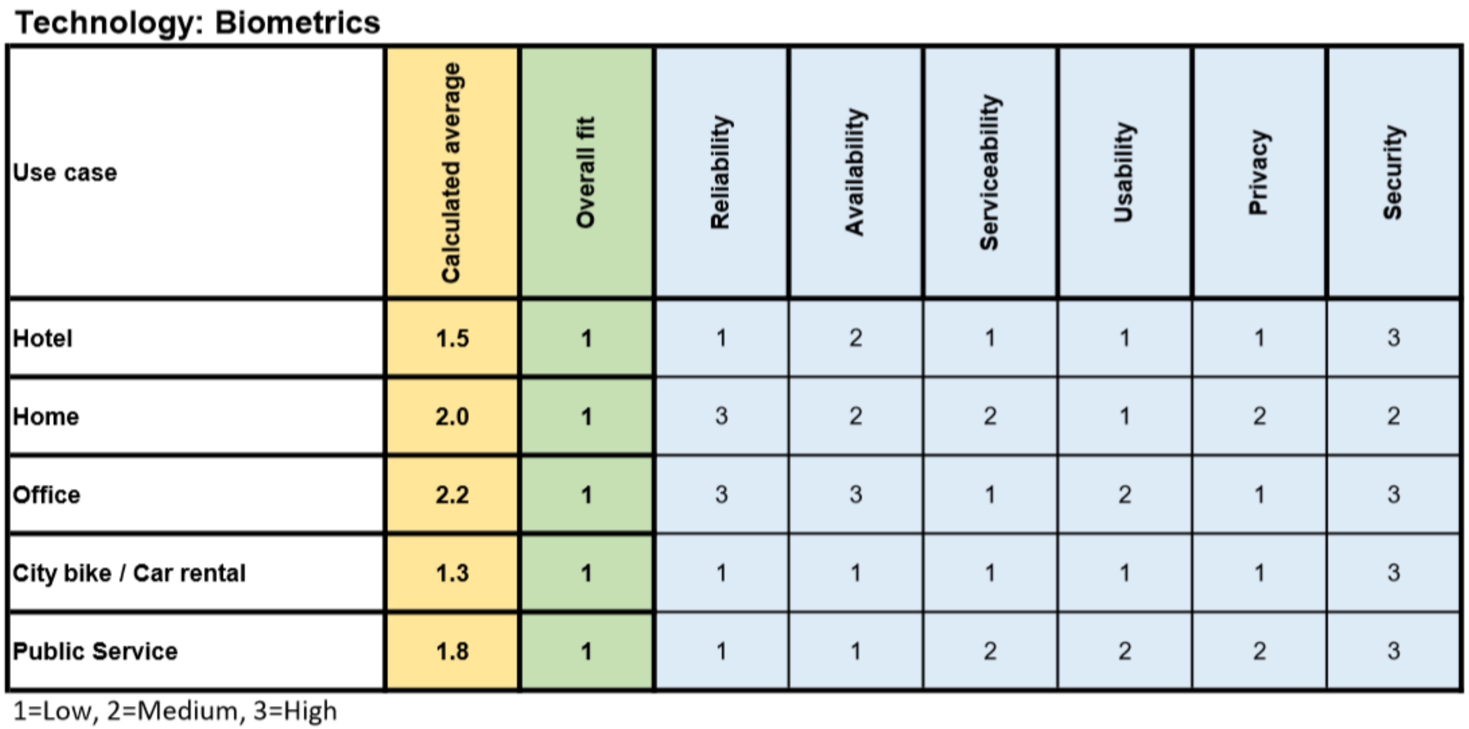
| Use case | Calculated average | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|---|
| Hotel | 3.0 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| Home | 2.7 | 3 | 3 | 2 | 2 | 3 | 3 | 3 |
| Office | 2.8 | 3 | 3 | 3 | 3 | 3 | 2 | 3 |
| City bike / Car rental | 2.3 | 2 | 3 | 3 | 2 | 1 | 2 | 3 |
| Public Service | 2.5 | 2 | 3 | 3 | 2 | 3 | 2 | 2 |

1=Low, 2=Medium, 3=High

**Fig. 13.** Comparison chart of ‘Proximity card’ access control technology suitability scoring against different access control use cases

(continues)

## APPENDIX 1. (continues)



Technology: Biometrics

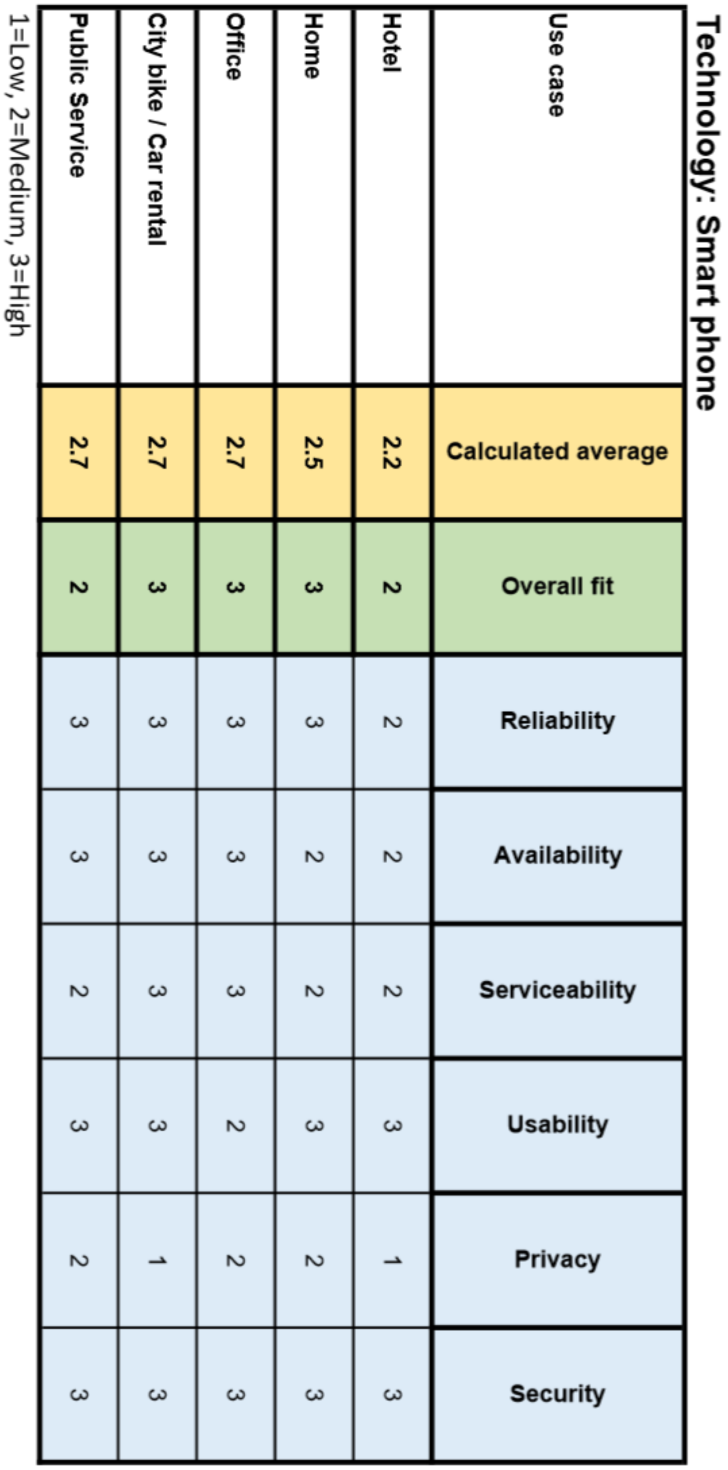
| Use case | Calculated average | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|---|
| Hotel | 1.5 | 1 | 1 | 2 | 1 | 1 | 1 | 3 |
| Home | 2.0 | 1 | 3 | 2 | 2 | 1 | 2 | 2 |
| Office | 2.2 | 1 | 3 | 3 | 1 | 2 | 1 | 3 |
| City bike / Car rental | 1.3 | 1 | 1 | 1 | 1 | 1 | 1 | 3 |
| Public Service | 1.8 | 1 | 1 | 1 | 2 | 2 | 2 | 3 |

1=Low, 2=Medium, 3=High

**Fig. 14.** Comparison chart of ‘Biometrics’ access control technology suitability scoring against different access control use cases

(continues)

## APPENDIX 1. (continues)



Technology: Smart phone

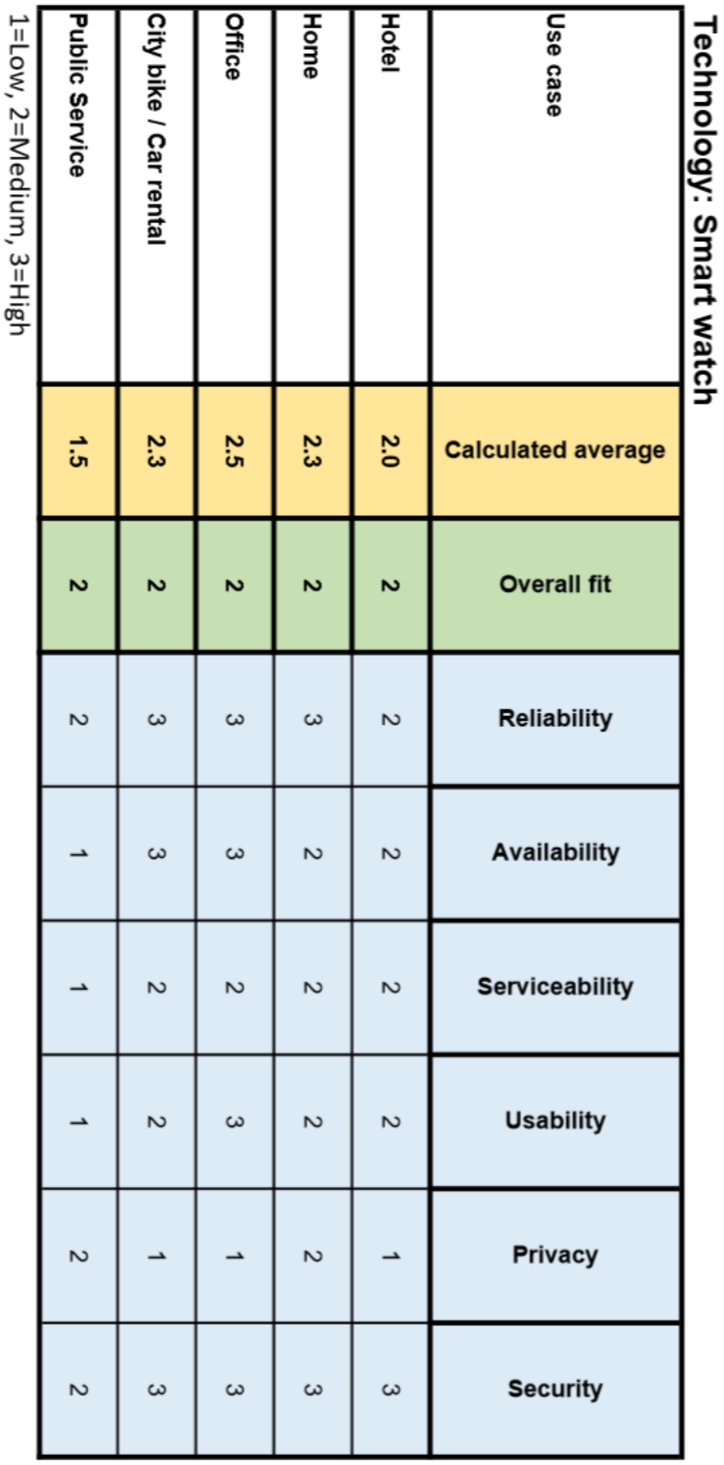
| Use case | Calculated average | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|---|
| Hotel | 2.2 | 2 | 2 | 2 | 2 | 3 | 1 | 3 |
| Home | 2.5 | 3 | 3 | 2 | 2 | 3 | 2 | 3 |
| Office | 2.7 | 3 | 3 | 3 | 3 | 2 | 2 | 3 |
| City bike / Car rental | 2.7 | 3 | 3 | 3 | 3 | 3 | 1 | 3 |
| Public Service | 2.7 | 2 | 3 | 3 | 2 | 3 | 2 | 3 |

1=Low, 2=Medium, 3=High

**Fig. 15.** Comparison chart of ‘Smart phone app’ access control technology suitability scoring against different access control use cases

(continues)

## APPENDIX 1. (continues)



Technology: Smart watch

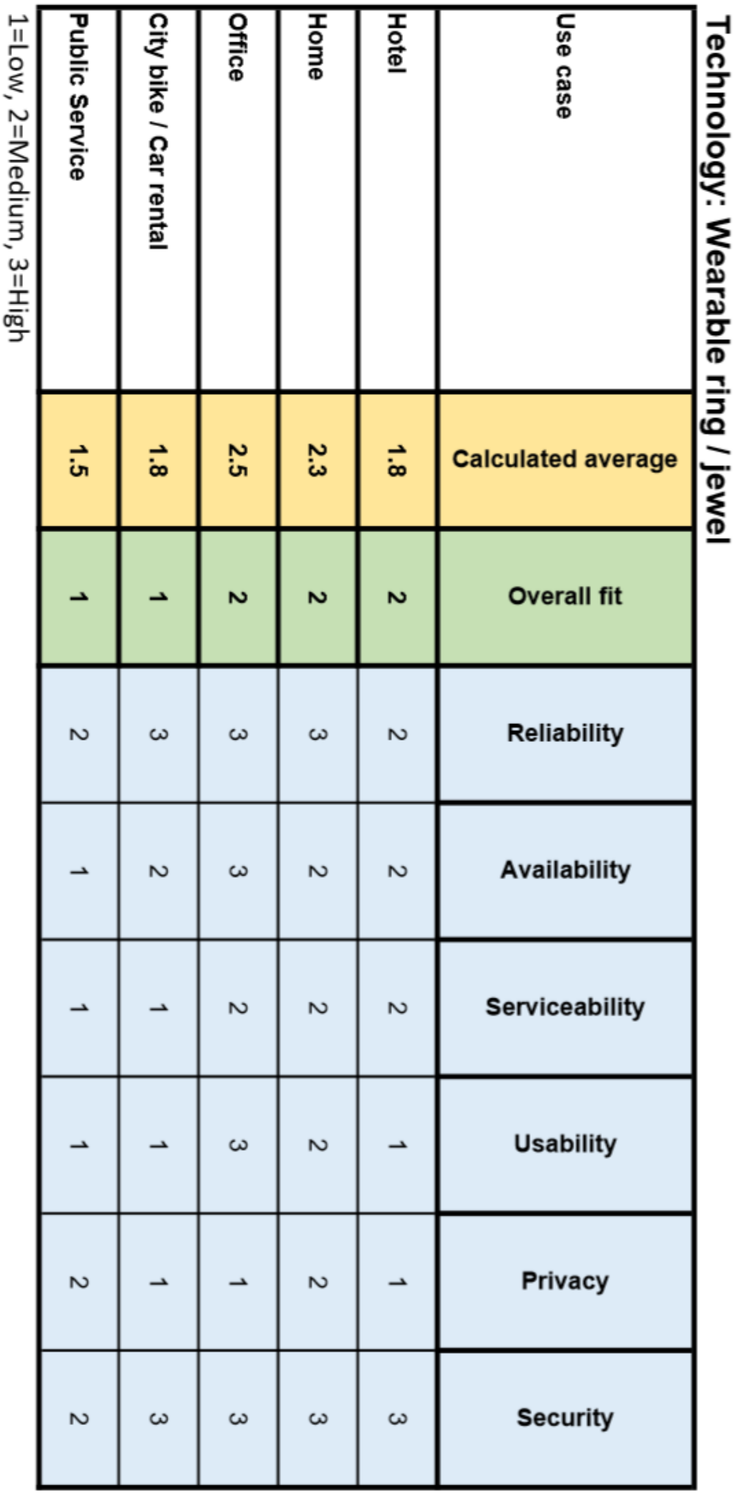
| Use case | Calculated average | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|---|
| Hotel | 2.0 | 2 | 2 | 2 | 2 | 2 | 1 | 3 |
| Home | 2.3 | 2 | 3 | 2 | 2 | 2 | 2 | 3 |
| Office | 2.5 | 2 | 3 | 3 | 2 | 3 | 1 | 3 |
| City bike / Car rental | 2.3 | 2 | 3 | 3 | 2 | 2 | 1 | 3 |
| Public Service | 1.5 | 2 | 2 | 1 | 1 | 1 | 2 | 2 |

1=Low, 2=Medium, 3=High

**Fig. 16.** Comparison chart of ‘Smart watch’ access control technology suitability scoring against different access control use cases

(continues)

## APPENDIX 1. (continues)



Technology: Wearable ring / jewel

| Use case | Calculated average | Overall fit | Reliability | Availability | Serviceability | Usability | Privacy | Security |
|---|---|---|---|---|---|---|---|---|
| Hotel | 1.8 | 2 | 2 | 2 | 2 | 1 | 1 | 3 |
| Home | 2.3 | 2 | 3 | 2 | 2 | 2 | 2 | 3 |
| Office | 2.5 | 2 | 3 | 3 | 2 | 3 | 1 | 3 |
| City bike / Car rental | 1.8 | 1 | 3 | 2 | 1 | 1 | 1 | 3 |
| Public Service | 1.5 | 1 | 2 | 1 | 1 | 1 | 2 | 2 |

1=Low, 2=Medium, 3=High

**Fig. 17.** Comparison chart of ‘Wearable ring / jewel’ access control technology suitability scoring against different access control use cases