A Requirements Based Selection Model for Future Proof Non-Intrusive Authentication Technologies in the Office

Master Thesis Business Information Technology

Faculty of Electrical Engineering, Mathematics and Computer Science

University of Twente, Enschede

September 2021

Author:	C.G.J. Putman
Student Number:	S1596179
First Supervisor:	Dr.ir. J.M Moonen
Second Supervisor:	Dr.ir. M.J. van Sinderen
External Supervisor:	D. Nijkamp MSc.

Abstract

This research focuses on the future of authentication methods for use in and around the smart office building. A focus is put on authentication methods which are as non-intrusive as possible. That is, have the least impact on the daily operations of an office user. Firstly, this context of the smart office is explored and elaborated upon to determine a research gap between the context and research topic: authentication systems. Once the context is clear, it aims to chart the available and conceptual authentication technologies which are used or may be used in the sector. Continuing, the possible additional requirements of the stakeholders in and around the office which may have arisen due to the coronavirus pandemic are elaborated upon. The question if modern authentication technologies can fulfil some of these requirements is answered. Based on the insights gathered from these topics, a weighted criteria driven selection model for authentication systems is developed. Besides this, a critical look is taken at the lifecycle of modern technologies. These insights are consequently translated to the field of authentication systems, to see how this lifecycle can potentially be redesigned by incorporating best-practices. The end goal of this is to ensure optimal user comfort while also preserving maintainability and extend the lifespan of these systems. Insights about these mentioned topics are gathered by means of a mixed-method approach, combining knowledge from literature with information gathered from semi-structured interviews with experts from the field. The final developed model is evaluated through additional consultation with these experts. It is found that in research revolving around the office of the future or smart offices, only little attention is paid to authentication or access control. This while it is likely that this will only become more important due to personalization around the workplace by means of smart office technologies such as environmental control, smart desks and meeting management systems. It is found that a multitude of solutions are already available, and additional conceptual solutions are in development. These solutions may contribute towards achieving the goals of stakeholders of office use. Solutions may be combined to increase security, create a solution which is experienced as being as least intrusive as possible and contribute to fulfilling many stakeholder requirements. Through evaluation it was found that the model was deemed to be correct and effective, although the final product could benefit from an improved user experience. The selected system(s) should consequently be installed by taking into account open hardware architecture principles and by connecting applications to each other through the use of APIs and middleware software to ensure maintainability and longevity.

Table of Contents

List of Used Abbreviations

In this research, some abbreviations are used which might feel unfamiliar to the reader not familiar with the topic. These abbreviations with their meaning are (in alphabetical order) as follows:

2FA	Two-Factor Authentication
AI	Artificial Intelligence
API	Application Programming Interface
BMS	Building Management System
BVP	Blood Volume Pulse
COVID-19	Coronavirus Disease 2019
ECG	Electrocardiogram
EEG	Electroencephalography
GPS	Global Positioning System
HVAC	Heating Ventilation and Airconditioning
IB	Intelligent Building
ICT	Information and Communications Technology
IoT	Internet of Things
IPS	Indoor Positioning System
IT	Information Technology
KPI	Key Performance Index
MFA	Multi-Factor Authentication
NFC	Near Field Communication
PACS	Physical Access Control Systems
QEM	Quality Environment Modules
QR	Quick Response
RFID	Radio-Frequency Identification

1. **Introduction**

Intelligent building technologies have been around for decades. The definition of what comprises an intelligent building, however, has been under constant development. This is primarily due to the significant technological developments the world has gone through over the past couple of decades. While one would not directly link the emergence of new high tech innovative solutions to the real estate sector, and quite rightly so, they are certainly there and have had quite some impact on the sector as well (Deloitte Canada, 2015; Barry & Feucht, 2020). Recent technical developments relating to the Internet of things (IoT), big data and artificial intelligence (AI) have created new opportunities in this field which deserve to be explored and utilized.

While technologies have changed, the way the office is being used has changed as well. This is not the least sparked by the ongoing coronavirus pandemic. As of writing, offices are hardly used at all, and employees are encouraged to work from home in expectation of better days to come. What the exact consequences of the pandemic will be on the long term is still to be seen. However, companies are already expecting and preparing for changes in the workplace. These changes mainly relate to the frequency and motivation of office visits by employees. Expectations are that the future of the office will revolve around being a meeting spot instead of a place to perform day to day tasks (ApolloTechnical, 2020). A brief inquiry around the largest employers in the Netherlands showed that a significant number of organizations are expecting to be using less real estate in the future than they would need before the pandemic (Nieuwsuur, 2021). However, a similar number of employees and clients will be visiting this smaller surface of real estate. This results in offices, meeting rooms, desks, parking spots and many more things to be shared with co-workers, flex workers, and third party business relations instead of private individual use. Furthermore, office buildings might shift from single tenant to multi-tenant use, whereas previously these would have been reserved for workers of an individual organization.

As a consequence, this raises new challenges in how to manage that all these different people can work the way they want to and without too much administrative hassle involved before they can start their daily desk work or important business meeting. Furthermore, attention should be paid to making sure that a workspace still feels personal while being shared with co-workers. Customizability of workspaces based on personal preferences and one's schedule is key, and tools are available to achieve this (Future Workplace, 2019). However, personal preferences should remain personal and therefore require to be securely stored and accessed. Modern authentication systems which are intertwined with physical access control systems can play a significant role in this. However, authentication should never be a major task which influences one's day at the office. It should be virtually invisible and easy to use. This is what in this research is referred to as "non-intrusive".

Topics relating to this include, but are not limited to, meeting management platforms, physical and digital authentication and indoor positioning systems (IPS) (Kvistö, 2020;

Mørch, 2019). While many off the shelve solutions are available, they are certainly not one size fits all. This raises another question: how should these solutions be catered to different users and stakeholders? A solution adequate for a service employee, such as an interior cleaner, is unlikely to fit the needs of a client visiting for a business appointment. Some stakeholders have the ability to plan multiple days ahead, while others need to be able to have their needs to be fulfilled on an ad-hoc basis.

Lastly, an interesting topic of discussion connecting to this, that has been sparked only quite recently, relates to how one can create a maintainable life cycle for intelligent building technologies. In the case of this research, this does not revolve around the standard definition of sustainability. While maintainability and sustainability always has been an important goal when applying smart building technologies, this mainly revolved around making the building itself sustainable, or in other words: good for the environment (e.g. energy reduction, So et al. (1999)). Technologies age and need replacement, much faster than buildings need replacement (Memoori, 2019). After a certain time, the technical lifespan of a product has been reached. It is worn out or can no longer perform the desired tasks. For a single dimensional product, such as for example a drill, this is easily determined and resolved. However, smart building technologies are multi-layered products combining hardware with multiple layers of interdependent software to create the optimal user experience. While software might be updated frequently, hardware is often more difficult to replace when it is embedded in a building. Both need to be in par to create the optimal technical and economical lifespan. This brings the requirement to take a critical look at the lifecycle of smart building technology and implement it correctly, or adjust it where needed. Incorporating technologies which are maintainable in itself, that is products and its supporting services which have longevity and can be used, maintained, upgraded and overall remain smart for their entire lifetime have only recently seen increased attention. This requires open standards, inter-connectivity options and long-term commitment of the smart services providers (RS2 Technologies, 2008). How this can be supported and implemented in a way that is efficient and effective for both buyer and seller is something that can no longer be ignored when bringing a product on the market. Therefore, finding out how hardware and software should be aligned to achieve a long-lasting upgradeable and maintainable product is a topic that deserves to be looked into on a deeper level for this research as well.

2. Research Design

In the previous introduction section, the general context and direction of this research has been laid out. Now that this is clear, the more detailed research outline can be presented. What follows is the research problem, research goal and consequently the research questions which contribute towards solving this problem and achieving the goal. A research approach fitting to the various research question is chosen and elaborated upon.

2.1 Research Questions

The purpose of this research is to determine the change of needs of stakeholders revolving around commercial real estate, or to be more precise, office buildings in a modern era. Extra attention is paid to addressing the changing needs after the expected consequences of the coronavirus pandemic. This research tries to find out if and how these stakeholder needs can be (partially fulfilled) by incorporating non-intrusive authentication systems within a building. A conceptual model for the selection of a suitable system based on requirements of these stakeholders will be designed, taking into account the readily available and conceptual authentication methods that are described in popular and academic literature. The model will consequently be validated by means of interviews with experts in the field. Lastly, the additional dimension of maintainability and sustainability, or more precisely the product life cycle, will be addressed as well. Therefore, to serve this purpose, the following main research question is formulated:

"How and which non-intrusive authentication systems can best be applied in office buildings to increase the comfort of its users, while ensuring these authentication systems remain maintainable?"

To support this main research question, it has been broken down into multiple smaller research questions. This is done to make the entire process more manageable. These sub questions help to create a body of knowledge as well as directly contribute to the design of a conceptual model for the selection of non-intrusive personal authentication systems around the workplace. For this entire design process, a total number of six sub research questions have been formulated.

The problem context in which this project is defined is the office, or taken a bit broader, the workplace or commercial real estate. For this project no new technologies are created, but existing technologies are instead used and combined to create innovative new concepts. It is therefore necessary to know which technologies are already available for use in practice in this context. This defines the first sub question:

> **SQ1:** "Which technologies are available to support non-intrusive authentication systems in the office of the future?"

To check to what extent these discovered existing technologies are capable of fulfilling the needs of the users or stakeholders involved in the use of office buildings, these first have to be determined. Possible gaps which cannot yet be fulfilled have to be addressed through this new concept design. This research question makes use of a mixed-method approach, combining insights from literature with insights from experts through conducting interviews:

> **SQ2:** “What are the main stakeholders that make use of commercial real estate and are involved in using this technology, and what are their requirements?”

An event which as of writing is still having a disruptive effect on the world is the Coronavirus pandemic of 2020 and 2021. Working habits and use of office buildings have significantly changed during the course of this pandemic. This has changed the way people look at office buildings and how they are used; requirements have changed and additional requirements have emerged. It is uncertain if these requirements will change for good, or are only temporary changes in the way. This poses the following question:

> **SQ3:** “Which changes do major employers anticipate in respect to changed working habits due to the coronavirus pandemic, and how has this changed the requirements of them, their employees and third-party stakeholders?”

The insights gathered through sub questions one to three can be used to determine a concept model for the selection and implementation of smart authentication systems for the commercial real estate sector. What such a concept could look like, is focused on in this sub question.

> **SQ4:** “What would a concept design for selecting and implementing non-intrusive authentication methods in the commercial real estate sector look like?”

A concept is only as valuable as how valuable stakeholders think it is. It therefore has to be tested for applicability and validity.

> **SQ5:** “To what extent does this concept design fulfil the requirements of its primary users, and how can it potentially be improved?”

To address the broader topic of maintainable and sustainable technologies, a critical look has to be taken to how the product life cycle should be (re)designed. Results of this sub question are not necessarily only applicable for this concept, and may contribute to the broader field of knowledge surrounding intelligent building technologies. It is therefore a supportive sub question to the concept design, but not integral for the implementation of the concept in a real life situation.

> **SQ6:** “How should the product lifecycle be redesigned so that these non-intrusive authentication systems can be applied in a maintainable way that benefits all stakeholder groups?”

Both the research and sub questions have been determined through earlier conducted research as presented in “The Office of the Future: Exploring State of the Art Smart Solutions in the Commercial Real Estate Sector in a Post COVID-19 Era”.

2.2 Research Design

Looking at the research goal, research question and sub questions as presented above, it can be seen that a process is followed which starts with gathering knowledge and works toward designing an artifact. Multiple methodologies exist to support the design of an artifact, however, for this research it is chosen to make use of the Design Science Methodology. This is a research methodology specifically for design problems and is presented in Wieringa (2014). A quick overview of what encompasses this methodology can be found in Figure 1 below. It focuses on solving a design problem by making use of the so-called design cycle. This consists of the steps problem investigation, treatment design and treatment validation. These steps can be repeated if necessary to refine the result. The issue tackled in this research is most definitely a design problem, since the end goal of this research is to present a concept design for the selection of a (preferably) non-intrusive personal authentication system for the commercial real estate sector (with a focus on office buildings). Most of the sub questions contribute directly to solving the design problem (e.g. the problem context, stakeholders and its requirements; SQ1, 2, 3, 4).

For the knowledge questions, information gathered from both popular and academic literature will be used. In conducting this research, the method as presented in Wolfswinkel et al. (2013) is used as a guideline. The method is not followed to the letter. Performing a literature review focused on academic resources only would result in missing significant amounts of relevant literature. Instead, the nature of the literature research aspect of this article follows a less systematic, more narrative approach. This is done to ensure that relevant, emerging literature focusing on this topic is included. Examples of such literature can be found in whitepapers of consultancy organizations, blog posts from experts in the field and news articles from major (international) news outlets.

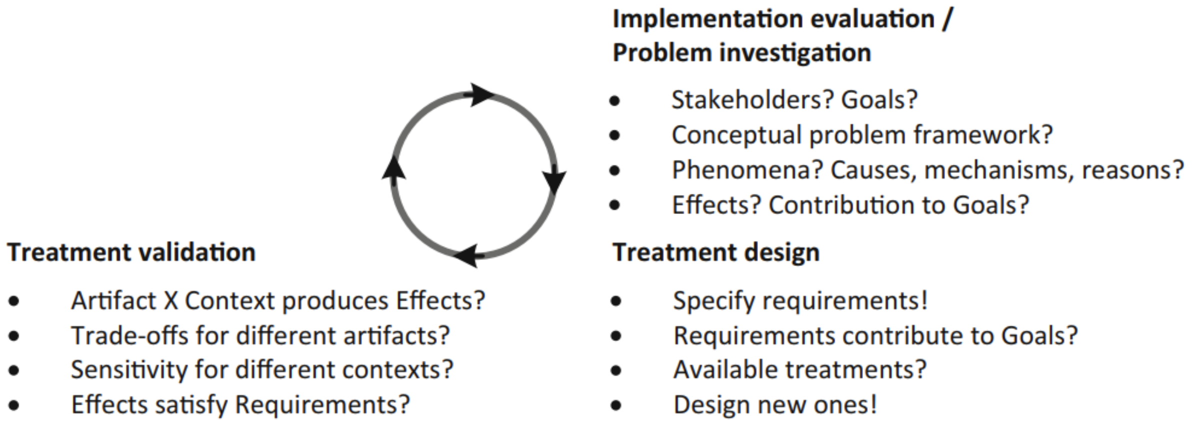

Implementation evaluation /
Problem investigation
• Stakeholders? Goals?
• Conceptual problem framework?
• Phenomena? Causes, mechanisms, reasons?
• Effects? Contribution to Goals?
Treatment design
• Specify requirements!
• Requirements contribute to Goals?
• Available treatments?
• Design new ones!
Treatment validation
• Artifact X Context produces Effects?
• Trade-offs for different artifacts?
• Sensitivity for different contexts?
• Effects satisfy Requirements?

Figure 1: Design Cycle as presented in Wieringa (2014)

To be able to make use of this design cycle, the purpose of this research has to be translated to a design problem. Wieringa (2014) provides a template for defining a design problem. This format consists of a model in which four gaps have to be filled in, and is as follows:

"Improve ***<a problem context>*** *by* ***<(re)designing an artifact>*** *that satisfies* ***<some requirements>*** *in order to* ***<help stakeholders achieve some goals>****."*

Based on this template, the following design problem has been formulated:

1. *"Improve* ***the use of office buildings by its occupants***
2. *by* ***redesigning the on premise authentication system used by its occupants***
3. *that satisfies* ***requirements for non-intrusiveness, smartness, maintainability and its different users***
4. *in order to* ***create an attractive piece of real estate with low ownership costs, decrease real estate tenant costs and improve productivity and comfort of its users****."*

Through formulating this design problem, the main purpose of this research has been determined and summarized. Consequently, research questions can be determined.

2.3 Qualitative Methods

Besides knowledge (previously) gathered from available popular and academic literature, currently unavailable knowledge from the corporate world in regards to the consequences of the Coronavirus pandemic is desirable. Earlier research as presented by Nieuwsuur (2021) could prove to be useful, however, an enquiry to get access to the complete untrimmed results has yet remained unsuccessful. Since this knowledge is highly desirable for a correct design, it is possible that such information should be gathered through the incorporation of a survey or different form of qualitative research methods.

For numerous other sub questions it can be useful to make use of qualitative research methods as well to gather insight in real life situations and validate findings. For example, the concept of the possible solution will have to be tested for applicability. This can either be done by surveying stakeholders' response on the core ideas and principles of the concept, or survey experts in the field to validate the added value of the presented concept. The most efficient and effective qualitative methods used for each question could be as follows:

SQ2: Interviewing - Data gathered from desk research has already provided a direction, mainly on what the stakeholders are and what the most obvious requirements are. For the more subtle requirements, information from the stakeholders itself is necessary. Due to restrictions in time and resources, it is difficult to not possible to interview a very large number of stakeholders. Therefore, experts in the field should be interviewed as they are likely to have knowledge of what most stakeholders look for when implementing authentication systems.

SQ3: Interviewing, questionnaire, surveying - Each of these methods could be used, depending on how many results one desires and how much data has already been gathered about the phenomenon. A questionnaire is likely to be most effective, as a broad number of companies can be contacted and the responses of the companies are not limited to a predefined set of answers.

SQ5: Interviewing - For SQ2, interviews with experts have been conducted to determine the requirements. This should be repeated to ensure that the found solutions are applicable and effective in the set environment. It is important to interview experts in the field, and not just the users of the products, as these might not have the knowledge to determine if a certain method can be realistically and effectively implemented to resolve a certain issue. The results of these interviews can be used to improve the concept, directly or in the future. Furthermore it can contribute to indicating the limitations of this research.

The success rate of all of the above mentioned methods of course depends on the willingness of third parties to cooperate in this research. If, for some reason, the number of responses turns out to be too low, alternatives have to be taken into consideration. Alternatives could be existing research data (if available) or a switch from a questionnaire or survey to expert interviews. This can be done conducting expert interviews requires the number participants to be much lower. In such a case, it is hoped that an appeal to the authority of these experts can at least partially compensate for the loss of a broader span of data.

2.3.1 Interview Methodology

For the conducted interviews, firstly the categories of interviewees which are deemed to possibly be interesting to interview were determined. These are as follows:

- Domain experts: these include experts from the field which are occupied with designing, maintaining and implementing authentication technologies or access control systems.
- Base level interactors: these include interviewees which act with the authentication system on the base level of merely using it to authenticate one-self to be able to get access to a room or service.
- System level interactors: these include interviewees which directly interact with the process of authentication, beyond the level of merely using it to authenticate oneself. Sometimes they might even be an integral part of the system. An example of such a subject is front-desk employee, issued with providing authentication to individuals and handing out id-cards or keys.

The interviewees are selected by the author for eligibility and perceived knowledge of the topic. In terms of design of the interview, a semi-structured approach is used. This ensures free flow of conversation and prevents any bias. A set of topics which are to be discussed and some orientating questions are determined upfront. These include topics in regards to the interviewee's experience with authentication technologies from a personal or professional perspective, perceived developments of authentication over the years, future expectations of developments of authentication and lastly how one feels the coronavirus pandemic is going to affect office use in the future (and how authentication could be a part in this). This last topic is discussed to enrich the information acquired from literature as will be discussed in Section 8.

During the interviews, notes will be taken where necessary. All interviews are recorded and the recordings are stored as well (unless the subject did not provide permission for this) to ensure academic integrity.

2.3.2 Interviewees

Over a period of approximately 2 weeks, a total number of 7 interviews were conducted. A larger number was preferred, however, due to several availability issues of multiple potential interviewees this was not possible. However, interviewees of all of the three categories above were interviewed which should result in a satisfactory result in terms of information extraction. The division of the number of interviewees interviewed per each of the categories can be found below.

- 6 Domain experts were interviewed
- 7 Base level interactors were interviewed
- 2 System level interactors were interviewed

Note that some of the categories may overlap. Since authentication is such an integral part of day to day life, it makes sense that each of the interviewees is a base level interactor. Nearly all organizations make use of some type of authentication that goes beyond the use of simple metal keys in current days. These are often keycards or other Radio-frequency Identification (RFID) tag related solutions.

A short profile description of each of the interviewees is given below. As indicated, each of the interviewed subjects possesses the role of base level interactors next to the role as described in their short profile description. To try to ensure that the interviewees do not answer base level interactor questions from the point of view of system level interactor or domain expert, they are specifically asked about their personal experiences using authentication technologies.

Expert 1 is a system level interactor. She is and has been a front desk employee at a high-tech organization for over 35 years and has seen the sector and job description change significantly over the past decades.

Expert 2 is a senior domain expert. He has 20 years of experience at a high tech organization focusing on physical access control systems (PACS) technologies used for various applications. Over the past two decades he has seen projects succeed and fail, and can therefore provide useful insights in regards to the potential of certain authentication solutions. Both in commercial and technical respect.

Expert 3 is a senior domain expert. He has 20 years of experience at a high tech organization focusing on PACS technologies used for various applications. His primary focus lies on authentication technologies for parking purposes. He also possesses significant knowledge about the software side of access control solutions, primarily related to cloud solutions.

Expert 4 is a domain expert as well as a system level interactor. He is the contract manager for electronics, and measurement and control technology at an institute for higher education. From his function, he is responsible for nearly every piece of hardware and piece of wire running through the ground on the campus site. Data generated from this hardware is beyond his responsibility. Because of his function, he has the final responsibility for the access control systems used everywhere on the campus site.

Expert 5 is a junior domain expert. He has 4 years of experience within a high tech organization focusing on PACS technologies used for various applications. Here he has occupied several functions relating to smart solutions and identification technology. His primary focus currently lies on developing new innovative propositions, mainly relating to vehicle access control and the commercial real estate sector.

Expert 6 is a junior domain expert. He has 3 years of experience within a high tech organization focusing on PACS technologies used for various applications. His main expertise relates to biometric access control solutions and developing software to support these solutions.

Expert 7 is a senior domain expert. He has over 20 years of experience in software development, and is currently working at a startup company focusing on developing privacy proof biometric authentication technologies. His experience with such a new, innovative proposition can provide crucial insights in the future of access control solutions and therefore determine the feasibility of certain concept solutions.

A summary of the interviewees' characteristics for reference can be found in Table 1, on the next page.

Expert no.	**Categories**	**Professional role**	**Years of experience**
1.	System level interactor	Front desk employee	35 years
2.	Domain expert	Technical expert access control	20 years
3.	Domain expert	Technical expert access control	20 years
4.	Domain expert/system level interactor	Contract manager for electronics at an educational institution	20 years
5.	Domain expert	Business developer access control	4 years
6.	Domain expert	Technical expert biometrics	3 years
7.	Domain expert	Technical expert face biometry	20 years

Table 1: Summary of Interviewees' Characteristics

2.4 Research Questions Positioned in the Design Cycle

Below one can find an overview of how the design science methodology of Wieringa (2014) is used in this particular research. As can be seen in Figure 2, each of the sub questions is grouped with regards to the stages of the design cycle, and coupled with the main activity that is being conducted to be able to answer that specific question. Furthermore, as can be seen in stage one, a division is being made between the use of theory and qualitative research methods.

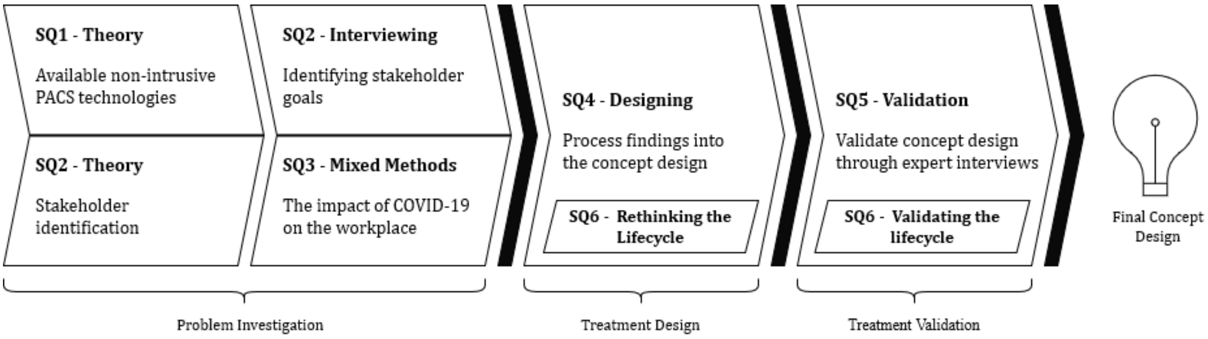

SQ1 - Theory
Available non-intrusive PACS technologies
SQ2 - Interviewing
Identifying stakeholder goals
SQ2 - Theory
Stakeholder identification
SQ3 - Mixed Methods
The impact of COVID-19 on the workplace
SQ4 - Designing
Process findings into the concept design
SQ6 - Rethinking the Lifecycle
SQ5 - Validation
Validate concept design through expert interviews
SQ6 - Validating the lifecycle
Final Concept Design
Problem Investigation
Treatment Design
Treatment Validation

Figure 2: Overview of the Research Design

2.5 Components of this Thesis

The first major artifact which is presented in this research is an extensive set of requirements. These requirements are engineered throughout this research by means of a literature review and interviews with experts in the field of authentication technologies. These requirements relate to criteria which non-intrusive authentication systems should satisfy for optimal implementation in an office of the future and range from basic technical requirements to usability requirements. The latter contribute significantly to finding a non-intrusive solution.

Once the requirements are engineered, available solutions are reviewed to see if these may qualify in satisfying these requirements. It may be the case that a single off the shelf solution may suffice to fulfil (some of) the requirements in a certain scenario, or that an extensive set of solutions might be necessary to only fulfil the smallest requirement of a specific stakeholder. Continuing, a concept incorporating an extensive set of available smart authentication solutions may not per se be the right for every context. A large organization with a large building and significant capital implicitly has to do more to satisfy similar requirements when compared to organizations occupying a significantly smaller building. Furthermore, such larger organizations are also likely to be able to adopt a more complete solution due to that they have more financial capacity. For the concept to be applicable to as many contexts as possible, a static model is unlikely to be fit. This introduced the second major artifact: a dynamic model decision support model. Such a model in which users can assign weights of importance to different criteria is much more likely to be usable in a wide range of contexts. This to determine which components are a must have and which are nice to have for each desired outcome.

Lastly, the topic of the product's lifecycle has to be discussed. Complex information systems such as authentication systems nowadays consists of a combination of interdependent hardware and software. This is under constant development, with users demanding more and more on the software side as they have expectations relating to user experience. However, since the hardware is often embedded in the building, hardware and software are unlikely to develop at the same pace. Such a difference in development speed has an impact on the lifecycle of these technologies. The last component of this research therefore focuses on analyzing authentication technologies for smart offices, and determining which best practices can be applied to optimize this lifecycle.

3. The Concept of "The Office of the Future"

In Section 2.1, the problem context was shortly introduced. However, to get a deeper understanding of the problem context in which the proposed solution will be applied, additional background knowledge about this context is required. Because the subject of this research is non-intrusive authentication systems for use in the context of the office of the future or the smart office, the body of knowledge revolving this subject is elaborated upon. A literature review is conducted in this field to find the definition of what comprises an office of the future, how this definition has changed and developed over time and how this differs between different areas around the world. This knowledge is consequently used to determine which potential solutions might be useful for adoption in this problem context. This is elaborated upon in Sections 4 and 5.

3.1 The Methodology in Practice

When one thinks of the office of the future, one likely immediately thinks of a futuristic, revolutionary view at the design of an office or the appliance of intelligent technologies inside the building. But is that necessarily the case? In Chapter 2, the general methodology for conducting a literature review as presented in Wolfswinkel et al. (2013) was elaborated upon. This method is now being put into practice. To be able to answer this question, the academic literature search engines of Scopus and Google Scholar were consulted. Luckily, academic literature revolving around intelligent buildings (IB) is sufficiently available, and should be able to answer this question. As initial search terms, "Intelligent Office Building", "Smart Office Building" and "Smart Office" were used. When finding literature, I choose to limit the age of the literature to approximately 20 years old. This is chosen due to the great technological advancements which have been made, especially in the sector of information systems and the internet. It is worth noting that the first definitions of an IB date back to the mid and late 1980's, and that this definition has been changing constantly ever since, incorporating aspects previously ignored or deemed not important enough (Leifer, 1988). Furthermore, I tried to put focus on the aspect of enabling technologies in office buildings, as such an enabling technology is the scope of this research. Nevertheless, some background knowledge is always necessary for correct understanding of the existing theories. Final search results were selected for being relevant to the topic by evaluating the article's title and abstract.

Following a brief scan of the results, it was clear that the results found when using the word "Smart" instead of "Intelligent" were found to be significantly less relevant, indicating the preferred terminology among scholars. Furthermore, many articles were found to be too topic specific, relating to case studies or implementations of specific components for an IB. These were consequently excluded. Since for this research it is not necessary to dive into the details of all the aspects of IBs, it was found that looking at literature reviews and major theories would be sufficient. Focus was consequently put on identifying these reviews. Primary research was found to be presented in Wong et al. (2005), which reviews work relating to requirement modules to which IBs can be tested on. Through backwards searching of this article, a landmark article in the field was found which was previously excluded due to age limitations. A major part of this work is based on research as presented in So et al. (1999), which strives to redefine the definition of IBs. This theory has been built upon and was extended in the years that followed. More recently, Ghaffarianhoseini et al. (2016) builds on the research as presented in Wong et al. by taking a look at this issue from a global perspective. That is, it explains how the fundamentals of IBs differ in the context of different regions and cultural perceptions. Of course, due to the nature of this research and the context it is conducted in, the results focused on Europe and North America are likely most useful for further analysis.

3.2 A Method for Finding a Context-Based Definition

Chapter 2 of the article by Wong et al. (2005) is dedicated to the exact question of the definition of an IB. According to the authors, at time of publication of the article, over 30 definitions of intelligence in relation to buildings existed. Most of them focused on technology and disregarded interaction entirely. This technology centered approach has been criticized significantly by many researchers, as changes in an organization which occupy the IBs should be reflected in changes of the building and the technologies involved. Multiple authors therefore indicate that buildings should respond to its user needs, and therefore should be in constant development. If this is not the case, this could reflect upon the wellbeing of the people working in these buildings, resulting in negative effects on productivity, morale and satisfaction. This ability to respond to changes is therefore included in the definition of an IB by some scholars, highlighting the necessity of buildings to be able to learn from its users and adjust based on its occupancy and the environment.

This, however, still does not lead to a precise definition of IBs. It merely defines some vague aspects relating to a supposedly IB which should, for some reason, be universally applicable. However, the definition is not set in stone. Specific situations require specific solutions, or in other words: there is not a single definition which covers all types of IBs. This was also recognized by So et al. (1999), which proposed a new definition for IBs (for Asia, however, it is not unlikely the strategy is universally applicable) through a two leveled strategy. The first level involves eight so-called Quality Environment Modules (QEM) (Modules M1-M8); areas that deserve attention of some sort. These modules are: environmental friendly, space utilization and flexibility, life cycle costing, human comfort, working efficiency, safety, culture and image of high technology. Another 2 modules, construction process and health and sanitation, were added later by Chow (2005) bringing the total number of modules to ten (M9 and M10). The second level of the model relates to intelligent building facilities contributing positively these QEMs, which are consequently assigned to one of the modules in order of priority from the user's point of view. The new definition of an IB, according to the authors, is therefore as follows:

"An Intelligent Building is designed and constructed based on an appropriate selection of quality environment modules to meet the user's requirements by mapping with the appropriate building facilities to achieve long-term building value."

This method recognizes that, for any given type and use of a building, the priority of QEMs differ and therefore the definition of an IB differs. An example of applying this method using these QEMs is provided in Table 2, which can be found below. Here it is clearly visible that in this case, for office buildings, human comfort and space utilization (as expected) are of the utmost importance as they are deemed to be beneficial for productivity. This can be seen as they are given priorities 1 and 2 (with 1 being high and 8 being low). The table is based on the initial QEM model, which was only limited to eight modules. When the additional two modules as presented in Chow (2005) would have been included, it is likely that M10 (health and sanitation) would be on P1 for at least a hospital building. Even more so, the prioritization can easily shift over time as well. During the 2020 and 2021 coronavirus pandemic for example, it is very likely that M10 would be on priority one (P1) for most of the different building types. Continuing, "image of high technology" is becoming more and more important as well, as many organizations wish to label themselves as being high tech to gain an advantage over their direct competitors.

	Environment Friendly	Space Utilization & Flexibility	Life Cycle Costing	Human Comfort	Working Efficiency	Safety	Culture	Image
Hospital	P1	P7	P5	P3	P4	P2	P6	P8
Residential	P4	P6	P5	P1	P7	P3	P2	P8
Commercial	P3	P2	P5	P4	P1	P7	P6	P8
Transport Terminals	P3	P7	P6	P2	P8	P1	P5	P4

Table 2: An example of module assignment to four building types (So et al., 1999)

The theory as presented in So et al. and Wong et al. could prove to be very helpful for future research conducted in this field. One can apply the theory by presenting it to different stakeholders of office buildings. This could, for example, be done by means of a survey. For instance, one could ask the stakeholder to rank the QEMs based on the building type of the stakeholder, or let the participant indicate which facilities they feel are the most important in their situation. This could clearly indicate the different priorities of different stakeholders. Furthermore, by pre-selecting some facilities of which the participants can make a selection from (limiting the selection freedom of the stakeholder participating in the survey one may test the possible market opportunity of these selected facilities. This might be too complicated to execute for a broad set of building types since this would require a large number of participants, but since this research focuses on a single building type (commercial real estate or office buildings) this could very well be possible.

Lastly, since the last global health crisis predates to over a century ago, previous results might not prove to still be applicable due to the changed demands and mentality of each of the stakeholders. After all, not every office worker has the potential consequences of health and sanitation risks printed in the back of his head during the course of each day, as this is not one of his main concerns. However, the effect of a pandemic such as the coronavirus pandemic must not be underestimated. It might easily have switched priorities, making revisiting this research necessary and valuable.

3.3 A Look Across Global Borders

Just like Wong et al. (2005), the article as presented in Ghaffarianhoseini et al. (2016) has gone over the different definitions that exist for IBs and which changes could be observed through the different publications over the past few decades. However, in addition to the main findings as presented in Wong et al. (2005), this more recent provides a clear overview of the most important features that influenced the change in the definition of IBs through an aggregate table. For reference, this table can be found in the appendices section of this research as Appendix A. Some aspects not present in this table as presented by the authors in 2014 have been added following the findings as presented in this research. For a deeper understanding of smart offices, topics regarding the Building Management System (BMS), intelligent control strategies, learning capabilities, communication systems in general and the increased focus on energy efficiency are definitely worth looking into on a deeper level.

Continuing in this respect, the article by Ghaffarianhoseini et al. (2016) stresses the importance of enabling innovative technologies in IBs to reach its full potential (which it is claimed to not have reached yet). Among these technologies, cloud computing to minimize the physical footprint of computers on the client side and the application of embedded sensors for personalization and instant feedback are included and widely recognized as becoming more and more important in the future. This is especially the case for embedded sensors, which are slowly but steadily becoming integrated in the standard definition of IBs, as buildings need knowledge about their environment to be able to constantly adapt and respond to their occupants. This is supported by Clements-Croome (2013), which defines Information and Communications Technology (ICT) and web-based electronic services as some of the key constituents IB technologies, and consequently of sustainable IBs.

Lastly, as indicated in the introduction of this section, an emphasis is put on the differences in points of view in different parts of the world on what constitutes an IB. The authors go deep into the different guidelines, features, standards and priorities of scholars, architects and local IB institutions. Summarized, however, the following findings are presented:

North America/Europe:

It is found that (research on) IBs in Europe and North America mainly focus on the role of Information Technology (IT) infrastructure, and additionally but in lesser respect, human capital/education and environmental implications. In Europe, IBs are often seen as an important element of the popular concept "smart cities". Energy efficiency is being promoted in Europe by a 2010 EU directive which strives to achieve the goal that newly built buildings are energy neutral by 2020. In North America, on the other hand, performance and cost-effectiveness through the application of innovative technologies have been the priority ever since the emergence of IB systems in the 1980s.

Southeast Asia:

Although some focus is put on energy efficiency in the "western world", this is much more present in the fundamentals of IB design in Southeast Asia. It is argued that, for example, in Malaysia and Singapore, IB design is closely intertwined with green design and sustainable development. Design of IBs is characterized as a "multi-dimensional metaphor" for the development of buildings that are green and environmentally friendly instead of buildings that exclusively incorporate the newest ICT solutions and advanced technologies.

Far East Asia:

Unsurprisingly, in far East Asia (Korea, Hong Kong, China and Japan), sustainability is an important aspect as well, together with smartness. Energy conservation and environmental friendliness are a crucial part of the IB system. Sustainability, however, is also viewed here as being sustainable for its user, paying attention to the issues users are experiencing to ensure a higher quality of life. This is especially the case for Japan, which is leading up front in terms of service oriented IB systems. It is likely that this is caused due to the high energy and land prices in Japan, and relatively high environmental and ecological awareness of the land's citizens. In China, focus lies more on the smartness aspect, with a system oriented approach. This means incorporating IT and IB Systems in the buildings (mostly Information Systems, Intelligent Systems, and Infrastructure Systems). Less focus lies on the environmental aspect, although it is likely that their buildings are more environmentally friendly by nature than buildings built in the post-World War II period in Western Europe, sheerly due to their age.

From these different points of view, it is concluded that there is not yet a standard definition for IBs. Just like was concluded in the research of Wong et al. (2005) and So et al. (1999). The authors therefore present four Key Performance Indices (KPIs), which should be considered in the IB's components of systems, performances and services, to be called: smartness and technology awareness, economic and cost efficiency, personal and social sensitivity and environmental responsiveness.

3.4 Main Takeaways

It is clear that the world is still far away from a unified definition of what comprises an IB. Priorities in different parts of the world are just too far apart, and due to rapid technological developments in various fields which might seem to only be remotely related to the topic of IB systems are changing the definition constantly. This also introduces a more philosophical question: is an intelligent building of today still deemed an intelligent building in a decade, or even in only a couple of years' time, when the typical economical life span of a building lies between 35 and 60 years? (Marsh, 2017) A car which is ten years old is often viewed as being still quite modern, while a mobile phone is often viewed as ancient after a similar period of time (e.g. the iPhone 4, introduced in June 2010). Is a drastic development needed to change how we view existing technologies, or does a base level exist of what is deemed smart? These are all questions which deserve an answer, but are probably difficult to find an adequate answer to. However, the theory as presented in the reviews as discussed above do provide some starting points for this research. This is especially the case for the study by So et al. (1999) and the research that extended the theory regarding the Quality Environment Modules. This theory is used and quoted in a significant number of articles regarding IB systems, and seems to be the leading theory in the field. By using this theory, a new concept for the an intelligent office building can be created based on the priorities of the different stakeholders incorporating the prime facilities and concerns of this time. This concept should be created by consulting the actual stakeholders itself, through qualitative data gathering methods, such as surveys. Consequently, potential intelligent building facilities and QEMs which are deemed to be most important could be put in focus to be researched with more attention to how these can be applied effectively in its context.

4. Non-Intrusive (Personal) Authentication Systems

Now that the context in which the concept will have to be applied is clear, it makes sense to elaborate upon the basics of the concept that is being developed. When looking at the title of this chapter, one can clearly distinguish two aspects which will have to be defined before digging deeper into the contents of this topic. These are the aspects of "non-intrusive" and "personal authentication systems". For both of these aspects, a definition will be presented in the coming sections. This definition will be based on available (academic) literature, and adjusted to fit the studied context if necessary. Based on the definitions of what comprises non-intrusive authentication systems, fitting solutions can be identified and selected for supporting the stakeholders within the context of the smart office. This is elaborated upon in Sections 5 and 6.

4.1 Personal Authentication Systems

Let us first take a look at what academic literature has to tell about this subject. When using the query "Personal Authentication System" OR "Personal Authentication Systems" in the academic literature database of Google Scholar, a total number of 1130 results pop up. Most of these results relate to the design of a single system, where most of these systems are based on the use of biometrics. Examples of this use the commonly seen fingerprint scanner, but also less often seen innovative concepts using hand vein, palmprint, knuckle print or audiovisual features of individuals. Most of these results are published quite recently, with over 95% of the results being published in the last 20 years. This shows that it is an emerging topic. A clear evolution can be seen, with the oldest results often relying on the use of fingerprint recognition technology and the newer results focusing on a more mixed method approach often supported by the use of AI technologies.

While these results are certainly interesting and useable for this research when looking for the available solutions which can possible be incorporated in the to be developed concept, they do not provide a definition of what a personal authentication system exactly is. In the articles, basic knowledge about what such a system should do is assumed. It is therefore necessary to de-compose even further and dive into the definition of authentication, as both the terms "personal" and "system" are unlikely to require any additional explanation.

4.1.1 Defining Authentication

The Oxford dictionary defines authentication as "the act of proving that somebody is a particular person" (Oxford Dictionary, n.d.). It should not be confused with the closely related concept of identification: while identification relates to indicating an individual's identity, the goal of authentication is to prove that this identity actually belongs to this individual. Generally speaking, there are three recognized types of authentication: something you know (1), something you have (2) and something you are (3) (Pearson IT Certification, 2011). A short explanation including some examples of authentication types within each of these levels can be found in Table 3. To increase security, it is advised to not use a single authentication method but instead combine multiple identification methods between these three categories. When combining multiple identification methods, it requires the attacker to possess more than a single skill to impersonate someone's identity. This increases the likeliness of an attack to fail. The idea of combining multiple authentication technologies was first filed for a patent by AT&T back in 1996 but has since expired. (Blonder et al, 1995). Combining multiple identification techniques is called multi-factor authentication (MFA) and has become more and more popular on the internet over the past decades. This makes sense, as the number of internet services requiring an account only keeps on growing and people often re-use the same password over and over again. Combining this unsafe practice with a second or even third layer of defense strengthens the position of the user significantly. Often used combinations of authentication methods are those combining a user specified password with a randomly generated token. Now that smartphones have become common practically all over the world, token generators do not have to be a single dedicated device used for a single application, which used to be common practice in the past. Software developers can make use of smartphone applications to take the place of these token generators. Examples of services making use of such applications are plenty, as can be seen when searching for "authenticator" in the Google Play Store (Google, 2021).

	Description	**Examples**
Knowledge	Anything that you can remember and consequently type, say, do perform or recall when needed	Includes passwords, combinations, pin codes, code words, secret handshakes
Posession	Phyisical objects	Includes keys, smart devices, smart cards, pen drives, token generators, chips
Inherence	Any part of the human body which can be used as verification. People's unique physical and behavioral characteristics, commonly referred to as biometrics	Includes fingerprints, hand palms, face, retina, iris, voice, veins, shape of hands

Table 3: The three commonly recognized authentication categories and some of their examples

4.1.2 Continuous Authentication

A relatively new type of authentication used in IT systems is continuous authentication. When searching for the topic of "continuous authentication" in academic literature search engine Google Scholar it becomes clear that the topic has emerged in the late 90s, with only few mentions up to the year 2000. However, it has seen significant attention in the past decade and is really gaining traction over the past few years. Conventional authentication methods authenticate users at a single moment, when the user initially logs in. After this initial security check has been bypassed, further security checks are often absent, which makes the system vulnerable to malicious practices. Continuous authentication aims to resolve this issue by continuously monitoring user behavior. Examples of behavior that can be monitored are keystrokes, touchscreen touch dynamics or even one's writing style. Due to the emergence of smart devices, use of such continuous authentication methods are more and more becoming a serious option; smart devices have access to a significant amount of sensors which makes monitoring of behavior much easier than ever before. This new type of authentication can especially be of interest in this research, and therefore deserves to be taken a look at on a deeper level.

4.2 Non-Intrusiveness

Continuing, now that the aspect of authentication has been introduced, it is time to look at the second aspect of what this research strives to achieve: non-intrusiveness. Everyone has some idea of what non-intrusiveness might look like, however, this definition is not set in stone. Unlike the concept of authentication, intrusiveness is something which is subjective and very context dependent. Oxford Dictionary defines the word "intrusive" as "too direct, easy to notice, etc. in a way that is annoying or upsetting" (Oxford Dictionary, n.d.). What is too direct, or found annoying or upsetting differs drastically between people, and is influenced by someone's frame of reference. It is unlikely someone finds noise to be intrusive when you are at a football stadium, but only the slightest noise in a library or study hall is often frowned upon and found very intrusive.

Some technologies commonly used in the field of authentication were already shortly introduced in the previous section. For some of those, it is quite easy to say that one is more intrusive to one's day to day activities than another. For example, a key is likely to be found more intrusive than a fingerprint reader. You can forget to bring the key with you, it is likely that you need more than one key to access the majority of rooms in a building and have to get the key out of your bag or pocket and actually insert and turn it to make use of its function. A fingerprint reader is readily fitted to the wall next to the door and can be used without any additional effort other than existing: the key is always there in your hand because it is your hand. Even though opening a lock by using a traditional metal key is unlikely to feel as a very intrusive activity to many people, relatively speaking it is much more burdensome than a fingerprint keylock. However, if it is possible to authenticate an individual without having to perform any additional activity at all, for example be identified directly when walking in front of a locked door equipped with sensors and cameras, a fingerprint scanner might even be viewed as being relatively intrusive. This is, of course, all dependent on what is possible and what one's definition of intrusive actually is.

4.2.1 Balancing Intrusiveness, Usability and Security

To define "intrusive" in this context, is therefore necessary to first of all make an inventorization of all commonly available authentication technologies. This will create a playing field of authentication technologies, which consequently could be ranked from most intrusive to least intrusive. There are many ways this can be realized. For this research, the goal is to increase the user friendliness of office building use through smart authentication technologies. It should make sure users can focus on doing their work, without putting too much effort in non-essential issues. The authentication technologies should therefore be assigned a score on different (usability) aspects which relate to authentication technologies to be able to rank them from top to bottom. This would include the common aspects of effectivity and usefulness, but also aspects such as keyless operation and scalability for different users. An alternative could be to present this entire range of technological solutions to end users, and ask them to relatively rank them from most intrusive to least intrusive. The latter, however, is a very labor intensive task for both the participant and designer of such a survey and requires a great number of respondents to return an acceptable result. Furthermore, participants not familiar with novel authentication concepts are unlikely to be able to rank those properly and might therefore require additional explanations about these concepts. This makes the process all the more difficult, and is therefore unlikely to be a realistic option within the scope of this research.

Defining a relative scale for intrusiveness of technology is therefore the most logical option. However, the entire operation is unlikely to be this plain and simple. Sure, when non-intrusiveness is the only thing that matters a scale can be constructed. In that case, the authentication systems which score well on usability aspects such as key and touchless operation and low skill level required would likely be put on top. However, this often results in trade-offs to be made. Examples of such trade-offs could be costs, safety and invasion of one's privacy. Therefore, it is unlikely that a solution which is very unintrusive in terms of effect on the user's daily operation will be applicable in a multitude of contexts. A context based scale is therefore required. Or in other words: a scale should be constructed based on the different requirements that the potential users and operators of these authentication technologies may have. Literature already provides some indications of requirements which may be included. An example of requirements which cover both the aspects of security and usability can be found in Figure 3. But, for the sake of completeness and to make sure the requirements are up-to-date to what users currently find important, it is necessary to get insights from the actual user and incorporate these in the ranking and final concept for non-intrusive authentication. Therefore, making use of qualitative research methods is advised. As already explained in Section 2.2.1, semi-structured expert interviews will be conducted to construct the requirements. The insights from these interviews will be used to define this multi-dimensional authentication score, which should combine aspects from both the usability and security fields to create an easy to use and understand, but secure implementation. This will be elaborated upon in Section 6.3.

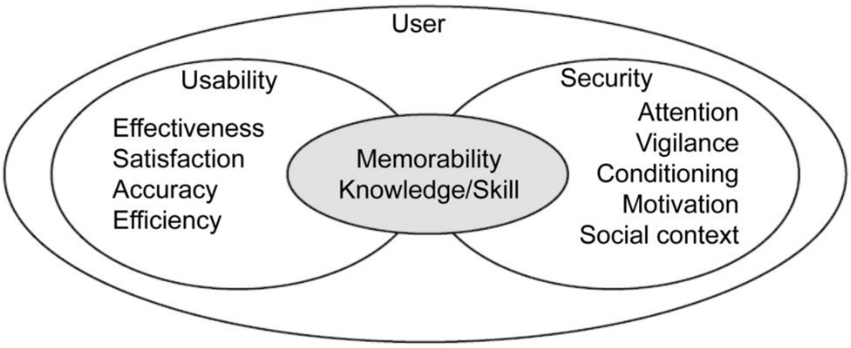


Figure 3: Security and usability requirements (Kainda et al., 2010)

5. Review of Available (Concept) Authentication Systems

Now that the definition of non-intrusive personal authentication systems for this research is clear, the body of knowledge surrounding this can be explored. A lot of information regarding this topic can be found in both academic and popular literature. However, for the scope of this research, it is important to make sure that the contents do not become too technical. The search for information should focus on how the systems work from a user's point of view, how it can or is generally implemented and what potential benefits it can offer to the user experience. Since this research focuses on the application of personal authentication systems in smart office buildings, it makes sense to initially search for comprehensive reviews of such technologies in this context. If this does not suffice, which seems likely, reviews of available authentication methods in general should be consulted. Lastly, to make sure no technologies are missed, articles regarding individual solutions may be addressed. Popular literature should not be disregarded and might be used to look for novel ideas, especially due to the recent developments regarding the global coronavirus pandemic. Knowledge gathered in this section may consequently be combined with stakeholder and authentication requirements which will be identified in Sections 6 and 7 to determine which solutions should be included or discarded in the final selection model.

5.1 Authentication Systems for Smart Office Buildings

Comprehensive academic reviews of authentication facilities for intelligent office buildings are scarce. This is even more so the case if one wishes to limit the results to articles which were published quite recently, say in the past one or two decades. Most articles focus on the application of technologies such as IoT, machine learning, artificial intelligence (AI) and big data as supporting technologies for the development of IB facilities in general. Information about the actual application and use cases of these technologies is even more difficult to find, and if available, often tailored to a single specific solution. Furthermore, some available research is dedicated to the use of standards in building automation and management systems as well as machine to machine standards.

What about individual concepts for the smart office? Some information is available, although it does not entirely fit the purpose of this research as it is focuses on presence and intrusion detection. It may, however, be used to support authentication technologies as it could possibly identify individual users. For example, Borodavkin (2019) focuses on the application of sensor powered IoT devices of different standards to determine office use and monitor environmental factors. The possible use cases for these devices are consequently elaborated upon. Unlike most articles, this article also analyzes the possible use cases and available solutions which make use of the Bluetooth and Global Positioning System (GPS) standards for locating purposes within buildings. Akbar et al. (2015) approaches similar problems through an entirely different solution: determining occupancy of smart offices through recognition of electricity consumption data. The benefit of this approach should be minimal investment costs, as additional hardware or sensors are not necessary if smart energy meters are already applied in the building, which the author claimed is likely the case if a building strives to be intelligent.

This aspect of presence detection may be combined with technologies within the area of security, by detecting an individual and consequently authenticating this person to be able to use certain services within the building via IoT devices or integrated network technology. Research as presented in Tao et al. (2011) strives to achieve this goal by installing infrared sensors in the ceiling of the office building to detect presence inside a building, and tackle the issue of tracking persons which located in roughly the same position within the same room by applying motion direction tracking. They indicate that, over time due to analysis of movement by a learning algorithm, authentication of individuals should be made possible as well. This article is especially interesting as it provides a novel solution to the issue this research aims to tackle, by firstly focusing on the concept of physical access to or within a building in contrast to access to electronic devices such as computers, and secondly it strives to achieve this goal without the use of additional tools or biometric characteristics such as fingerprints or iris scan.

An alternative to this non-intrusive authentication solution is proposed in Sanchez et al. (2019). This article shows the major steps that have been made over the past decade in this field. Their findings are also focused on authentication, but on the level of accessing a device or information system. The area of AI, and specifically (deep) machine learning algorithms has developed rapidly in the past years. This is made possible by the increase of computational power that is made available to the general public. Interaction with heterogeneous IoT devices can generate a significant amount of data, which can consequently be used to create rich behavior patterns. Mobile devices such as smartphones or smart watches play a big role in this respect. This extended analysis of data increases the accuracy of the authentication process drastically, and may be used to grant a user access to their devices and consequently sensitive (company) data in real time. If computational power allows for this process to be executed indefinitely, a very powerful implementation of continuous authentication might be achieved. Combining research of Tao et al. (2011) with the findings of this research might open up possibilities for a nearly uncrackable code which does not longer require any pin codes or passwords to be remembered. This cuts out what is often deemed as being the weakest link of security systems: the user itself.

Both these authentication related solutions, as interesting as they are, were unfortunately only tested on a very limited basis and therefore only represent what might be possible. The articles do not mention any actual implementation in a real life scenario besides the testing environments. The actual success rate of these technologies therefore remains to be seen.

5.2 Authentication Systems in General

Because, as expected, academic literature specifically aiming at exploring or developing authentication systems for the smart office is limited, taking a broader approach to this issue seems necessary. This means exploring the different available technological solutions within the field of personal authentication systems in general. As indicated, once again the search starts by looking for reviews of this topic. The search of academic literature for this topic is done on the search engine of Google Scholar, by making use of the search query "Authentication Systems" AND "Review". It is chosen to apply an inverse chronological approach when going through the articles. This is done because it is likely that more recent articles include all of the systems which are described in older literature. For example, if an article which is found focuses on a specific topic, e.g. biometric authentication systems, and this article pre-dates a different article on a similar topic which was already included in the review of this paper, it is not included.

Once again it becomes clear that the topic of authentication has received increased attention over the past decade: over 75% of all the articles found through Google Scholar were published in or after 2010.

5.2.1 A Comprehensive Review of Continuous Biometric Authentication Systems

The first article which is reviewed was published in 2021 and revolves around reviewing continuous multimodal biometric authentication systems (Ryu et al., 2021). It reviews authentication systems discussed in articles published after 2010, which ensures that only relatively modern technologies are included in this review. Focus lies on authentication method which are used for IT systems instead of physical access to rooms or buildings, or to be more precise: computers, mobile devices and wearables. This does not, however, mean that all the systems discussed can not be applied in other ways than described. A total number of 39 articles were reviewed. Through the process of reviewing these articles, 21 biometric authenticators were discovered to be used in an actual or conceptual implementation. These are, divided between three categories, as follows:

> Behavioral: *keystroke/typing, mouse, gesture, touch, phone movement, speaking, linguistic style, haptic, gait, wrist, behavior profile and voice.*
>
> Physiological: *face, ear, iris, fingerprint, palm, electroencephalography (a method for measuring brain activity, commonly abbreviated to EEG), electrocardiogram (ECG) and blood volume pulse (BVP).*
>
> Soft: *skin color.*

It is clear to see that behavioral biometric authenticators are favored in literature. This is also acknowledged by the authors, which indicate that 46% of the reviewed articles only combined authentication methods from this category. Methods only using physiological traits were discussed in only 28% of the reviewed articles. An explanation for why this could be the case is given as well. Behavioral biometrics can generally be collected in a non-intrusive way, and often do not require any additional hardware such as a camera or fingerprint scanner when implemented. It is also thought that behavioral biometrics require less computational power when compared to physiological biometric systems, since the amount of information collected is lower and generally more simplistic. Lastly, 23% of the reviewed articles combines both physiological and behavioral traits. It is argued that this may improve performance and measurability as they complement each other. The most used combination is keystroke dynamics and face recognition, once again because this generally does not require much additional hardware or interaction with a dedicated task-specific sensor. This is inherently more cost-efficient, which is something that should definitely be taken into account for this research as well. This aspect of cost-efficiency may highly influence the adoptability rate. Especially within smaller, less wealthy organizations.

All in all this article provides a clear and highly complete overview of the possibilities within the area of continuous biometric authentication. Furthermore, the arguments provided why certain biometric traits might be preferred over another are useful insights when aiming to design a concept with a high focus on user friendliness. Lastly, the methodology used in compiling this review makes sure that no relevant articles and therefore technologies are missed. All the major academic search engines were used, and the criteria for selection are clearly defined and argued why they were selected. Combine this with the fact that the article was published very recently, this study could be of great value for this research.

5.2.2 A review of Multi-factor Door Locking Systems

Another recently published article revolves around implementing MFA on a level of locking physical doors. Even though the article was only released quite recently, and therefore does not have a significant amount of citations, it touches an interesting topic. Generally, such MFA methods are only applied on the level of information systems. Motwani et al. (2021) attempts to perform a comparative analysis of scientific research relating to this topic in the field of security control systems. It is looking at the changes in development that the solutions have gone through over the past decades when MFA systems have evolved rapidly.

The authors highlight the development of the topic over the past couple of years, with locks having developed from traditional metal locks to seemingly un-hackable password locks in which users are encouraged or even forced to change their passwords every once in a while. This is also the first concept that is highlighted by the authors as being presented in research: a lock which features a keyboard and small display panel, connected to an Arduino device (small circuit board computer) to control the authentication mechanism. More advanced options are presented as well, including IoT powered locks and biometric authentication systems. Most of the solutions presented, however, are still in an experimental phase and are not yet commercially available in their presented form. This could express a feeling of amateurism. Continuing, some solutions are very similar to commonly available authentication systems available in most hardware stores, like the earlier described keylock powered by an Arduino. The only main difference of this locking mechanism when compared to a simple pin-code powered keylock is that is used a full size keyboard and requires the passwords to be changed periodically. One could therefore argue that the novelty factor the presented solutions is therefore rather absent. Some more examples of relatively obvious and commonly used authentication systems are presented in this article, however, it is important to not disregard these solutions either: they might be suitable for situations where basic authentication methods suffice. An overview of the reviewed technologies presented in this article, with the descriptions as they were given by the authors in the text, can be found below, in Table 4.

Even though the article claims to focus on MFA methods, it turns out that in most of the cases the authentication methods do not qualify as MFA methods. This is a shame, since the authors touch an interesting subject which is rather underexposed in literature. In only 40% of the cases multiple authentication methods were combined as security measures. Often, an alarm or notification is added when multiple authentication attempts by the user were denied, but this does not imply MFA. Furthermore, sometimes multiple methods of authentication are implemented as accepted methods. This seems to be more secure, but in fact is not. It is, however, more convenient for the user. Lastly, use of a fingerprint sensor seems to be the most popular option, as it is cost efficient, relatively secure and easy to implement. More advanced authentication methods using face recognition are present as well, but surprisingly only once the use of location (GPS) was implemented in a solution. This is surprising, because the opportunities for the use of (infrared) sensors or geofencing could be very promising but apparently are not being paid significant attention to in academic literature focusing on new authentication methods for physical doors. At least according to the findings as presented in this literature review.

Description	Method 1	Method 2	Alarm
Password Based Door Lock System Using Arduino	Password		
Remote Sensing Global Ranged Door Lock Security System via GSM	Keyword(s)	SIM	Yes
Smart Lock Based on Internet of Things	Phone app		
Digital Door Lock on the Access Control System using OTP	GPS		Yes
Security Analysis of Mobile Phones Used as OTP Generator	Generated pass		
Keyless Smart Home: An application of Home Security and Automation	Phone app	Password	Yes
Fingerprint Based Door Access System using Arduino	Fingerprint		
Fingerprint Based Door Locking System	Fingerprint		
Enhanced Security Methods of Door Locking Based Fingerprint	Fingerprint	Passcode	Yes
Biometric Security System with Phone Text Alert Notification	Fingerprint		Yes
Smart Door Lock System	Fingerprint	Generated Pass	Yes
Smart Door Lock Using Fingerprint Sensor	Fingerprint		Yes
Keypad/Bluetooth/GSM Based Digital Door Lock Security System	Passcode[1]		Yes
Smart Door Locking System using IoT	Phone app	Fingerprint	
Smart Door System for Home Security Using Raspberry pi3	Phone app OR face		Yes
Face Recognition Door Lock	Passcode	Face	
Color Image Edge Detection	Face		
Smart House Two Level Security System	Password	License plate	
CNN Image classifier on Raspberry pi 3B using pre trained data	Face		
Automated Door Accessing System with Face Recognition	Face		
Mobile Controlled Door Locking System with 2-FA	Video	Generated pass	

Table 4: Overview of reviewed (concept) authentication methods extracted from Motwani et al. (2021)

5.2.3 A Systematic Review of Authentication Methods and Schemes

This extensive review as presented in Velásquez et al. (2018) focuses on reviewing the entirety of literature revolving around authentication schemes and authentication methods, of which the first was published all the way back in 1974. Unsurprisingly, this article focuses on the use of text passwords. Through a thoroughly executed systematic literature review, a total of 515 single factor and 442 MFA techniques were identified. The authentication methods found are once again divided between the known authentication categories. Most of the methods which were found were also already found in the articles elaborated upon previously, however some additional new methods were found.

[1] Even though the passcode can be entered through either a keypad, a smartphone app via Bluetooth or text message, the method of using a passcode remains the same. This is not multi-factor authentication.

Important findings include an elaborate overview of the most used combinations of authentication methods when MFA is applied. Where the article by Ryu et al. (2021) only explains a few of the most used combinations, this article provides an overview of all the combinations found in the large number of articles discussed. This includes two-factor authentication (2FA) methods, as well as authentication methods consisting of three methods. Most commonly used combination is the combination of a text password and keycard, followed (on a great distance) by the same combination supported by some type of biometrics. An overview in which these authentication methods are applied or tested is also presented. In this overview, "smart environment" is included as one of the studied contexts. Although this context was only discussed in 7 articles, it is interesting to see that the focus in these articles was almost entirely put on the aspect of achieving authentication through methods of possession (6 times) and only once on inherence. Knowledge based authentication is clearly not viewed as suitable in the smart environment, hence why it was not used once in this context. Why it is not viewed as a suitable authentication method in this context is not elaborated upon. To know this for certain, it might be useful to apply backwards search methods to identify the original articles in which this was discussed. This could shed light on the design decisions that were made and help contribute to the to be designed concept.

An interesting body of knowledge which was also shortly discussed is the topic of decision frameworks for the selection and comparison of authentication methods. These frameworks may provide useful insights to define the structure for conducting interviews with the stakeholders of authentication within office buildings, and is therefore definitely worth looking through.

5.2.4 A Classification of Authentication Systems

This extensive literature review extends on other literature by classifying authentication methods on multiple levels. First and foremost the already known classification between ownership (have), knowledge (know) and inherent (are). For these three classes, their major threats and drawbacks are also indicated. Furthermore, a division is made between the implementation of authentication types. This is similar to the earlier discussed article of Ryu et al. (2021), which made a division between behavioral, physiological and soft. This article by Barkadehi et al. (2018) proposes a division between graphical centered, smartphone centered, touch-based centered, EEG-based centered and web-based centered authentication systems. This goes one layer beyond the classification of Ryu et al. (2021) since the question of how the implementation may be done in practical becomes a more tangible asset. Especially the extensive section dedicated to how smartphones may be used for authentication could prove to be of worth when looking for low or non-intrusive authentication methods. Smartphones have become such a part of day-to-day life that nearly everyone owns one, and brings it everywhere, always. Using something which people take everywhere eliminates the necessity of bringing other means of authentication, like keys or a keycard. Furthermore, the sensors and communication chips present in a smartphone make it easy and relatively low-cost to implement on-premise. The NFC chip within a phone, for example, is an often used aspect in authenticating users, next to the often used built-in camera and location positioning technologies such as GPS or NFC.

For all of the five categories, for each of the reviewed solutions the authentication factors and contributors are listed. This provides for an easy to understand overview of which devices and technologies are necessary to implement a certain authentication system. Furthermore, it is listed where each the authentication method is resilient against or would be prone to in the case of an attack. Taking into account various contexts, one may determine if something would be worth the risk to take since chances of it occurring is minimal. This could determine which solution may or may not be adopted. Continuing, the important factor of cost-effectiveness is taken into account as well. Based on review of articles, the most commonly used authentication methods are listed (EEG sensors, mobile, smart-card, microphone, e-pan or e-pad, mouse and keyboard, RFID tag and fingerprint sensors) with corresponding their cost-effectiveness and implementation difficulty. These are ranked with either low, medium and high and easy or hard.

All in all, this article provides a lot of information on various types of authentication methods. Too much to even start to assess all individually in this research. The different authentication methods which are discussed start from simple password protection and go beyond novel implementations using multiple methods in one system to provide the strongest possible means of authentication. Some of them may be suitable for application within the context of a smart office, while some go far beyond this goal or are merely suitable for authentication within information systems. Nevertheless, the contents of this article have to be considered when making a selection for technologies which could possibly be used in the office of the future.

5.3 A Focus on Innovative Authentication Methods: Location and Gait

In the previous section, many authentication methods were already identified. Most of them speak to the imagination, as they are already implemented on a wide scale. Some other authentication methods might still be quite novel, such as the use of an iris scan or face recognition, but have been quite common in science fiction for decades and are therefore easy to understand for most people. However, some of the other introduced novel authentication methods such as the use of gait or location tracking are likely to be unknown. This makes sense, as the literature reviewed in Section 5.2 does not even go that deep into these two topics. They are, however, very interesting. Especially when looking at authentication methods which are as least intrusive to one's day to day life as possible. What follows is a more focused review on the topic of using gait or location tracking for authentication purposes. Goal is to determine what the state of development is, what technologies are used to implement it and what the main reasons are why this is not yet widely implemented.

Once again the academic literature search engine of Google Scholar is used, since this was also done in the previous literature lookups to ensure consistency. The keywords

"Authentication System" AND "Location" and "Authentication System" AND "Gait" were used. Search results were limited to being a maximum of 10 years old. This is done to ensure that modern technologies are used, as well as to limit implementations which require a significant amount of additional hardware: the smartphone emerged as common technology around 2010. Both these search queries provided a significant number of result, although the search query regarding "gait" resulted in only a few thousand results, where the search query revolving "location" resulted in nearly sixteen thousand results. This makes sense, as location positioning technologies such as GPS have been around for decades, while IoT, smart devices and smart wearables are still a relatively emerging technology. Once again, a narrative approach is taken in selecting the literature based on title and abstract content extraction.

5.3.1 Location Based Authentication Systems

Location based authentication systems make use of the wireless connectivity chips inside smart devices such as smartphones or smartwatches to track one's individual location. This is, of course, not sufficient when wanting to authenticate an individual user for access to a system, room or building. This estimated location at least has to be linked to a unique identifier of a certain to device to at least ensure that the location is coming from the device it is expected to come off. Consequently, it can be expected to come from the user which is the rightful owner of the device and therefore be allowed to be authenticated. There are different ways to achieve this goal, depending on the security requirements. For example, being authorized to the temperature control of a room is of much less importance than be authenticated to the company's IT infrastructure. In literature, two main approaches are presented: use of coordinates or use of ambient network information.

When thinking of location based authentication, the use of the GPS module in a smart device instantly comes to mind. And, in some cases, this could be sufficient when combined with some additional parameters. However, GPS is only accurate up to several meters and can easily be spoofed. Kawamoto et al. (2017) tries to resolve this issue, by making use of ambient information collected from numerous wireless networking access points and other networking devices around the building. Examples of data collected from these devices could be its Media Access Control (MAC) address, a unique identifier for each device within a network, the Service Set Identifier (SSID) of a connected device, a naming method for wireless networks, and lastly received signal strength. The principle that the authors use in their research, is that the combination of this ambient information can be unique for select locations. This principle can consequently be used to identify and authenticate a user which requests, for example, access to an advanced security part of a building complex (e.g. a military grade environment). The ambient information collected by the authentication system can be matched with similar information sent by the user, which claims to be present at a specific location at a certain moment. If the information from both client and authentication server side matches, the presence of a user can be guaranteed and access may be granted. An example of how such a system a system architecture could look like is presented in Figure 4. For optimal functioning of such a proposed system, a fine-meshed wireless network system is of course preferred. However, such networks are already quite common in commercial real-estate buildings, with often having more than 1 wireless access point available to users at each given time (albeit sometimes made invisible to the user). This provides an additional advantage, since minimal investment costs have to be made on the aspect of hardware and installation. Constantly collecting data from users may, however, come at significant performance costs which have to be taken into account.

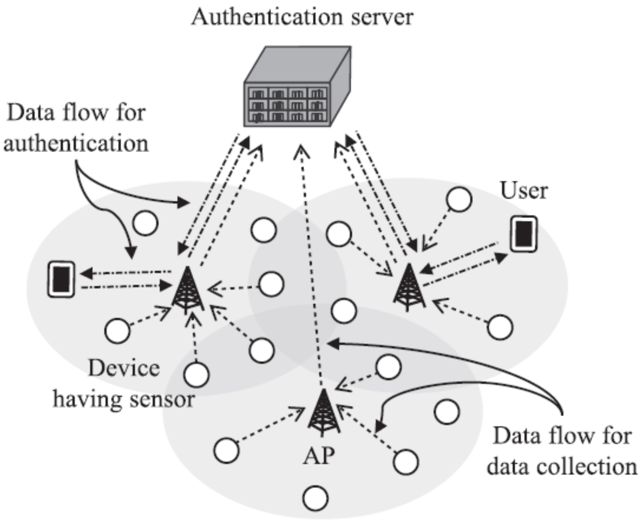


Figure 4: Example architecture of the proposed authentication system (Kawamoto et al., 2017)

Fridman (2017) does instead make use of GPS localization technologies when the user which wanted to be authenticated was situated outdoors. When indoors, the authors resorted back to the use of Wi-Fi for accuracy reasons. According to the authors, no previous attempts were made to make use of the GPS chip for continuous authentication purpose prior to the release of this article. The authors combined the location data gathered from either GPS or Wi-Fi with three other biometric modalities to ensure accurate authentication for mobile devices: text entered via the soft-keyboard, use of applications, and websites visited. The combination of these four modalities proved to be very effective, with minimal false acceptance rates. Surprisingly, the single modality of location (a GPS coordinate) had the lowest false acceptance rate of all the individual modalities. Or in other words: in most cases the use of a single GPS coordinate was sufficient to correctly verify a user with a false acceptance rate of under 10%. The false rejection rate was even lower, being only 5%. Depending on the security levels one wishes to achieve, this could be sufficient and therefore prove to be a useful and viable option to implement non-intrusive authentication for multiple applications.

These two methods of authentication through either Wi-Fi or GPS can of course be used for on-sight authentication. However, its main use might quite possible lay elsewhere. A great example of where this approach could be used is in a work from home situation. Such a scenario has been explained thoroughly in Takamizawa and Tanaka (2012), in which an asynchronous learning environment is used as the example context. To be able to verify the identity of a student taking an exam, without having to resort to proctoring software which might be found privacy intrusive, the student's location at time of taking the exam is compared with the location records of the student as found in the database of the educational institution. If the student's GPS coordinates roughly match those as known in the database, the student is verified and allowed to continue in taking the exam.

This approach could be used as an additional verification mechanism when working from home wishing to log in to the company's network infrastructure. This method of authentication can possibly be extended, by linking it to more unique characteristics such as the network used to send the location information or the unique identifier of the phone that is used to poll the employee's location.

5.3.2 Gait Based Authentication Systems

The aspect of gait based authentication systems was already shortly introduced in section 5.1, through the articles presented by Tao et al. (2011) and Sanchez et al. (2019). Simply put, it aims to create a unique user profile based on the way an individual acts and consequently uses this unique user profile to authenticate a user to open a lock or get access to a system. This can be done in multiple ways, where a basic division between two types of gait-based authentication methods is often made: vision based and sensor based (Divya and Lavanya, 2020). As the name suggests, vision based gait authentication makes use of an image captured through cameras to identify an individual, where the sensor based approach uses sensors either on the body or in the building to ensure identification. In the case of vision based identification, the individual is either identified through separation of the detected visual body image from the background, or mathematical induction through analysis and detection of kinetic movement. A classification of gait based human identification methods can be found in Figure 5.

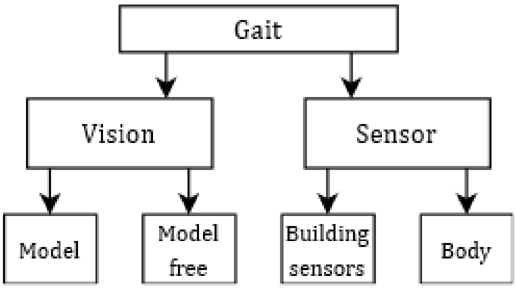


Figure 5: Classification of gait based person identification methods

In case of the latter, the most commonly applied method involves the use of sensors worn on the body. In current days, these are often the sensors within a smartphone or wearable smart device such as a smart watch, as the user is likely to carry this device with him/her in most situations. However, the concept of gait authentication and identification was already introduced some time before the widespread adoption of smartphones in day to day life: Gafurov et al. (2007) already revealed a concept involving a wearable accelerometer sensor to measure multiple metrics. This concept was rather successful: from the different metrics which were tested, absolute distance travelled was measured as being the most accurate with an equal error rate of 7.3%. It was indicated that gait analysis based on wearable sensors is most likely to be useful in the field of application of authentication within mobile devices, where the sensors are already built-in into the device itself. Sensors placed in/on floors, walls or ceilings of buildings are indicated to likely be more applicable for PACS. Consequently, the user experience could be improved by extending the system with an indoor location and direction system, possibly supported by a digital twin building map. On one side, this shows the potential for such non-intrusive authentication systems. On the other side, this also shows that before such non-intrusiveness can be achieved, major changes to buildings may be required to reach the desired level of security. This possibly involves making significant additional costs. Such systems may therefore not be suitable for every organization, even though they might be eager to take the step.

While in literature the potential of gait based authentication for smart devices is widely recognized, only little is known about the possible uses for authentication in PACS. As indicated by Gafurov et al. (2007), vision and building sensor centered gait based identification systems are likely the better option in these contexts. Besides the concept which makes use of infrared sensors installed into the ceilings of buildings, as explained in Tao et al. (2011) in Section 5.1, a few other concepts were presented in literature. An example of a concept implementation of vision based gait identification was presented in Sudha and Bhavani (2011). Results of their research showed a promising future for gait characteristics as a unique behavioral feature of individuals. The concept implementation as presented in the article confirmed this, with adequate accuracy of nearly 98%. However, the results were presented with some serious side notes and limitations. For instance, it was unlikely that the concept identification and authentication system would suffice in a real life scenario as the implementation only functioned from a single camera stand point. For correct gait based identification, the person should always present a side view to the camera, something which seems unthinkable in any non-experimental context. It is indicated that the concept and algorithm which analyzes the characteristics should be extended to work in situations where a person moves at an arbitrary angle to the camera.

That vision based gait authentication systems show promise, but are still prone to various attacks and furthermore still significantly flawed, was also confirmed by Masood and Farooq (2017). The authors indicated that the necessity for a full viewing angle was still one of the main issues when designing such a system, even though the article was presented six years after the concept as was presented in Sudha and Bhavani (2011). It is argued that security cameras provide a “self-occluded view” of the human body. Or in other words: the identified bodies look like a small cross section area of a full body, instead of an actual full body, which is necessary to perform adequate gait characteristics extraction and analysis. A solution, however, is proposed as well, albeit it still experimental. By casting multiple shadows upon the subject through IR light, consequently captured by IR cameras, the visible body image can be enlarged without the system becoming more intrusive to the user. While making the system quite a bit more complicated, it is an interesting and novel solution to an otherwise difficult problem nevertheless.

5.4 An Overview of the Identified Authentication Methods

In the literature as reviewed above, various authentication methods are presented. What follows is an overview of the mentioned authentication methods. The authentication methods as found in the table below are generalized; that means that various variations which incorporate a certain technique, e.g. fingerprint, are not individually mentioned (like has been done in Table 4). As the division between inherence, knowledge and possession was a recurring theme across most reviewed articles, this division is once again maintained. The authentication methods are presented in alphabetic order.

	Used method of authentication
Knowledge	Cognitive authentication
	PIN (Personal Identification Number)
	Codes/Text based passwords
	Visual/graphical passwords
Possession	(Printed) Barcodes
	Mobile Smart Devices
	One Time Password (OTP) Tokens
	Smart Cards (or other ID based methods using digital tags)
	Traditional metal keys
Inherence	Brain activity
	Face biometrics
	Fingerprint scan
	Gait biometrics
	Hand gestures
	Handpalmprint biometrics
	Heartbeat
	Iris (from an eye) biometrics
	Knuckleprint biometrics
	Location
	Typing (keystroke) dynamics

Table 5: An overview of authentication methods

6. Defining the Stakeholder and Requirements of Office Real Estate

To be able to take into account which different requirements a smart office building, or an office building in general, has to fulfil, one first has to identify the different stakeholders which are involved in office use. This question can be approached in the broadest sense possible, but some limitations have to be set due to the scope of this research. First of all, it has to be noted that the indirect stakeholders of real estate are to be disregarded. These so-called external stakeholders are anyone not directly involved with the building. These are stakeholders such as nearby residents. These stakeholders are affected by the presence of the building, but do not make use of it or are invested in it in any way. Taking into account the requirements of these stakeholders when implementing features to create a pleasant user experience inside the office makes no sense, and would only incur additional costs. Furthermore, some stakeholders can be generalized into one stakeholder. From the point of view of performance, for example, the owner and investor of the building could be identified as being the same entity. Both parties have the same interest: making the building as interesting as possible for (some of) the other stakeholders involved. Otherwise the building is not interesting to rent out or use, and therefore will not become profitable, making the investment or ownership of the building worthless and a significant liability.

Identifying the stakeholder and their needs is done by means of consultation of literature. Popular literature is used since scientific literature did not bring up any useful results. This makes sense, as stakeholder analysis of office use is not a topic worth of a scientific study, but more part of one's personal business plan. Furthermore, common sense and knowledge is used to fill in some of the gaps, based on clues provided by the sources used. Examples of search terms which were used relate to needs, demands, requirements and standards and regulations for (users of) the real estate sector. The requirements for general office use should consequently be combined with requirements which specifically focus on the use of authentication systems, to see if the combination of these can be fulfilled.

6.1 Defining the Main Stakeholders

Taking into account the limitations to this scope, one can immediately define four stakeholder groups for each and every office building:

- **Office workers:** First and foremost, the end-user of the building, commonly known as the office workers. These are either private contractors or employees of a larger organization which owns or leases the building.
- **Real estate leaser:** This automatically introduces the second stakeholder group, the organization or individual which leases the real estate from a property owner or larger real estate investment/management organization.

- **Property owner:** When the building is not owned by the party making direct use of it, another stakeholder group is the earlier mentioned property owner or real estate investment/manager organization.
- **Supporting stakeholder group:** Perhaps most important is the service provider stakeholder group (or the supporting stakeholder group), which provides services to each of the above mentioned stakeholders.

Of course, the different stakeholders group may overlap. As an example, take an executive board of an organization which orders to buy, construct or renovate a property. Additionally, take into account that this organization is the sole initiator of this real estate acquirement, construction or renovation project, and has the intention to use it as an office building for its employees. Then all of the boxes are checked by a single organization, or even a single individual employee. After all, the executive board has to have a place to work as well, and thus they are a direct stakeholder of proper design of the office property. This is, however, highly unlikely as major real estate projects are often realized through the involvement of real estate investment organizations and switch ownership quite often. As an example, the in 2014 developed world famous smart office building occupied by Deloitte, The Edge in Amsterdam, has already had two owners in its short lifetime. It is now owned by German real estate investment organization Deka Immobilien, where it was previously owned by Netherlands based OVG Real Estate (RTL Nieuws, 2014).

The supporting stakeholder group likely profits the most from smart innovation in the office area. This stakeholder group includes service providers such as cleaners, catering services, emergency services such as firefighters and maintenance workers. By having access to additional data such as occupation rates, which doors are closed and which are open or which room or sanitary facilities are used more intensively, efficiency and service quality can be significantly increased.

These three stakeholders and the supporting stakeholder group which are relevant for this research relate to every simple ordinary office. It was indicated that other external, less directly involved stakeholders would be excluded from the scope of this research. However, as this research revolves around the concept of the smart office and the research is conducted in collaboration with an organization involved in developing smart office technologies, this last stakeholder must of course not be forgotten. This is, unsurprisingly, the provider of the smart office technologies. The stakes of this technology supplier are of course largely dependent on the requirements of the previously mentioned stakeholders. When the requirements of these stakeholders are not met, or are met insufficiently, competitors may come in and take over the contract. This makes it all the more important to correctly identify the requirements of these stakeholders.

6.2 Finding the Basic Stakeholder Requirements

When designing an office building, requirements of the earlier mentioned stakeholders have to be taken into account. What follows is an analysis of requirements based on each stakeholder perspective, including the obvious aspect of legal requirements applicable to anyone in a certain environment.

6.2.1 Basic Legal Requirements

First of all, some requirements are not there by choice. Basic legal requirements for the workplace as defined and enforced through local regulations have to be fulfilled. These often relate to ensure health and safety on and around the workplace. An example of this is the requirement of the minimum measurements for each individual workplace, or minimum space between desks. In the Netherlands, such space requirements are managed by the NEN, the Stichting Koninklijk Nederlands Normalisatie Instituut (Dutch Royal Foundation Institute for Normalization). The exact requirements of this Dutch norm can be found in NEN 1824:2010 (NEN, 2010). These requirements are there to protect the employee, and are there for the employer to adhere to. Next to that, there are the obvious requirements in respect to the property itself, building regulations, which apply when you plan to refurbish, build, demolish or occupy a building. In the Netherlands, this is laid out in the so-called Building Decree (Bouwbesluit), of which the most recent version has been published in 2012. When compared to earlier versions, increased focus is put on energy saving measures (Rijksoverheid, 2012). Of course, when you are the tenant of the building, these regulations are often the responsibility of the owner of the building, as one may expect a building to be adhering to set standards.

6.2.2 Office Worker Requirements

What is required, however, is not always what the people want. The requirements of specific employees are at least as important, this as they influence the requirements of all the other stakeholders. After all, without employees, no functioning organization. To attract employees, an attractive workplace is a necessity. It is, however, not always clear what people want. A gap exists between what organizations think they have to provide and what employees deem to be important. Furthermore, an employer can only do so much to make a workspace attractive. How one experiences its job is primarily related to content of the job itself, interaction with coworkers, recognition and other more socially oriented aspects (Sid, 2020). However, the employer does have significant influence on improving the wellness of his employees. To do this effectively, surveying workers is key.

This has been demonstrated through a Harvard study relating to wellness on the workplace. It was indicated that employers were expected to spend an average of 3.6 million dollars on wellness programs in 2019, such as onsite gyms, standing desks and promoting a healthy lifestyle, as employers felt this was important. This makes sense; a healthy employee is a more productive employee, is a cheaper employee. However, this study suggests that these wellness programs often yield unimpressive results (Miller, 2019). To find out what employees actually do find important in the workplace, Future Workplace (2019) surveyed 1601 workers across North America. Results indicated that basic perks were found to be viewed as much more important than extensive wellness programs, with air quality and comfortable light comfortably leading the charts. Elements such as fitness facilities and tech-based health tools, as often found in smart office buildings, were not deemed to be important at all. Complete results can be found in Table 6. These results can be important when determining what to invest in first. Furthermore, it should be noted that the deemed lack of importance of tech-based health tools does not mean that there is no place for smart solutions around the office. As long as they are not a goal, but serve a purpose. Smart office solutions could help achieve the other wellness perks. An example of this is an advanced Heating Ventilation and Airconditioning (HVAC) system, which can significantly aid in improving the air quality and room temperature, or smart lighting which can adjust lighting to environmental conditions or personal preferences. The importance of personalization of environment conditions is also found in this study. Home automation products are becoming more and more common, and employees are beginning to expect to have these personalization privileges at the workplace as well. More so, between 42% and 28% of surveyed employees would rather have such personalization than a paid vacation. Personalization can be as simple as being able to adjust the room temperature using the thermostat. However, this only works well if it is a private room. When it regards an open floor plan, and the desk one is using varies between office visits, this becomes much more complicated. Subtle adjustments have to be made which have to be applied locally. Preferably on desk level, and preferably without much of a hassle. This is where identification and authentication may come in. Imagine having some kind of authentication method (smart device, NFC, card reader or fingerprint scanner) installed on every individual desk, connected to a central server containing each employee's personal preferences. Such a system could enable instant adjustment of one's work spot, simply by swiping a card, putting a phone down or touching a scanner. This might even be established by making use of localization of a device, as explained in Section 5.3.1.

Wellness Perk	Importance
Air Quality	58%
Comfortable Light	50%
Water Quality	41%
Comfortable Temperatures	34%
Connection to Nature	30%
Comfortable Acoustics	30%
Healthy Food Options	26%
Fitness Facilities	16%
Tech-based Health Tools	13%

Table 6: Workplace Wellness Perks that Matter to Employees (Future Workplace, 2019)

Continuing on the aspect of office organization and personalization, a survey by Clutch found that of the 503 workers which participated in the survey, 52% preferred having a personal private office. This was followed by an open floor plan (28%) or cubicles (20%). Furthermore, the presence of a variety of types of office space within a building was found to be appreciated as well. Examples of this are, besides private offices: meeting rooms, collaborative spaces, places to relax and space to work in silence. This is especially important when an office is designed using an open floor plan, as communication and collaboration might profit from this concept, but working alone in focus might actually suffer (Herhold, 2019). In Europe, results are likely to differ since cubicles are less common. Private or shared offices are much more common, with open floor plans following on a significant distance (Pouwels, 2020).

6.2.3 Employer Requirements

It might seem obvious, but an employer is happy when its employees are happy. But for the employees to be a happy, you first must have employees. And in this day and age, for some professions at least, this can prove to be very difficult. This is called the "war for talent", which refers to an ever increasingly competitive playing field for hiring and retaining talented (soon to be) employees. This term was first mentioned by Steven Hankin, an employee of management consulting firm McKinsey & Company (Chambers et al., 1998). Sectors in which the war on talent is clearly visible are sectors which show increasing demand along with a slower increase or even declining supply of trained workers. An example of such a sector is the IT sector, in which graduate students have a significantly higher chance of finding a job in a short period of time than other, more traditional sectors (Randstad, n.d.). The technical sector in general has been one of the most competitive sectors over the past decade. This is expected to only increase, as through automation over 50% of professions is projected to have disappeared by 2030. The professions that remain require increased creative, social and emotional intelligence, something your average worker might be not capable of (Andrew et al., 2014).

But what does this have to do with requirements of an employer looking to move into a new office? Simply put, it has to beat the competition. And since the competition is fierce, it has to try to beat the competition in any imaginable way possible. An office which suits to the needs of the (future) employees and distinguishes itself from the competition helps to recruit and retain talent. This has also been demonstrated through a joint research by CBRE (an international real estate company) and the University of Twente, conducted in 2017. Over 120 employees were closely monitored for a period of seven months. Their workspaces were manipulated by including more plants and improved lighting, as well participants being encouraged a healthy lifestyle. Results were astonishing, with energy and happiness levels rising, as well as employees feeling more healthy. Participants indicated they were glad that the company cared about their employees' wellbeing. This authentic message is indicated to contribute positively to creating a stronger employer brand, increasing the opportunity to attract talent. It is argued that this is even more the case for the current and coming generations, Generation Y and Generation Z, as they are more focused on quality of life than previous generations. An attractive office is no longer "just a cool building", it is an environment which contributes to the wellbeing and quality of life of everyone working in it (Nelson et al., 2017). This aspect relates closely to the requirement of "image of high technology" which was mentioned by So et al. (1999) in their Quality Environment Modules, as discussed in Section 3.2.

Besides this, the employer obviously benefits from motivated, productive and efficient workers. This is all achieved by fulfilling the requirements of the employees. That being said, in some sense, the employer has the same requirements as the employee. However, the employer also has an additional aspect in mind: costs. If it is possible to cut cost and still largely is able to fulfil the requirements of the employees, it will likely consider this. Especially when the organization is not operating in a high demand low supply employee market. For example, if employees can and are not against working from home, reducing office space is an efficient way to cut back operational costs. In contrast, as indicated in previous section, investing in gym equipment while no one is really going to use it is a poor financial investment and a total waste of increasingly becoming more expensive office real estate. It is clear that optimizing the workspace is key, and that an optimized workspace is clearly a requirement of the employer. Of course, the aspect of optimization has many sub-requirements hanging below it. It is, however, often difficult to assess how workspace can be optimized. Insight in how the office is used can significantly change the requirements of the employer. Furthermore, this is an ever changing subject as technological, cultural and generational changes contribute to a changing view of how workspace is used. Use of workspace should therefore constantly be monitored. Installing systems to be able to monitor the workplace could therefore be installed, next to the earlier mentioned method of periodical surveying. Examples of this are sensors, cameras, authentication systems and computer use monitoring software. Occupancy data or the frequency of which a door is requested to be unlocked may be translated to a heat map on a digital twin, indicating frequently used spaces or hallways. By analyzing data, changes in office use can be spotted, changing requirements can be formulated and change can be put through. This, however, imposes some additional issues upon the employer which have to be taken into account, as this could be seen as an invasion of one's privacy.

6.2.4 Property Owner Requirements

The property owner has similar requirements as the employer. However, in this case the subject is not a human being, but the property itself. It has to make sure the property is interesting for a potential tenant or buyer. How important this is totally depends on the saturation of the local market in terms of property availability. Offices in the economic heart of major cities are likely to be much more in demand than offices situated remotely in an industrial area. Especially for property owners focusing on this last type of real estate, making sure your building distinguishes itself from the competition is one of the prime priorities. This situation is supported even more by recent numbers from research conducted by real estate company JLL, regarding the occupation rates of Dutch office buildings. As of November 2020, around 8% of Dutch office buildings is unoccupied. This number is based on the country in its entirety. When comparing this number to the capital of the Netherlands, Amsterdam, only around 5% of office buildings is unoccupied. And a building shortage is predicted, with demand for the largest and healthiest buildings likely to increase even more (JLL via BNR, 2020).

6.2.5 Service Provider Requirements

Perhaps the stakeholder group which can profit the most from innovations at the work environment is the service provider stakeholder group. This includes, for example, cleaners, catering providers, emergency services, maintenance personnel and information and communications technology (ICT) staff (OCC, 2020). The environment they are working in should be tailored to aid the tasks they are performing. This is in the interest of both the party that is paying these service providers as well as the people working for these third-party service providers so that they can excel in what they are doing. Since it is a third-party provider, it comes naturally that some expectations are in place relating to the availability of basic provisions. Literature regarding requirements of this stakeholder group is scarce. Therefore, assumptions have to be made based on logical thinking and common knowledge.

Knowledge about the context one is going to perform its services in is one of these basic necessities for performing a job right. This is therefore likely an important requirement. This applies to a broad category of service providers. In all cases, the client aims to get the highest quality for an as low price as possible. Efficiency therefore is key, and contextual information helps to increase efficiency. This has been recognized for several decades now, and lies on the basis of Supply Chain Management theory (Stanford, 1999). Take for instance the scenario of hiring a catering company for the in-house canteen or restaurant. Based on building occupancy data, one can determine how many lunches have to be prepared. Sensors or location tracking systems installed for authentication might be used for this purpose, killing two birds with one stone increasing the investment value. This is the case because it eliminates food waste, as well as reduce personnel cost as this can be adapted to the demand. Continuing in the same sense, it is not check a coffee machine for refill if it has not been used for the past couple of days. In that case it is better to just skip servicing that specific coffee machine at that moment, and spend time on other tasks that still have to be done. On the other hand, when a machine needs more regular servicing, the necessity for this can be spotted before problems arise if information regarding this is available. The same can be said for technical or building maintenance personnel. For instance, imagine replacing a light bulb because it is expected to reach its maximum burn time soon. Without proper knowledge of the amount of burn hours of lighting, lamps might be replaced too soon or too late. This is unwanted for both economic and environmental reasons. Knowing that only a small number of people have accessed a certain room over a certain amount of time could give an indication of the bulb's life status, without the need of smart lighting equipment. Besides that, it wastes costly labor time as replacing thousands of lights is a labor intensive task. By having data about usage of specific rooms, maintenance or cleaning can be done through means of a dynamic schedule, reducing costs significantly.

Of course, it totally depends on the contract whether efficiency is desirable for the service providing company. If a company performs work based on an hourly rate, efficiency is unlikely to be a top priority. In contrast, when the company works on an outcome based rate, efficiency is key as employees can be used elsewhere to increase revenue. This is something that has to be taken into account. In all cases, it is likely that the contracting party benefits from high efficiency, as it may reduce costs, as well as minimize any unwanted nuisance caused by the service provider performing its job.

Another important third-party service group is the group of emergency services. Buildings have to adhere to certain regulations with respect to availability of emergency response tools accessibility of emergency services in case of emergencies such as a widespread fire. For office buildings, these regulations can be relatively basic. When it regards the more industrial sector, more severe regulations may apply, sometimes even demanding to have a personal on-premise fire brigade. Even though regulations may apply, the actual execution is often reliant on human behavior, which is prone to human error. Regulations may prescribe that a certain entrance must not be blocked at any times, or a specific door must be unlocked at any time. However, what is prescribed does not directly describe reality (Davies & Adams, 2015). Information about the current status of emergency aspects such as blockage of hallways, lock status of doors or presence of smoke in a certain room can be crucial to determine the best approach for emergency services to help in a situation. This is especially an aspect where well-implemented authentication technologies can assist in making one’s job easier.

6.3 The Requirements Summarized

Below one can find an aggregate table which includes the requirements of each of the stakeholder. This should provide a clear overview of what has been found in literature. The legal requirements are not included in the overview for the simple reason that these differs drastically between different countries, states, provinces or even cities and are a given non-negotiable fact.

	Requirement	**Description**
Employee	Wellness	Relates to environmental conditions such as air, lighting and water quality. Less important aspects include food options, fitness facilities and health tools.
	Personalization of workplace	Relates to being able to control these environmental conditions on a personal level.
	Private offices	Relates to the significant preference of having a private office versus an open floor plan or cubicles.
	Variety of workspaces	Relates to offering a variety of workspaces besides the one where someone's desk is situated. Examples of this are meeting rooms, collaborative spaces and places to relax a little.
Employer/leaser	Distinguish itself from competition	To be able to distinguish itself to attract employees in a competitive market environment, one has to offer comfortable working conditions. That is: a building which contributes to the wellbeing and quality of life of its employees.
	Insight in needs	Relates to knowing what employees want, and therefore being able to anticipate on this demand to create comfortable working conditions. Can be achieved by surveying and data gathered from sensors and IT equipment.
	Cost efficiency	Closely relating to previous point in this table, cost efficiency can only be reached by knowing where to invest and where to cut costs. Investing in gym equipment is seemingly a waste of money, while investing in a new HVAC system could be worthwhile.
Property owner	Distinguish itself from competition	The property owner wishes to sell or lease out his/her property. In some regions, this might be easy due to high demand. However, for low demand areas offering a property that distinguishes itself from the competition could be a must. Having high-tech authentication technologies on site might contribute to a distinguishing image.
Service Provider	Availability of basic provisions	Relates to the party hiring this stakeholder group having to tailor to the basic needs of the service providers.
	Knowledge about the working context	To perform a task well, it is necessary to have knowledge about the context they are going to work in. Flow of information from and to this stakeholder group is therefore key.

Table 7: Overview of the requirements of stakeholder groups

7. Requirements for Authentication

Besides the requirements set by stakeholder groups for office use in general, basic requirements focusing on the potential solution to some of these issues have to be addressed as well. Since this research focuses on the use of authentication systems as a partial solution to these requirements, the requirements relating to authentication systems need to be elaborated upon. Of course, the important aspect of security directly comes to mind. However, there are many other requirements that have to be taken into account. These are requirements which primarily relate to the aspect of usability. An example of some of these requirements was already given in Figure 3, in Section 4.2.1. Unfortunately, when one wishes to fulfill a usability requirement on one hand, this often comes with a security trade-off on the other hand. What follows is an analysis of general authentication requirements as found in literature, followed by some additional requirements derived from the conducted semi-structured interviews as conducted through the methods explained in Section 2.2.1. Once these requirements have been laid out, the final decision making model can nearly be constructed.

7.1 Basic Requirements for Authentication

In literature, a standard division for authentication between so-called physical and logical access control systems is made. Physical access control is self-explanatory; this encompasses physical access to buildings, rooms, safes and more. Logical access control is defined as virtual access, or in other words, access to data or information systems/services. Since the digital and physical world are slowly melting together, especially in the office of the future, requirements of both physical and logical access systems might be important for this research. As such, the requirements which are deemed to be relevant are addressed in the following sections.

For access control systems often the initial questions when determining which solution is right relate to the context it will be installed in. A system for a single office building drastically differs from a multi-site enterprise or a football stadium. Therefore the following context-based requirements may be in place (BSIA, 2016; OpenPath, n.d.).

Level of security: will the system be installed in a low, medium or high security site? In a low-security situation, where everyone is authorized for access to the entire building, a less complex system may suffice. However, if one is dealing with more sensitive information or technology, one may wish multiple security layers with each having progressively more advanced authentication methods. This is the main requirement to take into account.

Throughput: a system which is installed in a context where several hundreds or even thousands of users will have to make use of it in a short period of time, it is unlikely to be preferable that authentication requires a complex procedure. No employer wants to see employees lining up at 7:30 AM in front of a ticket machine to get a ticket to enter the parking garage. This causes delays and decreases the time employees can spend working. The system has to be adapted to this.

Scalability: besides the number of doors and gates that need to be served by the system, there comes more to scaling. For example, if one's business operates on multiple sites. Traditional access control systems require individual servers for every location, and may require users to request access on each individual site. This requires additional employees on each site, which consequently increases costs and workload. If scalability is important, a cloud based remote access system might be preferable.

Budget: as with any investment, the budget must be appropriate for the desired goal. A high-tech solution which is as non-intrusive as possible is of course desirable for most organizations, but may not weigh against the costs that it brings with it or simply not be affordable for the investor.

Continuing, some additional requirements are in place which are dependent on the actual implementation or solution that is chosen. This is often where trade-offs have to be made: for instance, an initial larger investment might lead into lower cost of ownership over the long run. Furthermore, a technically extensive and complex system might be more secure but significantly harder to service when something is malfunctioning when compared to a simple off the shelve solution.

Cost of ownership: everyone wants an investment to last. The first step is therefore to understand what the life expectancy of the chosen system is, and what continuous service of the system and replacement parts for the system will cost. The latter is something where interoperability and open standards come into play, as they might reduce the costs significantly by offering a broader selection of parts to choose from. Lastly, one must not forget the aspect of software upkeep, licensing and maintenance. This requirement therefore consists of a very extensive and complicated set of aspects which all contribute to the total cost of ownership.

Ease of installation: installation of an access control system could require significant work to be done in the building it is being installed in. In some instances where environmental noise and vibrations may disturb activities conducted in the building significantly, this is extremely undesirable. Choosing for an easier to install system may then be preferable and something to take in consideration.

Interoperability: even though this is mostly dependent on the vendor of the authentication systems and not the type of authentication system in general: the vendor ultimately decides to adopt open standards and I/O ports or not. However, this is still an important factor to take into account. Increased interoperability with third party vendors results in a longer lifetime of products (and therefore a more maintainable and sustainable product lifecycle), more flexibility, better throughput times and less errors.

Customer service/serviceability: this is partially dependent on the vendor of the authentication system as well, as the quality of customer service departments between vendors may vary drastically. However, it is safe to say that a more complex product will require more regular service attention, simply because it is more prone to failing. A major factor in this is human error, which is why one might opt for a more traditional system instead of using one's personal smart devices. Using personal devices diversifies the technical portfolio drastically, requiring increased compatibility of a product with a multitude of devices.

In line with these requirements, there is another important requirements which in essence consists of multiple smaller sub-requirements. These requirements all relate to usability (Kainda et al., 2010). It is, however, too simple to write usability down as a single requirement. Usability is different for each context: a fingerprint reader might be seen as perfectly usable for a normal office environment. However, when the context changes to a hospital where hygiene is much more important and surgical gloves are often worn, this suddenly becomes a totally non-usable option. This brings the following requirements which fall under the umbrella which is called usability:

1. Accuracy: does the authentication method correctly authenticate users with an acceptable failure rate?
2. Efficiency: does the authentication method require as less steps necessary (while still fulfilling security and other criteria) to authenticate a user, or can some steps be omitted to make the process more efficient?
3. Skill: does the authentication method require the user to possess significant amount of skill to interact with it, or is it easy to understand and use?
4. Touchless: does the authentication method require physical interaction between the user and the "lock" to authenticate users (and how much)?
5. Keyless: does the authentication method require some form of key to authenticate users?
6. Initial effort: does the authentication method require some kind of set-up process, and if so, how much effort does it take to complete this process?

Of course, additional requirements exist and one can keep de-composing requirements deeper and deeper to create requirements for every smallest user scenario. For the goal of this research, however, it is chosen to not do this and remain on a more global level.

7.2 Additional Findings from the Expert Interviews

Through the conducted expert interviews with the interviewees introduced in Section 2.2.2, an additional requirement has been found and some additional comments and supporting statements for the already identified requirements were provided. The additional requirement as well as an important sidenote to implementing authentication technologies are elaborated upon below.

Privacy: Another important requirement that is becoming more and more important with the rise of biometric authentication methods, according to **Experts 5, 6 and 7**, relates to one's personal privacy, which is often a tradeoff to many usability and security aspects. Novel authentication methods often involve using sensors or cameras, as explained in Section 5. These sensors and cameras collect information for the purpose of authentication, but also data of random passerby. This is difficult to circumvent, simply because the cameras need to be constantly monitoring for efficiency and accuracy reasons. Someone who is willingly and actively using the system can be asked for permission for data collection and processing, as long as the collection and processing remains within the legal boundaries of the rules and regulations applicable in a certain country. A passerby can not do this, making this a significant requirement which may not be disregarded.

While the importance of privacy is quite clear for the end-user, it also poses several dilemmas for the provider of the authentication service. What information do you want to process? What is the purpose of this data processing? What information do we store in our databases? For how long do we store this information? These are just a small selection of questions that need to be considered, and with the rise of privacy regulations around the world this list is likely to become even longer and longer. The importance of thinking about these dilemmas is stressed by **Expert 7**, whose company specializes in face recognition software. He indicated that because of these dilemmas caused by strict rules and regulations, they strictly focus on the development and implementation of the face recognition algorithm. Input is provided by means of a face in front of a camera which is compared with data fetched from a database, based on a picture taken at an earlier moment. Output is provided in terms of a possible match between the camera and stored data: either 1 or 0, match or no match. What the party responsible for the operation of the lock or gate consequently does with this information is up to them. This decision is likely made to not having to deal with that part of the legal system, by moving a certain part of the responsibility towards the purchaser of the face recognition algorithm product. Rules and regulations revolving around privacy are often quite extensive, and complex to completely understand and adhere to. Taking on this challenge and responsibility could significantly increase operational costs.

Fit for purpose/proportionality: This is not really a hard requirement, but more of an important note which was stressed by the experts. There are many novel solutions available in terms of authentication and access control, as has been summarized in

Section 5.4. However, the most novel innovative solutions might not be the most practical choice, especially when looking beyond the single criterium of finding the most non-intrusive solution. Such solutions can often be found in concept buildings showcasing the technology organizations have to offer. Examples of such buildings are The Edge in Amsterdam, The Crystal in London or IBM Watson's IoT Headquarters in Munich. All of these buildings are at least partially used as office buildings, but have the secondary purpose of being an exhibition of modern technology. This is especially the case for the latter two. However, in normal situations, finding the most innovative, non-intrusive solution should never be a goal on itself. One could install hundreds of sensors all around a building and monitor every single movement of employees by using cameras to achieve authentication. However, if this involves having to overhaul the entire building which consequently results in potential long-term disturbance of one's employees general activities, this might be counterproductive. Furthermore, this does not yet even take into account the potential expenses that have to be made to actually realize this from a technological as well as from an organizational perspective. That is, an organization has to overcome the challenges involved in convincing users of the potential benefit of the newly installed technology and persuade them to actively make use of it. Since this might not be achievable in all cases, for example if the novel system might not achieve desired accuracy in all scenarios or because of the earlier mentioned potential privacy issues, an alternative authentication method has to remain present at all times to serve as back-up. Presence of such an alternative method might in turn be even more unbeneficial for the adoption rate of the new technology, since this removes the actual need of technology adoption. Or in other words: "Why use the new system if the old one that I am used to works just fine?".

The experts provided some examples and requests from clients where one overthought security infrastructure and its connection to different platforms, overshooting the target entirely. **Experts 2 and 4** indicate that nowadays, organizations wish to connect everything to each other to ease operations for the user. Authentication is no exception to this: a popular example is the "Sign in with Google" option offered by many websites. However, by connecting everything together, one instantly creates numerous extra security holes. These consequently have to be plugged requiring significantly more effort. Continuing, one could develop a self-service platform where one can manage the access permissions to these different services. This could give the user a false sense of security, as the user may think that he is in total control of his credentials, but instead creates another potential point of attack. For high security sites, this is therefore avoided entirely by creating an offline subsystem not connected to any network connections. Reasons for this are two-fold: it ensures that the authentication system cannot be tapped in to remotely, as well as that the authentication system does not provide access to the internal network where sensitive information may be stored and processed. Such offline security systems are often used in banks, as well as in the organization of **Expert 4**. In the system he described, access cards have to be authorized each day. That is, information is written to the card to grant access to certain areas which is read by the offline lock system. This means that if a card is stolen or lost, it loses access to areas within a day minimizing the chances of misuse. It can consequently be blocked from the system, denying any future authorization or access. The decision to continue using this system was deliberately done, because it served their purpose very well, was deemed to be user friendly enough and therefore there was no reason to upgrade to a more advanced system.

Even though the expert interviews only provided one additional hard requirement, they were still a useful addition in terms of confirming the requirements found in literature. Overall, through the extensive conversations with the experts, most of the requirements were (in)directly mentioned as being important considerations when choosing or designing authentication systems.

8. The (Long-Term) Impact of the Coronavirus Pandemic on the Office

As was already found when researching the exact definition of what an IB is in Section 3, this concept is constantly changing and evolving due to developments on various facets. One of the main drivers behind this changing definition is, of course, technological development. However, as can be seen in previous section, most technologies that are researched and developed are still very much in a conceptual phase. Looking past technological developments, including the influence of other external factors should therefore be done as well. Looking at the most influential events of the past and current year, there is of course one which can and should not be overlooked: the coronavirus pandemic. In this section a brief look is taken at the possible future developments within the field of the smart office building and smart authentication technologies as a consequence of the coronavirus pandemic. Focus is put on and this may potentially influence the requirements of office users. Once these last insights and requirements are determined, the decision making model can be constructed.

8.1 The Potential Disruptive Effect of the Pandemic

At time of writing, the coronavirus pandemic is slowly being pushed back in the United States and Europe, but is still going strong and having its effect on nearly every part of day to day life in most other parts of the world. Actions which one previously would not think twice about such as shaking hands or going to the office for a day's work are now strictly guided, limited or even forbidden by law. Adjustments to day to day life were and still have to be made to counter the spread of the virus. Social distancing and the order to stay inside if possible have likely had the biggest impact of all on conducting daily activities. Where once a room could accommodate over 20 persons, now it is only good for a handful of people. Working from home has become the standard for everyone who is able to. When one goes to work, precautions have to be taken into account, which can sometimes be experienced as very intrusive. This has raised questions in how this might impact the way people work, and will work in the nearby future. Because of these new questions, it has become more difficult to assess the applicability of literature published before 2020 discussing the future of IBs, as the impact of a global pandemic is unlikely to have been incorporated in these publications. Of course, technologies discussed in these articles are still applicable: the technologies do not suddenly seize to exist and development is unlikely to be stalled directly (although focus might be put on other aspects, slowing down the process). However, the way they are to be applied might have changed drastically. Therefore, it is important to understand the consequences the coronavirus pandemic has had on life at the workplace.

For this analysis the earlier introduced stakeholders are used. The stakeholder group of service providers is not individually treated in this section. This would not be possible, as this stakeholder groups consists of an nearly endless amount of type of stakeholders on which the effect of the pandemic differs wildly. For example, it would have no influence at all on emergency service workers since they will still respond to emergencies and do their best to resolve them. In contrast, catering suppliers and maintenance personnel are likely to see a significant decrease or complete drop in workload. While buildings still suffer from decay over time due to the influence of the elements, a lamp which is not turned on due to absence of presence of people in the building does not need replacement. This can, however, not directly be said if there are still some building occupants: a single person will still need a (partially) lighted building. Of course, a general statement can be made that extra precautions have to be taken into account, just as every randomly picked civilian would have.

8.2 Impact on Employees

Before the coronavirus pandemic, the US Bureau of Labor Statistics (2020) estimated that in the Unites States, around 82% of people that were employed did some or all of their work at a workplace outside the comfort of their own home on the days that they worked. In contrast, only 24% of people that were employed did some or all of their work at home (note that overlap between the two groups may exist). In the EU, figures are not that different, with the percentage of employed working from home only being around 9% as of 2019. Statistics for self-employed were significantly higher (Milasi et al., 2020). Continuing, as of June 2020, it is found that 89% of U.S. employees are at least somewhat afraid of COVID-19 in their workplace, and therefore a part of these individuals is now working from home. Either forced, or by their own choice. (Udemy via Robinson, 2020). Labor unions in the Netherlands indicate that as of February 2021, over 60% of the surveyed union members which were unable to work from home, were afraid to contract the disease at the workplace (NLTimes, 2021) The amount of people scared of the virus on the workplace is likely to have decreased over the course of the pandemic, when vaccinations have started. However, these “temporary” changes might have changed the way people think for good. While currently office space is significantly limited due to social distancing, all this office real estate should once again be available for use when the pandemic is over. It is however not at all certain that the entirety of this 82% will return to working from their offices when this can be done. This is mainly due to signals which show that working from home is more productive than working from the office. Reports are that productivity has increased by 47% since March 2020, when lockdowns hit the world economies all around the world. It is indicated that workers are less distracted by colleagues, and work avoidance is going down. Furthermore, time spent on commuting is a time of the past. This can save workers around 8.5 hours a week on average, which can consequently be spent on exercising increasing overall staff health, lowering costs (ApolloTechnical, 2020). All in all, on first glance, this seems like a win-win situation for all parties involved.

Of course, there is always an other side of the coin which deserves attention. Even though productivity might have increased, some other concerns relating to working from home are raised by multiple surveys conducted over the past couple of months. These issues mostly relate to the technical and mental aspects relating to working from home instead of at the corporate office.

Technological Issues

Stanford University reports that that only 65% of Americans had access to an internet connection fast enough of handling video calls (Bloom 2020). According to calculations of Tessares (2020), Europe does not offer any better conditions, with over two-thirds of Europe not having sufficient upload speed to handle two simultaneous video calls. Continuing, over 40% of employees experienced mental exhaustion from video calls while working remotely. 59% of employees reported feeling more cyber secure when working from the office when compared to home, and a similar percentage reported having discussed sensitive corporate information through work related video calls. Even more worrisome, over 10% of workers experienced their video calls being hacked while working remotely, possibly risking leaking this sensitive information. To counter these issues, measures were taken. Among other things, over a third changed their passwords, nearly a quarter upgraded their Wi-Fi connection and over 20% of employees working from home purchased a Virtual Private Network service to increase security of their internet connection. Several other technical issues were reported, such as power outages and hard- and software issues (Twingate, 2020).

Mental Strain

On the mental side, a survey conducted by scheduling technology firm Doodle under over more than 1100 U.S. employees indicates an alarming amount of burnout symptoms occurring among employees working from home. It is reported that, after a week of virtual meetings, 38% of employees feels exhausted and 30% feels stressed. Continuing, employees feel they are put into a more competitive setting due to increased performance anxiety and business pressure. 63% Of employees indicated they were likely to record their virtual sessions and replay them to see where they could improve themselves or the contact with their relationships. Furthermore, focus tended to be lower when compared to face-to-face meetings, due to background noise or poor audio quality disrupting the virtual meeting (52%). In 23% of the cases these issues with audio quality lead to miscommunication with clients. Talking in the background was found to be most disrupting, followed by notification sounds from computers or smart devices (Robinson, 2020). It comes with no surprise that especially parents with children at home suffer most from these issues, with 50% of parents with young children thinking they do not work more productively from home (McCann, 2020). A study conducted in Europe (based on remote working in general, not related to the pandemic) shows similar results in respect to negative consequences on the mental health, however, it also highlights that the potential positive effects should not be disregarded. Main issues seemed to revolve around the lack of leadership and lack of interaction with co-workers, as well as increased risk of burnout and loss of work engagement (Kotera & Correa Vione, 2020).

According to WalletHub, however, working from home is there to stay. American workers are generally quite positive about their new working situation, with a third of the questioned workers even believing physical offices have or will become obsolete in the nearby future (McCann, 2020). Furthermore, the statistics as mentioned above might be less meaningful as one might initially think. Burn-outs and other stress related health complaints have always been a significant issue at the workplace. These are not issues which have suddenly arisen due to the fact that everyone has suddenly started working from home. Comparative research specifically focusing on the differences possible statistical differences of occurrence of these complaints between working from home and working on-premise is currently lacking. This makes sense, since a situation where such research could be conducted on such large scale has never really occurred before. Research should therefore be revisited after the global pandemic is over, and workers have had the opportunity to start working on-premise again. This should answer the question if working from home is really better or worse than working at the office, at least in respect to one's personal health.

8.3 Impact on Employers

Of course, not only the employees have to adapt to the new way of working. In some situations there is no other possibility for employees than to come physically to work, even if the employee does not want to. In these situations the employer is tasked with making sure that this can be done in a safe manner. This often requires making adjustments to the workplace. The World Health Organization has set up guidelines for how this should be arranged. These guidelines, although defined in the early stages of the pandemic, are as follows:

- Workplaces should be clean and hygienic, that is, surfaces and objects need to be disinfected regularly.
- Regular and thorough washing of hands should be promoted. Hand sanitizer dispensers should be put in prominent places around the workplace.
- Respiratory hygiene should be promoted as well. This includes the availability of face masks and paper tissues.
- Social distancing should be maintained to decrease risk of virus particle spreading.

These guidelines can be a burden to adhere to, especially when regarding maintaining proper hygiene standard. This requires intense and regular cleaning, which is costly. Developing methods to make this more efficient and standardized take time, and once again, time equals money. All in all this can result in significantly higher costs while accommodating much less employees on-premise. Continuing, even if these guidelines are adhered to, state regulations may still prohibit employees to visit their workplace or there still might not be enough space to accommodate all employees while maintaining social distancing measures. This has brought uncertainty to all organizations, whether small or large. Many organizations have therefore adapted their organizational structure to the concept of remote working. As of Q1 2021, the pandemic is nearly reaching it one year anniversary, and thus remote working is slowly being seen as the new de facto standard (EY Belgium, 2020). This has resulted in large corporations re-thinking the way their employees will be working after the pandemic as well. Or in other words: getting rid of office space, or at least drastically redesign it.

The first signs of this are already showing. An enquiry done by Dutch business to business platform "De Ondernemer" in October 2020 indicated that "whoever is not making any changes in the design of its offices, will have a hard time". Experts predict that the in Europe commonly used open office floorplan is going to disappear, since employees are willing to give up their private working spot, but only if they can trade it in for a more tranquil work environment. This is something an open floor plan is unlikely to be able to offer. The traditional division of 70% work spots and 30% shared space is deemed untenable, with predictions of these ratios having been switched by 2030. Individual working is moved to the comfort of one's home, for whoever this fits of course (De Ondernemer, 2020). This is confirmed by a survey of Dutch news outlet Nieuwsuur, held among 25 of the largest employers of The Netherlands. Half of the companies expects to be using less office space when compared pre-coronavirus times. One of the questioned companies (Triodos, a Dutch bank with a focus on sustainability) indicates that in their new office building, there is room for only 550 employees while the company has around 1000 employees in total. This requires employees to be working from home by design, from one or two days at home pre-pandemic to two to three post-pandemic. The office space that remains is going to be used for face to face meetings with co-workers and clients. Main reason for this, surprisingly, is that it is indicated that their employees are more focused working at home than at the office. Therefore, more space would be redundant (NOS Nieuwsuur, 2021). This in contrast to what is found by both Robinson (2020) and McCann (2020), but in line with the general consensus that remote working increases productivity. This uncertainty is also visible among the other half of the companies which participated in the survey: they do not have the answer as of yet. Some organizations are still researching if downscaling is an option, some expect no changes to occur. If downscaling is an option also depends on, if applicable, the remaining length of lease contracts. Long-term corporate lease contracts of more than 10 years are not uncommon, and thus might throw a spanner in the works. Only a single organization expects to increase their amount of real estate.

In contrast, as was already indicated in Section 4.2.2, employees increasingly value their wellness. Continuing, due to a lack of supply of educated personnel in many areas of expertise, employers have to fight each other to attract the best personnel or any personnel at all. Providing working conditions that suit the needs of the employees is one of the primary ways to bind a worker to one's organization. This crisis therefore creates opportunity for employees to distinguish themselves from the competition. By providing a coronavirus proof working environment, either through the protocols as mentioned earlier at the office, or configurating a well-functioning work-from-home environment, by providing employees with the supplies they need, one can show that wellness is looked after. One could state that this is the least an employer can do in these desperate times, but significant differences exist between doing the minimum and doing the most one can do to make workers feel comfortable in their new working environment. Even though their new working environment is the comfort of their own home. One might even go as far as (voluntarily) monitoring the working conditions of workers at home by using software or sensors, and provide tips or tools to improve their home working conditions. As was already shown in previous section, surveying is already used extensively for this. However measuring air quality by merely using one's subjective observation will always remain quite difficult. Using sensors at home could prove to be a solution.

8.4 Impact on Property Owners

The impact on property owners is less clear. Of course, if the number of tenants or the amount of office space necessary decreases, this has will have some impact on the profitability of commercial real estate. However, due to the in the introduction mentioned long term lease contracts, consequences might not be directly visible. This will likely become visible over time, as lease contract will slowly come to an end and new terms and conditions will be agreed upon. Furthermore, as the crisis is still very much going on, it is still difficult to say how big of an impact it is going to have. What is, however, becoming very clear is that some companies are struggling to keep themselves afloat, and fear bankruptcy (van Barneveld, 2020). This is especially the case for smaller retail companies and businesses operating in the hospitality sector. These are often affected by the various lockdowns instigated by governments all around the world. Some damage is compensated for, but in a lot of instances this is not enough to stay afloat. If companies would indeed have to file bankruptcy, this should at least temporarily result in significantly increased vacancy of commercial real estate. This has a direct impact on the financial situation of the property owners, as revenue generated from tenants evaporates completely. Some revenue might already be lost, as in some situations property owners are working together with these struggling organizations to compensate for the loss in revenue by decreasing the client's rent. Examples of this are seen in the Netherlands, with several beer breweries compensating their tenants (Schouten, 2020). This is, however, something that can not hold on forever. Sooner or later the property owner will want to see the return on investment it counted on when acquiring the property.

Commercial real estate companies could try to mitigate the damage by thinking ahead and redesign their existing properties for the new way of working. This should incorporate the requirements of the employees and employers and focus on fulfilling basic wellness requirements and providing workspaces the post-COVID employee needs. This could mean redesigning an office by tearing down walls between personal offices to create larger meeting rooms or collaboration places. By anticipating on what your future client needs, the potential downtime when the economy will restart again is minimalized. Furthermore, since offices are not really being used at this moment anyway, no downtime is created at this moment in time. Office workers are not being disturbed by construction work, making this the ideal time to perform work for the future.

8.5 First-Hand Experiences

During the semi-structured interviews to determine the requirements for the concept for non-intrusive authentication, the topic of the consequences of the coronavirus pandemic addressed as well. In this part of the interviews, focus was put primarily on three different aspects: which consequences did you experience directly, do you think office use will change due to the coronavirus pandemic (and how?), and lastly how the role of authentication technologies might change due to the effects of the pandemic.

8.5.1 Direct Consequences

In this section, the direct consequences of the coronavirus pandemic on one's work are discussed. This is based on first-hand experiences gathered through interviews with the experts as introduced in Section 2.2.2. Ordinary cases which were affected by the pandemic in the general way (work from home, social distancing, etc.) are not discussed. Only if the person's domain specific operations were impacted these are mentioned.

Since this section heavily relies on the personal experiences of the interviewees, and these experiences are heavily influenced by their different characteristics, these can be found in Table 8, a repetition of Table 1, below:

Expert no.	Categories	Professional role	Years of experience
1.	System level interactor	Front desk employee	35 years
2.	Domain expert	Technical expert access control	20 years
3.	Domain expert	Technical expert access control	20 years
4.	Domain expert/system level interactor	Contract manager for electronics at an educational institution	20 years
5.	Domain expert	Business developer access control	4 years
6.	Domain expert	Technical expert biometrics	3 years
7.	Domain expert	Technical expert face biometry	20 years

Table 8: Summary of Interviewees' Characteristics

Expert 4, a contract manager responsible for electronics, and measurement and control technology at a Dutch educational institution, indicated that the direct consequences for him were quite drastic. This primarily related to regulating access control for the various groups of employees and sftudents which suddenly had to be refused access to the different buildings of the educational institution. Normally, all of the buildings on the campus are openly accessible for most employees and students. Of course, some restrictions are in place for specific parts of buildings such as laboratory spaces and offices. With the pandemic, this all changed. In the early days of the pandemic, this was still quite simple. No one was allowed inside the buildings, unless this was specifically indicated otherwise. Since the number of people which were exempted from being denied access was quite small, this was still manageable. However, when the situation around the coronavirus pandemic changed, more and more employees and students were allowed access to (parts of) buildings. For instance, students studying nanotechnology or chemical engineering were allowed to make occasional visits to the laboratories again. The system which was used did not provide an easy method to identify and allow larger groups of users access to the building, since they were not grouped by their specific occupation. All students or employees had to be granted access individually. As a consequence, it made sense to allow a front desk employee to work on-premise again. Continuously checking for requests to be able to enter a building and having to visit the on-campus security to grant access to the building by loading this key on their personal student or employee card was seen as too much of a hassle.

Expert 1, a front-desk employee of a high-tech company, obviously noticed that the office become much more tranquil. The number of visitors decreased drastically due to the restrictions imposed by the government. Some new employees had not visited the office building since the start of the pandemic, and the identification cards which were prepared for them still needed to be handed out. Surprisingly, the number of phone calls decreased as well; employees and customers were increasingly able to contact each other directly. Being a conduct for the employees was not that useful anymore, as there was less insight in what employees were doing at a specific moment since they are all working from home. Forwarding a phone call to someone working from home has a higher chance of being unsuccessful when compared to someone working from the office, because of possible distractions such as child care. E-mail or messaging through platforms like Microsoft Teams directly between employees was therefore preferred.

8.5.2 Expected Aftermath

Each of the seven interviewed experts was asked about how this person thinks what the period after the pandemic will look like. In respect to use of the office/workplace of course. Although this might not be their direct expertise, it is interesting to see how this compares to the predictions as laid out in the other subsections of Section 7 (and primarily: research as presented in Nieuwsuur, 2021).

Office use

Opinions on how the office will be used in the future differ quite drastically. **Expert 1** indicated that it is likely that at least partially working from home is likely there to stay. She indicates that “we might see working weeks of 2 of 3 days at the office and the rest of the week working from home”. However, she also indicates that for some employees working from home simply does not work or likely works in a less efficient way. This is primarily influenced by one’s individual home situation, family composition and function in the company. Lastly, she indicates that possibly she could perform her job from home as well, although this was less preferred. Employees seem to still like having a central point of contact, albeit only for some small talk or simple enquiries. This was supported by results from the interviews with **Experts 5 and 6**, indicating that having a receptionist radiates some type of professionalism and is therefore key to have in a large organization.

Three other experts on the domain of authentication technologies, **Experts 5, 6 and 7** indicated that the pandemic will have a lasting effect on the way we live and work as well. One of these three experts indicated that corona has been "an accelerant for hybrid working", which he explained as the change process in which life and work slowly blend together. He indicated that he saw this as already being somewhat of a trend before, but that the work from home mandate (instigated by the Dutch government) over the majority of 2020 and 2021 have really put the changes in motion. From his experience, some employers seem to be resistant to these changes, while many other organizations are seemingly embracing this. **Expert 7** indicated that working from home is there to stay, but maybe only for certain groups of employees. He provided an example regarding the programmers of his organization, which often prefer to work in teams to discuss problems they are having when doing their job. However, he also indicated many other tasks within most organizations could easily be done from home. This could also be seen when visiting the office of his organization, which was still largely unoccupied despite many of the work-from-home regulations already having been lifted in the Netherlands at time of the interview.

The earlier mentioned **Expert 4**, the employee of an educational institution, expects to see little difference between post and pre-pandemic times. He indicates that lectures might be recorded more often than they were recorded before, although this was already more of a general trend even before the pandemic started. Generally speaking though, education will likely mostly remain an on-premise physical activity. This makes sense, as the majority of students still prefer to receive physical education rather than online education (Nationale Onderwijsgids, 2020). But again, a hybrid format might prove to be the optimal solution. Two other interviewed experts, **Experts 2 and 3**, which focus on (parts of) the more technical aspects of authentication expect to see little difference as well. They feel that when the virus is under control and largely defeated, most employees will be likely to get back to work in the way that they used to.

What is interesting to note is that the three experts which feel that the pandemic will indeed change the way people will be working in the future, were on average much younger (two of them were still in their twenties) then the experts which feel everything will return back to the way it was. (of which all of them were in their mid-forties to mid-fifties). Even though the amount of interviews is too low to indicate a statistically meaningful relation, it still makes one think if the younger generation perhaps has less trouble adapting to these new conditions.

Impact on (authentication) technology

An event as impactful as a global pandemic is expected be reflected on the use and application of technology in the commercial real estate sector. Because of this expectation, each of the interviewees was questioned about how (available) technology could be used to help countering the effects and spread of the pandemic. Furthermore, questions are asked if, to their knowledge, organizations are changing their focus in terms of development of technologies because of the pandemic.

One of the first topics that was addressed related to tracking of the use of areas or rooms within the building. The interviews gave no indication that access control systems were used with this purpose in mind. **Expert 1** indicates that their organization, which makes use of a keycard system to access areas within the building, is able to view the activity of each of the keycards used by the employees or guest within the building. However, to her knowledge, this is currently not used actively for anything besides possibly security reasons. When suggested that this could possibly be used to monitor usage of rooms such as bathrooms or offices, she agrees that this could indeed be a possibility. However, actual implementation of such a system could be affected heavily by privacy regulations and therefore should be completely anonymized to be of any use. This is supported by **Expert 4**, which organization makes use of keycards for authentication as well. Tracking of card use is supported, but not actively used. Partially because it does not yet have a proper use case, partially because it requires the organization to take many privacy related aspects into account. He adds that this goal can just as easy be achieved by making use of occupation sensors, which are readily installed in most rooms of the organization anyway. Counting individuals could be difficult when making use of this method, however, the same can be said when applying tracking by means of keycard logs: this would mean that doors may never be kept open. This is, of course, not a real possibility for an educational institution where students freely walk in and out of lecture halls.

Secondly, an obvious topic of discussion relates to the transition to the use of more touchless technologies (with a focus on authentication). A majority of the interviewed experts, 5 out of 7 of which all were domain experts and one also fulfilled the role of system level interactor, indicated that the number of contact moments has to be minimized in case of a pandemic and innovation in authentication can play a role in this. For example, interacting with a front desk employee to receive a card may be avoided. Technology can easily realize this, for example through the use of some kind of terminal, but **Experts 1, 5 and 6** still believe a front-desk employee will remain to exist for a multitude of reasons. However, this automatically puts temporary keycards or metal keys which have to be retrieved and returned after each day at a disadvantage. The same can be said about fingerprint readers, because of the moment of contact when interacting with the lock (**Experts 4 and 7** specifically addressed this). More advanced biometric authentication methods such as facial recognition might therefore prove to be the solution. **Experts 4, 5, 6 and 7** see facial recognition or other vision powered technologies as performing a major role in the (nearby) future. The pandemic might have sped up developments in this area. However, privacy regulations put things in a complicated situation and hamper wide adoption of these technologies. Furthermore, regulations require to always have an alternative authentication method available on site. Therefore, its application is currently only considered in very specific situations according to **Expert 7**. These can be high security sites where it may be used in combination with cards as 2FA but also areas where touchless entry is preferred due to comfort reasons. Examples of such a location are gyms, where one often prefers to not bring a bag inside or wear shorts with pockets when exercising, or hospitals as hygiene is extra important here.

Another way of decreasing the number of contact moments between people and surface areas is by making use of personal mobile devices for authentication. Using mobile devices for authentication was definitely seen as technology but high potential by the vast majority of the experts. This is reflected in the number of interviews in which it was specifically mentioned: all domain experts saw some use for the smartphone for authentication purposes. By using a personal device, one could request access to a room, building or area through some kind of (web) application from the comfort of one's own home or when on the road. Consequently one can get pushed a personal access key for access to the requested room. For example, a (printable) Quick Response (QR) code, virtual access card through Near Field Communication (NFC) or Bluetooth security handshake. This, however, might bring with it several issues which will have to be addressed. Firstly, such an application has to be developed and maintained. If an organization is not (yet) specialized in software development and maintenance a department has to be set-up or transformed to do so. Because of the high variety of potential devices which may be used, this could turn out to be quite complex **(as mentioned by Experts 2, 3, 4 and 6)**. On a small scale, for example for internal use, this might not directly pose to be an issue as you can force the use of specific devices. However, when rolled out on a larger scale, support and maintenance can take significant time and effort. Such copious use of resources has to be carefully weighed against the potential benefits the solution might bring with it. Secondly, as **Experts 3, 5 and 6** indicate: adoption of the application could prove to be difficult as well as users have to be persuaded to see the added benefit of such an application. For returning users, if the application in question has to be downloaded and installed on a smart device and registration is obligatory, the effort of this process is likely to be returned over time quite quickly. Continuing, during a global health crisis, where people are used to taking an extra step to prevent contamination with a disease, taking this extra step is likely to be easily accepted as well. However, in normal situations, for an incidental visitor in a time where health and safety is less of an issue, walking up to the receptionist and asking for a keycard takes much less time and will therefore likely remain preferred.

8.6 Summarizing the Consequences

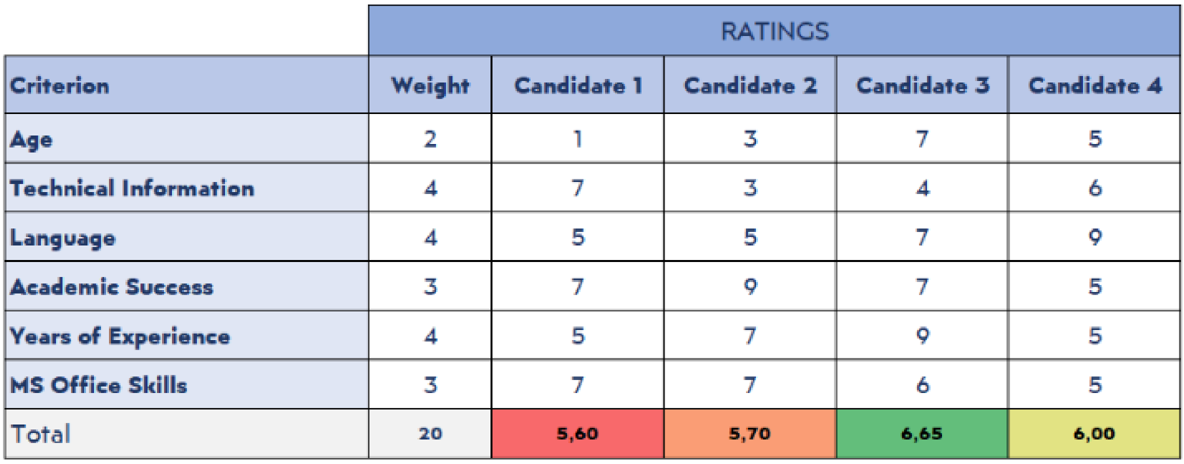
Summarizing, the direct and long-term (expected) consequences of the coronavirus pandemic on office use and the future of authentication can be found in Table 9. Some of the consequences, especially the long-term consequences, are far from certainties and are based on predictions of experts. They should therefore be treated as such, and should only serve as an indicator to base decision making on. It is to be noted that the short-term and long-term consequences standing next to each other have no relationship.

Impact on	Short-term	Long-term
Employee	Fear of going to the workplace because of risk of getting infected	New way of working, emulsification of work and private life
	Obligation to work from home	Desire for a more dynamic and more personalized work environment
	Alleged increased productivity (due to working from home)	Increased focus on wellness perks
	Time savings (due to working from home)	n/a
	Technological issues (due to working from home)	n/a
	Mental strain (due to working from home)	n/a
Employer	Increased health and safety regulations	Transformation of office floorplans and office real estate to support new way of working
	Opportunities to distinguish itself from competition by responding to new employee needs	Opportunities to distinguish itself from competition by responding to changed employee needs
	Direct closure and uncertainty of future due to lockdowns and other restrictions	Uncertainty of future due to the financial impact of past lockdowns and other restrictions
	Having to apply and manage strict access rules	n/a
Property Owner	Temporary decreased number of (possible) tenants due to bankruptcies	Temporary decreased number of (possible) tenants due to bankruptcies
	Benefit from downtime by redesigning office floorplans to support new way of working	Harvest benefits from redesign of office, distinguishing itself from competition
Technology	Touchless exchange of access cards	Possible use of authentication or sensors for tracking of room usage, although this is unsure
	Registration of presence and reservation of desks/working spots at the workplace	Accelerated adoption of touchless authentication methods such as face recognition
	n/a	Possible accelerated adoption of mobile devices for authentication purposes
	n/a	Possible replacement of front-desk employee with a self-service terminal
Office use	Presence of employees significantly decreased	Permanent lower presence of employees. Office is used as a collaborative working space and accelerant of creativity and innovation, in contrast to "just a place to work"

Table 9: Summary of (potential) consequences of the coronavirus pandemic relating to office use and authentication technologies

9. A Selection Model for Non-Intrusive Authentication Methods

By using the information gathered and presented in this research, the primary artifact can now be presented. Over the course of this research, it has become quite clear that a single best solution for and implementation of (a combination of) non-intrusive authentication methods does not exist. The optimal solution is dependent on a substantial number of criteria, and how important each of these criteria are for an organization in its respective context. Therefore, a weighted decision matrix which can be adjusted to each one's individual needs seems to be a more suitable solution. This matrix should incorporate the requirements as identified in Chapters 6 and 7, extended by insights from Chapter 8. Some of the requirements are difficult to directly map to the characteristics of the authentication methods, as they are totally vendor dependent. These should therefore not be included. This is for example the case with interoperability, which completely depends on the implementation, which can be specified to order. In contrast, one can reasonably state that an authentication method dependent on a large number of sensors is significantly more difficult to install than a system using card readers. Therefore, requirements of which one can reasonably say that they can be directly mapped to the characteristics of the authentication methods as identified and presented in Table 5 should be included. Each of these combination of mapped requirements and authentication methods should be given a relative score, corresponding to how well the authentication method scores in this aspect. This score ranges from 1 to 5, with 1 being the worst and 5 being the best. An example of a generic weighted decision making matrix can be found below, in Figure 6.



	RATINGS				
Criterion	**Weight**	**Candidate 1**	**Candidate 2**	**Candidate 3**	**Candidate 4**
Age	2	1	3	7	5
Technical Information	4	7	3	4	6
Language	4	5	5	7	9
Academic Success	3	7	9	7	5
Years of Experience	4	5	7	9	5
MS Office Skills	3	7	7	6	5
Total	20	5,60	5,70	6,65	6,00

Figure 6: An example of a decision making matrix for selection between multiple candidates applying for the same job (Someka, 2021)

The scores given to each authentication method are determined based on the knowledge as presented in previous chapters. These scores will of course never be 100% accurate, as they are an estimation based on the knowledge as found and viewed by the author and could change over time due to varying labor costs and supply and demand of parts and components. For example, at the time of writing of this research, manufacturers worldwide are dealing with a shortage of microchips. This has resulted in prices of products such as computer parts to have sky-rocketed over the past several months, and is likely to have an effect on the prices of chips used in access control systems as well. Estimates are that this shortage is bound to last through the majority of 2022 (Moore, 2021). Because of these fluctuation of scores, the model should allow the scores to be adjusted by the user for it to be useful over a longer period of time.

9.1 Selection of Criteria

As indicated, not all criteria are suitable to be included in the decision matrix. Therefore, a selection has to be made. Let us first look at the requirements for authentication, as defined in Chapter 7. Through the reasoning as provided in the previous section, the following requirements are chosen to be included in the decision matrix:

1. Level of security
2. Throughput
3. Budget
4. Ease of installation
5. Serviceability
6. Accuracy
7. Efficiency
8. Skill required
9. Touchless
10. Keyless
11. Initial effort
12. Privacy

Furthermore, from the stakeholder requirements as defined in Table 7 and elaborated upon in Chapter 6, the following requirement is added:

13. Image (of incorporating advanced technologies) – derived from "distinguish itself from competition"

The extensive table with each of the authentication methods and the corresponding scores for each of the criteria (or requirements) can be found as Appendix A.

9.2 Additional Notes for the Criteria and their Scores

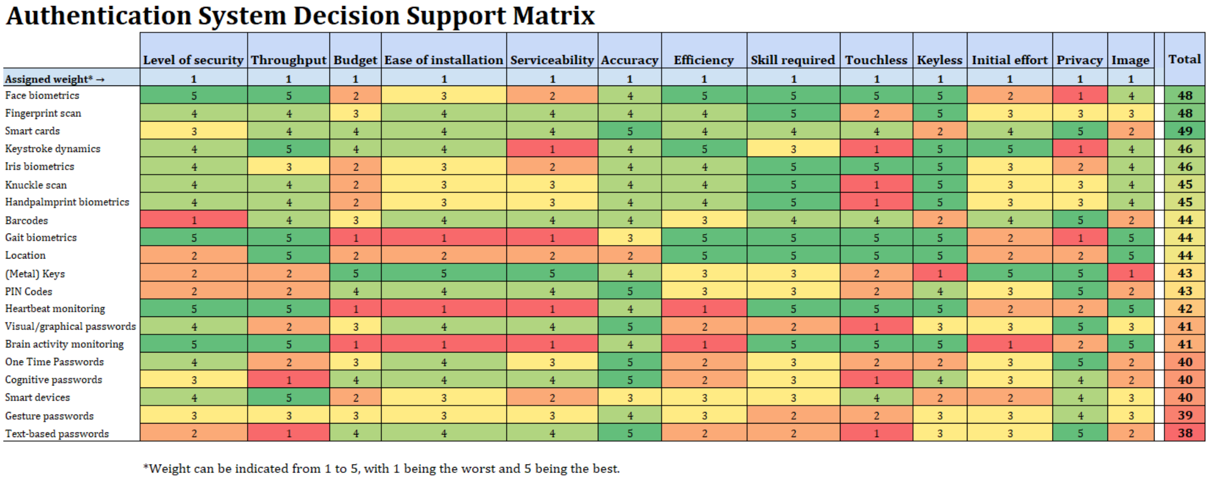
In Appendix A, one can see that some of the authentication methods are annotated with an asterisk (*). This is done to indicate these authentication methods are so-called continuous authentication methods which require monitoring characteristics over a longer period of time to be able to recognize patterns. They are therefore often significantly more difficult to implement for the application of PACS, in contrast to logical access control for which they are often used in current days. This is especially the case for keystroke dynamics, which is a very effective non-intrusive authentication method as well as being relatively cheap. It can significantly improve security of digital accounts when compared to merely using a login-based authentication system, this because such login-based systems can not authenticate users beyond the login screen. Applying this for PACS, however, seems impossible since life does not completely unfold itself behind a keyboard. At least not yet. In the case of heartbeat or brain activity monitoring, the user could potentially carry a device to collect and send/process such data. For monitoring of heart rate this seems viable, as most smart watches are able to accurately do so. In the case of measuring brain activity, this still seems to be lightyears away of being a commercially useful solution. This would likely require the user to wear a headband (for basic measurements) or tens to hundreds of sensors attached to one's scalp (for advanced measurements) to function well enough. It is unlikely users are willing to do this to gain access to a room or building.

Gait could potentially be classified as continuous authentication as well, and rightly so, as it can be implemented as such. However, in the concept as earlier provided by Sudha and Bhavani (2011) and Masood and Farooq (2017) implementing vision based gait it was used to grant access for a single lock making use of a snapshot captured by camera(s) and comparing this with stock footage. Single and multiple camera solutions were used, of which the latter functioned significantly better. When applied throughout a building, making use of a multitude of cameras and camera angles, one could offer a continuous authentication solution which could be used for site-wide PACS. Continuing, the same may be said about location based authentication. However, a snapshot of a single location point is unlikely to be useful for anything more than the most simple verification or authentication levels and can easily be spoofed. To at least be fairly useful for higher security sites the location should be constantly monitored to be able to recognize unique patterns, hence making it a continuous authentication system.

Once again it is important to note that the scores given to the criteria are an estimate based on information gathered through research. The actual scores may differ significantly based on content and implementation.

9.3 Presenting the Model

The weighted decision making matrix model can be found as an attachment to this research, and can be used by anyone wishing to support the decision making process in choosing a suitable (non-intrusive) authentication system for one's organization. An impression of the model can be found in Figure 7, below.



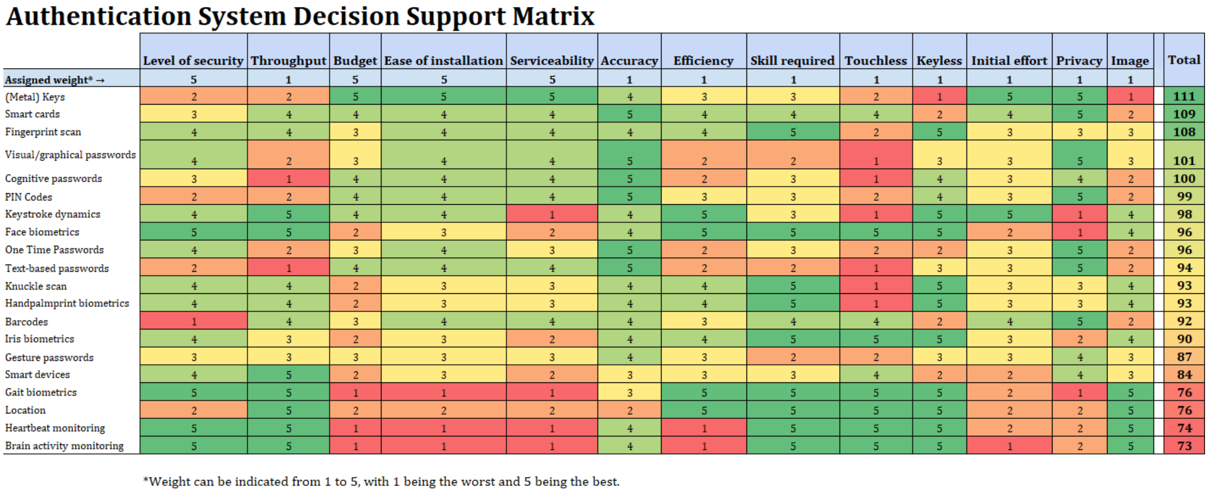
Authentication System Decision Support Matrix

	Level of security	Throughput	Budget	Ease of installation	Serviceability	Accuracy	Efficiency	Skill required	Touchless	Keyless	Initial effort	Privacy	Image		Total
Assigned weight* →	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**		
Face biometrics	5	5	2	3	2	4	5	5	5	5	2	1	4		**48**
Fingerprint scan	4	4	3	4	4	4	4	5	2	5	3	3	3		**48**
Smart cards	3	4	4	4	4	5	4	4	4	2	4	5	2		**49**
Keystroke dynamics	4	5	4	4	1	4	5	3	1	5	5	1	4		**46**
Iris biometrics	4	3	2	3	2	4	4	5	5	5	3	2	4		**46**
Knuckle scan	4	4	2	3	3	4	4	5	1	5	3	3	4		**45**
Handpalmprint biometrics	4	4	2	3	3	4	4	5	1	5	3	3	4		**45**
Barcodes	1	4	3	4	4	4	3	4	4	2	4	5	2		**44**
Gait biometrics	5	5	1	1	1	3	5	5	5	5	2	1	5		**44**
Location	2	5	2	2	2	2	5	5	5	5	2	2	5		**44**
(Metal) Keys	2	2	5	5	5	4	3	3	2	1	5	5	1		**43**
PIN Codes	2	2	4	4	4	5	3	3	2	4	3	5	2		**43**
Heartbeat monitoring	5	5	1	1	1	4	1	5	5	5	2	2	5		**42**
Visual/graphical passwords	4	2	3	4	4	5	2	2	1	3	3	5	3		**41**
Brain activity monitoring	5	5	1	1	1	4	1	5	5	5	1	2	5		**41**
One Time Passwords	4	2	3	4	3	5	2	3	2	2	3	5	2		**40**
Cognitive passwords	3	1	4	4	4	5	2	3	1	4	3	4	2		**40**
Smart devices	4	5	2	3	2	3	3	3	4	2	2	4	3		**40**
Gesture passwords	3	3	3	3	3	4	3	2	2	3	3	4	3		**39**
Text-based passwords	2	1	4	4	4	5	2	2	1	3	3	5	2		**38**

*Weight can be indicated from 1 to 5, with 1 being the worst and 5 being the best.

Figure 7: An impression of the decision support matrix, without additional added weights

At first glance, some of the authentication systems studied seem very similar, with face biometrics having a slight advantage compared to using a fingerprint scanner. However, when adding weights to indicate importance of different criteria to the matrix everything changes. If a budget-centric but secure approach is taken, with maximum focus on the areas of budget, ease of installation and serviceability, the ordinary metal key, fingerprint scanner, smart cards and pin codes appear to be a better solution. This can be seen in Figure 8, below:



Authentication System Decision Support Matrix

	Level of security	Throughput	Budget	Ease of installation	Serviceability	Accuracy	Efficiency	Skill required	Touchless	Keyless	Initial effort	Privacy	Image	Total
Assigned weight* →	5	1	5	5	5	1	1	1	1	1	1	1	1	
(Metal) Keys	2	2	5	5	5	4	3	3	2	1	5	5	1	**111**
Smart cards	3	4	4	4	4	5	4	4	4	2	4	5	2	**109**
Fingerprint scan	4	4	3	4	4	4	4	5	2	5	3	3	3	**108**
Visual/graphical passwords	4	2	3	4	4	5	2	2	1	3	3	5	3	**101**
Cognitive passwords	3	1	4	4	4	5	2	3	1	4	3	4	2	**100**
PIN Codes	2	2	4	4	4	5	3	3	2	4	3	5	2	**99**
Keystroke dynamics	4	5	4	4	1	4	5	3	1	5	5	1	4	**98**
Face biometrics	5	5	2	3	2	4	5	5	5	5	2	1	4	**96**
One Time Passwords	4	2	3	4	3	5	2	3	2	2	3	5	2	**96**
Text-based passwords	2	1	4	4	4	5	2	2	1	3	3	5	2	**94**
Knuckle scan	4	4	2	3	3	4	4	5	1	5	3	3	4	**93**
Handpalmprint biometrics	4	4	2	3	3	4	4	5	1	5	3	3	4	**93**
Barcodes	1	4	3	4	4	4	3	4	4	2	4	5	2	**92**
Iris biometrics	4	3	2	3	2	4	4	5	5	5	3	2	4	**90**
Gesture passwords	3	3	3	3	3	4	3	2	2	3	3	4	3	**87**
Smart devices	4	5	2	3	2	3	3	3	4	2	2	4	3	**84**
Gait biometrics	5	5	1	1	1	3	5	5	5	5	2	1	5	**76**
Location	2	5	2	2	2	2	5	5	5	5	2	2	5	**76**
Heartbeat monitoring	5	5	1	1	1	4	1	5	5	5	2	2	5	**74**
Brain activity monitoring	5	5	1	1	1	4	1	5	5	5	1	2	5	**73**

*Weight can be indicated from 1 to 5, with 1 being the worst and 5 being the best.

Figure 8: The authentication system decision support matrix with an overexaggerated budget-centric approach

9.4 Evaluating the Model

To evaluate the model, three of the earlier interviewed experts are once again asked for their expertise. For this evaluation, Experts 2, 3 and 6 were selected based on their expertise in the field. A set of documents (the model, information document, a selection of chapters from this research and the entire research for reference) was sent to the experts for review. The evaluation consisted of a set of pre-determined questions and topics that should serve as food for thought to discuss in a short follow-up interview. The questions which were asked were as follows:

1. In terms of identified systems; is the model complete or is it missing any?
2. Are the correct criteria selected?
3. Adding to the previous question: are there sufficient criteria included which relate to non-intrusiveness?
4. Are the scores which are assigned to the criteria, in general sense, correct?
5. Do you think the model could support the decision-making process in selecting a system from the perspective of the seller?
6. Do you think the model could support the decision-making process in selecting a system from the perspective of the client?
7. Is the model easy to understand and use?
8. In which way could the model potentially be improved?

9.4.1 Completeness

In general **Expert 2** did not see any systems specifically missing from the model in terms of authentication and identification of persons. He would, however, like to see additional authentication systems which are marketed and sold by his organization focusing on (for example) identification of vehicles. One of the methods he indicated he would like to have seen in the model was automatic number plate recognition (ANPR). He also indicated that he found it rather odd that there a multitude of biometric access control systems represented while other methods are generalized. Examples of this are mobile devices, which can make use several protocols, or smart cards which can vary from the older RFID standards up to the much more modern and secure cards running individually encrypted applications.

Expert 3 indicated that he did not directly see any systems which were missing from the model. He indicated the complete opposite: maybe too many systems are included. Because of the fact that systems which make use of heartbeat monitoring or brain activity to authenticate someone are included, he found it difficult to see the actual value of the model. This because these systems are unlikely to yet be used in a real life scenario, since they are still under heavy development and therefore are highly conceptual. He indicated that likely 80% would only use a basic selection of the included systems like biometrics, card systems or mobile devices.

Expert 6 indicated that the model was complete at time of writing of this research, maybe even overcomplete. He did, however, find it interesting to see some new novel systems which he did not yet know the existence of. The usefulness of the inclusion of these systems is, however, to be seen.

9.4.2 Selection of Criteria

Expert 2 did not find any criteria which were not included. However, he indicated that some of the criteria might not be clear to the user when not widely elaborated upon. Some of them are open to interpretation or closely related. For example, accuracy and throughput might seem very similar. Continuing, he added that “touchless” is generally regarded as being binary. This should therefore be explained more thoroughly.

Expert 3 thought the selection of criteria was complete, and that no other criteria which he knows which are used in the industry are missed.

Expert 6 indicated that the criteria were complete as well, however, may need some additional explanation in terms on which stakeholders they are applicable. For example, ease of installation could be regarded as installing a smartphone app for an end-user as well as ease of installation of the entire system by the system builder. After reading through the explanation of the criteria, this had become clear to him, however it might not be clear to users only consulting the end model.

9.4.3 Non-Intrusiveness

Expert 2 could not think of any additional requirements relating to non-intrusiveness.

Expert 3 indicated that possibly the aspect of "hospitality" could be included in the model. He explained a situation in which he was visiting a high-tech organization's headquarters, where he was greeted by a front desk employee. This employee took the time to set-up the authentication system for him, guiding him through the process and explaining how the different services within the building could be accessed. He felt that this could be seen as non-intrusive as well, as all of one's cares are taken away by someone who is familiar with the system. However, he added that it might be difficult to include this as a criteria as this is completely dependent on the implementation. It is, however, something to take into account when selecting a system.

Expert 6 indicated that the expected criteria were included, reflecting it to a typical user journey scenario of enrolment (which should be easy to do and can be mapped to initial effort) and user experience (touchless, keyless, skill required and efficiency).

9.4.4 Scores Assigned to the Criteria

Expert 2 indicated that he did not look through every individual score, but instead scanned all of the scores globally and took a focused approach on the system types that he was most familiar with. Doing so, he indicated that he could not entirely agree upon the scores of security given to smart cards. He found that modern smart cards should be rated as more secure, especially when compared to, for example, the score corresponding to fingerprint biometrics. He continued by noting that security significantly depends on the type of implementation: while old RFID based card technologies are easy to copy because the security was cracked (he referred to the old Dutch public transportation card), this is not the case for more modern and secure solutions.

Expert 3 indicated that, overall, the scores were quite accurate. However, he missed the important note which describes whether a score of 1 or 5 is deemed good or bad. Even though this is indicated in the information document, this is not clearly explained in the actual model file.

From all of the experts, **Expert 6** looked into the individual scores with the most attention. He indicated that there are a lot of nuances which are difficult to take into account, which are often dependent on implementation. This is, for example, the case with face biometrics. Implementations exist which require the user to first scan their face in a separate kiosk, while more modern implementations can do this on the spot. Having to visit a kiosk significantly decreases throughput and initial effort scores. Additionally, he indicated that smartcards are often more accurate than biometrics and are often significantly cheaper than any biometric reader system (because regulations require an alternative to be present, often a smartcard or pin-code based system). Furthermore, he had some questions relating to authentication methods which require training, such as heartbeat, brain activity and location based systems. He would think that initial effort and efficiency should be much better, but understood that this would not be the case if it would need extensive training. Furthermore, he would think that these systems are likely to be used as verification instead of authentication.

9.4.5 Usefulness

When **Expert 2** was asked if the model could be used for commercial purposes from both the buyer and seller point of view he answered with a clear YES. From the buyer perspective it can give the user some options while he is still in the explorative phase, looking for which products to choose from. Furthermore, from the perspective of sales, it can be used both as a marketing tool and tool for novice employees who still need to acquire additional knowledge about the topic of authentication methods.

Expert 3 found this to be a difficult question to answer. He indicated that up to some level, it could definitely be useful. However, it should be heavily commercialised. They currently provide the potential buyer of their systems with a comparison between the systems they offer. However, this is often based on only 2 criteria. Therefore the model could potentially be used as a more extensive comparison tool. A more substantial contribution of the model in terms of sales could be found when looking at public tenders. From a seller's point of view one can see which technologies they can offer, based on the criteria of the buyer, while the buyer can directly see which sellers are able to fulfil their needs.

Expert 6 saw less value from the perspective of the seller, since they should already have knowledge about the systems they sell. Furthermore, some of the techniques included in the model are simply not mature enough to be used for access control and therefore definitely not yet ready to mass produce and sell. From a buyer point of view, it could be useful since it can enable the potential buyer to make an easy comparison between different systems. However, it should be clear to the user which actual implementation is meant when looking through the options. Continuing, it could be a useful addition from a manufacturer's perspective to discover and map different available (novel) techniques. He indicated that "to stay competitive, novel techniques have to be monitored to make use of them when the time is right".

9.4.6 Usability

Expert 2 found that the model was easy to adapt when scores were deemed to be unrealistic or unsuitable for the situation. However, at first glance it seems quite impressive in size and rather complicated. It includes many different criteria and authentication methods and could use a more intuitive user interface. This would also directly make it commercially more interesting.

Expert 3 found that the model looked quite complex when quickly looking over it. However, when he looked at it with a little bit more attention, he found that it was OK in terms of usability. He still found it to be quite extensive. This could partially be solved by adding notes in an additional column, indicating which is the most common use-case scenario.

Expert 6 found the model quite useable and clear after reading thoroughly through the different criteria.

9.4.7 Areas of Improvements

Both **Experts 2 and 3** indicated that the biggest improvements could be made in terms of usability. This directly makes it commercially much more attractive. For example, one could design some kind of workflow with a significantly improved UI which could be used on the website of a supplier's organization. The user could select its use case, the criteria which are important for the used environment, indicate importance for each of these criteria and present the user with a limited amount of options. This way the user would not have to see the underlying scores of the matrix, which would make the model much less overwhelming to use.

Additionally, **Expert 3** indicated that the target group could potentially be specified in such a flow as well. For example, a group of elderly people is unlikely to be able to adopt a system using smartphones even though it might be a great solution for the younger generations. A card or barcode based system could potentially be much better. This could be used as an indication for which system to use.

Expert 6 indicated that the model could be improved by differentiating more clearly between the different implementation options which are available when choosing a certain technique. Furthermore, the difference between identification and verification is not always clear. For example, one may still need some type of smart device as identification to be able to use heartbeat monitoring as a verification option. Together they form one system, although this is not directly made clear. Lastly, being able to make a comparison between two systems directly could be a useful addition.

9.5 Concluding Remarks and Improvements to the Model

All in all, the experts generally responded positive to the model, both in terms of content and its potential contribution to selecting a fitting authentication system in various scenarios. However, the feedback did include some remarks which may not be ignored. These remarks are not ground-breaking to the model, but with some slight adjustments direct improvements could be made to the model. These adjustments are as follows:

- Scores have been adjusted where necessary.
- A legend has been added to the model file elaborating upon the meaning of various criteria.
- A note has been added indicating that score 1 is considered bad, and score 5 is considered to be good.
- Additional use case scenarios for the weight assigned to criteria besides the single one relating to a budget centric solution are included for reference. These may be used for four different typical building scenarios (these are the same as were used by So et al. (1999) in their QEM model) and can be found in Table 10 below.

	Security	**Throughput**	**Budget**	**Installation**	**Service-ability**	**Accuracy**	**Efficiency**	**Skill required**	**Touchless**	**Keyless**	**Effort**	**Privacy**	**Image**
Hospital	4	2	2	4	4	4	4	3	5	5	2	5	2
Residential	3	1	4	3	2	3	2	3	1	4	1	1	1
Commercial	3	2	3	3	3	3	4	3	2	3	3	3	3
Transport Terminal	2	5	2	5	5	4	3	5	2	2	4	5	2

Table 10: Example weight scores of four common building types

Besides this, many comments were made about the usability of the model. These can be fixed through adjustment of the UI, and creating a more user friendly flow, guiding the user through the model enhancing the customer experience. This way it can even be used by someone who is much less informed about authentication systems, making it commercially much more interesting. Creating this model would require to develop it from the ground up or through making use of a different platform. Since this is outside of the field of expertise of the author, directions are provided on how this could be achieved. This is elaborated further upon in the discussion, limitations, future work and recommendations section, which can be found in Section 11.

10. Maintaining Technologies – Rethinking the Lifecycle

Besides the model as presented in Section 9, one other important research question was proposed in Section 2. This relates to the lifecycle of (authentication) technologies. Nothing lasts forever. This can be said about nearly everything, from a living organism to a carefully designed and manufactured product. A "thing" goes through a series of stages during its lifetime until it eventually stops functioning. This, of course, can be said about authentication technologies as well. While it is a certainty that technologies stop working or become legacy products over a long period of time, there are some things that can be done to at least make sure this period of time is as long as realistically possible. The following section addresses this subject, by first pinpointing the issue, explaining how this relates to authentication technologies and lastly how this can potentially be improved in the future.

10.1 The Issue with Consumer Electronics

Modern tech products seem to no longer last as long as they did in the past. An often heard phrase is "They don't make them like they used to". And in some sense, this is actually the case. This concept is defined as "planned obsolescence", and is claimed to benefit both the manufacturer and the consumer (Hadhazy, 2016). A mobile phone is often linked to a data plan, which typically lasts about 2 years. After these 2 years, the phone is often stowed away in a drawer to serve as a spare (which it is never used as), sold online or thrown away/recycled if it is severely damaged. Continuing, television sets often lasted longer than a decade before the smart revolution transformed them into all-in-one computer systems for in the living room. This has brought more and more innovation into the homes of the everyday citizen. However, as with most things, with advantages come disadvantages. Nowadays, owners risk to lose critical functionality of their device after several years of use, even though the hardware can still do as much as it could when it was released (Hendrikman, 2016). This is an issue which is worth paying attention to.

The reason for this is often the software, not the hardware. Devices are still made to last, hardware wise, and do not physically break down more often than back in the days. A great example of this are cars, with the average age of a car on the road in the U.S. having more than doubled in the past 50 years. A contrasting exception in this are battery packs, which wear out over time when charged and discharged regularly (Hadhazy, 2016). But regarding the cause of this all, the software, this requires some nuancing as well. To be more specific, the culprit is often the interconnectedness of the device through this software to the world. While the hardware, software and technology standards around the world keep developing, which benefits the consumer, the hardware in the device bought several years ago is not. This often makes it unable to receive the latest software update and keep it connected to the smart world while also maintaining the manufacturer's standards. In some instances a software update is pushed nevertheless, but consumers complain about major slowdowns of their devices. In February 2020, electronics manufacturer Apple was fined for this exact problem: they failed to inform consumers that updating their device would imminently slow it down (BBC News, 2020). For desktop computers or laptops, this issue can sometimes be resolved by upgrading its components to make it somewhat up-to-date again. If one is not able to do this themselves, a computer specialist can often help doing this. For complex integrated devices such as smartphones or television sets, where everything is soldered to each other and not made to be easily repaired, this is not an option. Therefore one has to rely on the ability to connect the device to external devices, if this is possible at all. To enjoy the functionality one was accustomed to before the scheduled update, or to become up-to-date again with the latest innovations, the option of replacing the device in its entirety is unfortunately often the only one left.

10.2 IB Technologies: a Product Becoming a Service

Replacing a phone or a television set is one thing, but replacing an entire systems of sensors in an IB is a much more complex situation. This is why this aspect needs attention. When investigating how one can implement IB technologies in such a way that all stakeholders benefit from it, not only the short term effects must be taken into account. Even though technologies aimed at the professional market often have a much longer life span than consumer technologies, often spanning several decades, this is often not enough. This especially the case during the current so-called 4th technological revolution where an entire generation of technology can be skipped merely during the design and construction of the building, which can take several years (Memoori, 2019).

Because of this manufacturers of smart technologies have to understand that they are not solely committing to physically producing a product anymore. They are committing to creating and upholding a (cloud based) platform and establishing a network layer for the reasonable time the consumer expects product to last. Even when the product is deemed to be a legacy product by the manufacturer, there still might be existing users which wish to remain to use the product for many years to come. While this might seem as a burden to product manufacturers, this can also be seen as a new range of opportunities. It opens up possibilities to establish new longstanding customer relationships (Porter & Heppelmann, 2015). It is therefore important to think about “what if”-scenarios. For example, what if the client wishes to switch from its existing smart solution provider but wishes continue using the same sensors when switching to another party? What if the client wishes to incorporate additional products from a third party into their existing system, without replacing the entire system? What if the client wishes to add or replace software components with in-house developed software code? If systems are designed as a closed environment to specifically not cooperate with third party technologies through physical expansion slots, standardized protocols, Application Programming Interfaces (APIs) or open source software, this may impact the earlier mentioned stakeholders. Besides this, parties not directly affiliated with the users are impacted as well. The environmental strain that technological waste (also called e-waste) puts on society is significant. And as expected, with technology becoming more and more incorporated into day to day life and an increasing demand for these products from developing countries, this will only increase. (Needhidasan et al., 2014). Minerals used in smart products are becoming scarce, which has increased attention to the debate on how to recycle, re-use and extend the use of technology (Gabbatiss, 2019).

10.3 The Challenges and Potential Solutions for Authentication Technologies

But how does this apply to authentication technologies? To determine what the impact is on such a system, it is important to decompose it first. An obvious division which can be made is the division between the hardware and software layers of modern authentication technologies.

10.3.1 Hardware

The hardware layer consists of the electrotechnical components of the system. This includes system control processors, readers (card readers, fingerprint readers, multi-readers etc.), input/output interfaces and other peripherals that are desired or have to be used to complete the system. Since hardware costs are often the largest initial costs, it is important that this is done right. This is especially the case since the hardware is often embedded within the building, which makes it undesirable to change it out for alternatives if it functions in an unsatisfactory way. Because of this, for over a decade experts are agreeing upon the added value of making use of an open architecture when it regards hardware (RS2 Technologies, 2008). This entails using widely available hardware platforms which enable the user of utilizing components of different manufacturers. This allows the owner to extend the system with newly available features without having to completely overhaul the system, even if the system that is to be extended is from a different vendor than the components that are to be added. The importance of this was also stressed by **Experts 2 and 3**: their organization developed a reader system which supported a multitude of inputs. Alongside of this reader system, an application was introduced which could be used for authentication. Eventually, support for this application was dropped but due to the open architecture design of this reader system it could still be used in combination with other equipment or software. This made it possible for their clients to remain using their expensive hardware, extending the lifetime of the product indefinitely. The organization of **Expert 7** instead only provides the software part, not dealing with the hardware. This is all made possible by making use of open standards and APIs. It was indicated that their face recognition software could work with a multitude of systems and gates, since it only provides the result of a possible match between input and a database reference. This can consequently be translated in allowing or denying access to a user.

While incorporating an open architecture surely benefits the adopter of the system, it might not directly seem as an interesting option for vendors. A closed architecture system can be designed in such a way that it immediately creates a so-called vendor lock-in. This means that the client is bound to a specific vendor when looking for extensions, upgrades or maintenance; an optimal scenario for the vendor. When the initial contract with the vendor is over, the client has no other option than to either continue using the product without being able to upgrade, having to upgrade with third-party products (which are possibly less compatible and lack features when compared to the vendor offered products) and rely on third-party maintenance providers for service. That is, if this is even allowed by the original vendor without violating their terms and conditions. Violating these conditions could possibly result in losing their factory warranty or right to service in the future. Replacing the entire system as a whole is of course always an option, but at what costs?

10.3.2 Software

The hardware side seems quite simple: provide sufficient input and output interfaces, make sure that open standards are used for these interfaces and provide clear info regarding which data flows between hardware and software. This way software can be developed independently without relying on the manufacturer. Sounds easy enough, but often this remains to be an utopia. Because of this, software could pose to be a serious threat to the longevity of the product's (lifecycle). Ever since computers have been involved in authentication, the role of software has become more apparent and sophisticated. While first only used to support the correct authentication of the user, nowadays authentication systems might be extended with and integrated within additional applications as a service to the user. Authentication is becoming an important bridge to enable access to personalization and comfort for office users.

The increasing importance of embedding software into classic office elements to increase the comfort of its users can also be seen in literature. Mørch (2019) has identified the most influential smart office technology trends of 2019 and beyond. The major components which are mentioned as trends for the coming years are the use of IoT sensors for environment monitoring, smart lighting and intelligent climate control (or smart HVAC systems). Besides these common components of a smart office, three additional technologies are discussed. These are smart conference rooms, smart desks and the use of video monitoring. A smart conference room combines a number of smart features of which the aspect of monitoring room occupancy is the most important. Authentication systems could possibly play a role in measuring occupancy, since movement between rooms can be monitored by checking access requests for each individual door or gate. Besides that, it introduces the concept of a meeting management platform which indicates the usage of (shared) office spaces. This includes so-called hot desks (non-personal desks, shared with co-workers), phone boots for increased privacy and private meeting areas. Consequently, it should enable users to book these rooms and desks in advance, guiding them to these booked areas and making it possible for the organizer of the meeting to add additional equipment or services on request. Examples of such services are catering or the necessity of A/V equipment. Continuing, this system should alert users for events or changes in their meeting schedule as well, either through notifications on a mobile device or through displays hanging throughout the building and offices. A similar but significantly downsized concept is the concept of smart desks, which adjust the environmental factors to suit the user's wishes. This is of course all based on previously indicated preferences. To achieve this level of personalization, the desk is equipped with some type of reader system. The type of reader system obviously depends on the type of authentication method that is used in an office.

When asked about how the experts viewed the future of authentication, **Expert 5** had a clear vision. He sketched a scenario in which authentication would become the centre piece of a broader set of applications. The expert provided an example of a client receiving an invitation to visit an office building on his smart device. On this device he can indicate if he would need a parking spot, and automatically reserve and assign one based on availability around the time of the scheduled meeting. Other services can be requested as well, if available. The car is recognized through its license plate, denying access to any other vehicle. Once arrived at location, the visitor can access the building through the earlier received invitation. This can possibly be achieved by a vision based authentication method (which he viewed as being the future), or by using the phone as a key. Inside the building the visitor gets guided towards the area where the meeting will take place by means of an IPS powered by a digital twin.

Of course, the technologies and platforms mentioned above should only be available to authorized users and differentiation may be made between users regarding access to different services (for example, an intern should not be able to make a reservation for the board room). Integrating these technologies with the company's authentication and office's access control system therefore only seems obvious. Since it regards a system which should enable users to book rooms and services in advance, a smartphone application seems to be a good solution. All in all, this complicates the previously relatively simple software infrastructure of the authentication system significantly. For instance, the application should run on multiple platforms and on a vast number of different devices which all differ in terms of specifications. Continuing, since these technologies are all visible to the end user and contribute to the image of the company, one can assume it is desirable to keep them up to date with recent technological developments. This means that both hardware and software should be updated and upgraded over time. These updates likely have to be made significantly more often than upgrades to the access control system itself, which often has a lifespan of several decades (Rhodes, 2014). While it may be difficult for the average user to spot the difference between a 5 and 20 year old card reader system, it certainly recognizes a lagging interface or old television display.

While these updates and upgrades will have to be made more often, this should on itself not be an immediate issue. That is, it should not be an issue if the piece of hardware connecting the authentication system to the external applications can be upgraded on its own and if APIs are available to develop software to communicate with it. If this is the case it can be swapped out if new applications would require so, or in-house developed software may replace lost functionality. Clients which buy a solution might think that what they are buying will last them a lifetime, but experience indicates otherwise. For example, security encryption gets innovated time after time, and rightly so: if this was not the case hackers may operate at will. In a traditional access control system, there is no connection with the outside world, eliminating a potential weak spot. However, since applications such as described in previous paragraph require access to the internet to communicate with its users, software security (besides the security measures for internal authentication) has become extra important. If the interface connecting the system to the outside world is unable to work with the most recent security algorithms, it is likely to become unsupported quite quickly as it is deemed unsafe. An example of a product which was shut down because of not being able to cope with the latest security standards, were Smart TV sets by Philips. They were not able to implement the SHA2 security standard, while applications such as YouTube and Netflix required the implementation to continue working. (Hendrikman, 2016). The Smart TV suddenly became not so smart anymore, simply because the hardware could not keep pace with the software. To ensure safety, the device was simply disconnected from the internet. If specific components could have been swapped out, as explained in 10.3.1, or community developed software (connected through APIs) could have replaced lost functionality, this would not have been necessary.

10.3.3 Dealing with a Complex Software Infrastructure

When building a system from the ground up, one can anticipate on this by designing it in such a way that it is easily expandable and vendor independent. However, this is often not the case as large office buildings often come readily equipped with an access control system installed. Therefore, one risk that has to be dealt with directly flows from the possibility that parts of the system might be replaced or extended while the core system remains largely intact. When this involves some small adjustments or the addition of a single application, this might not directly be an issue. However, repeat this process a few times more, and one risks that the system organically grows to become a web of interdependent applications increasing the system's complexity. Such an interconnected web of applications is difficult to maintain, and individual applications are difficult or even impossible to replace without dismantling and reprogramming the entire software infrastructure. Furthermore, this could pose to be a significant security threat to the authentication system, as a security issue in one of these applications could potentially lead to be an entrance to the entire system.

Of course, all begins with understanding what dependencies exist between the different applications. To do so, one should start off by mapping and capturing the different applications which are used within the system or organization. Consequently, once the these have been identified, the mutual cooperation between these applications and the data that flows between them should be indicated. This map of interdependencies and collaboration between applications is often part of a larger discipline which is called Enterprise Architecture. Enterprise Architecture helps organizations with structuring its IT projects and policies to help them align with their business goals. Often the ArchiMate modelling language is used for visual representation. An example of a fictitious organization’s application infrastructure with complex interdependencies, represented through the ArchiMate modelling language, can be found in Figure 9, below.

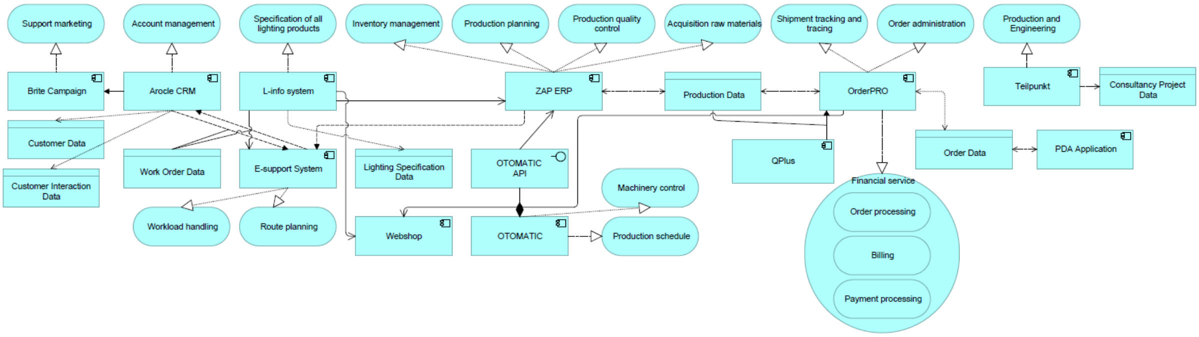


Figure 9: An example of a fictitious organization’s application infrastructure with complex interdependencies, represented through an ArchiMate model

As one can see in Figure 9, in this scenario there are various applications which are linked to each other in series. This means that, if for some reason one of the application earlier in the chain breaks down, everything further down the chain will feel the consequences. Depending on the implementation, this could mean that applications partially stop working or fail to work at all. There are, however, solutions to resolve this. One of them is integrating applications together and eliminating redundant applications. However, since this is unlikely to be possible for such a complex system, an alternative solution is probably more suitable. This is the use of middleware software. Middleware software is software that serves as a conversion or translation layer. It ensures that applications can communicate with each other, regardless of vendor or platform. Applications are often connected to and from the middleware software through APIs or web services. The connected software sends messages to the middleware software, which consequently sends the messages to the correct recipient. A simplified representation of the capabilities of middleware software can be seen in Figure 10.

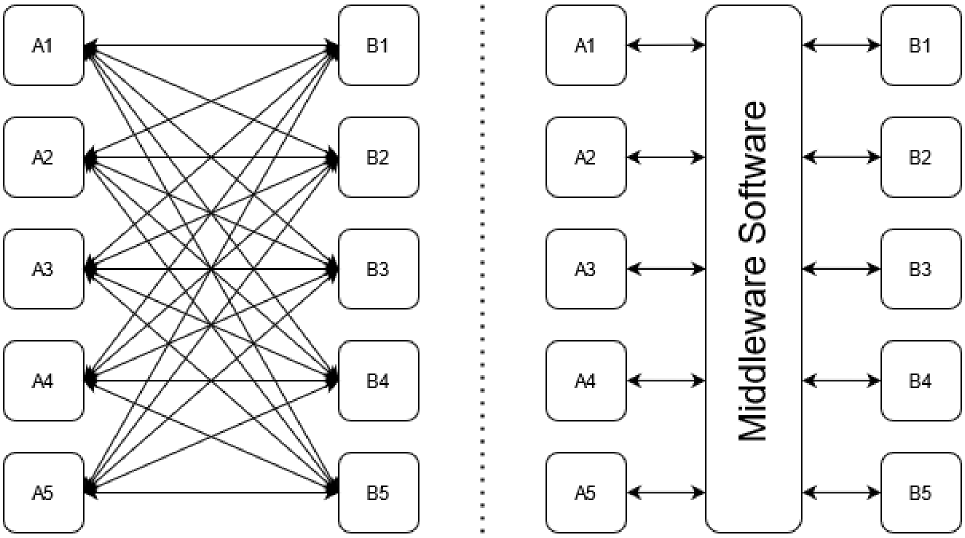


Figure 10: A simplified representation of connection between applications with and without the use of middleware software

If a system on either the sending or the receiving side goes down, it does not directly affect one another in terms of operability. The messages will form a queue in the middleware software until the application which was temporarily offline becomes available again. Because it acts as a translation layer, middleware software can be used to connect legacy applications to up-to-date (cloud based) applications. This is beneficial for both the developer of software and the purchaser of software. Developers can develop new applications in a wide variety of programming languages as long as it supports one of the communication methods the middleware software can interpret and process. Legacy applications can continue running until they are replaced, which can be done without significantly changing the integration of the software system.

As for its usefulness in this specific context: it can help modernize an authentication system which might on itself already be several decades old. Users are expecting the earlier described comfort features, while owners of the system wish to extend their product's lifetime. One should, however, not disregard that middleware software has a product lifecycle on itself as well. Nevertheless, incorporating these mentioned best-practices may contribute to (at least partially) achieving both of these goals.

10.4 The Opinions of the Experts

During the evaluation of the model as presented in Chapter 9, the experts were also asked to give their opinion on the topic of redesigning the lifecycle of authentication technologies. To be more precise, they were asked which primary design principles one should incorporate in an authentication or access control system to ensure it can be expanded to fulfil the growing customer needs while ensuring maintainability. The responses of the three experts (Experts 2, 3 and 6) can be found below.

Expert 2 immediately indicated that this was by no means his area of expertise. However, when explaining the situation a little bit more in-depth, and by providing some general directions, the expert in the end came up with some global remarks. He indicated that, considering that every system has a base software layer upon which all extensions are built, it is of utmost importance that this base layer is solid and can communicate with all potential future applications. Even though certain data might not yet be used for a basic authentication system when it is delivered to the client, data should be generated and be easily accessible for future use. Therefore there should be insight in the data that is generated, so that additional modules can easily be added and swapped out like LEGO bricks. His remarks, even though they do not go as far into the depth as was desired, are in line with the findings of this research.

Expert 3 directly recognized the problem. It has become increasingly become difficult to make a maintainable system when linking all kind of applications together. Previously one provider would create one all-encompassing integrated system. However, the expertise of the company providing the system would have to be very broad. In current days, this is deemed to be nearly impossible. One can not expect an organization which is able to develop and deliver a high-tech card reader system to also deliver a video biometrics based system. He therefore recommends creating API entry points in the base system to be able to profit from the expertise of different organization. Besides that, he indicated that some type of middleware software could be used as a potential solution to structure software as well.

Expert 6 indicates that most clients still have their authentication system running on-premise, with no connection to the outside world. This makes it difficult to update systems, which consequently leads to client postponing updates until there is no other option left. This results in very large update packages, increasing the chance of complete system failures. Continuing, hardware is often not replaced as "it still functions fine". Because of this, the systems are often not equipped with state-of-art security. Replacing this hardware is often done when it fails or when remodelling of the building has to be done. Reducing the number of hardware devices on-premise could be a solution, although he does not know how realistic this is. Reducing the amount of hardware would reduce the cost for the client, and might convince them to update and upgrade more often since it is significantly less impactful to daily operations. Cloud solutions may help in this respect, as it can replace local hardware and applications as well as that updates can be pushed to the user instead of the client having to pull updates. On the long term, renting the hardware of the authentication system instead of buying it could be a partial solution as well. From a vendor point of view, this is interesting as it creates a vendor lock-in principle. Furthermore, one is able to force the client to update because the product is not supported anymore. From a client side, this is beneficial as well as this can be done against lower costs, since the hardware is only rented.

10.5 Best Practices Summarized

Based on the insights as provided throughout chapter, the following issues and potential best practices which can serve as solutions for these issues can be identified:

- Access control systems are often only replaced when it is absolutely necessary, and as a consequence are often old and difficult to update.
- Reason for this is that they are often deemed to still be functioning "just fine", and are embedded inside a building. This makes replacing expensive and difficult.
- Users demand more and more personalization within buildings, this can be achieved through intelligent building technologies. Authentication is key in this. This issue is therefore likely to become only more and more apparent.
- Extending an old system by adding new applications is possible, but may lead to a complex interdependent software-hardware infrastructure. This increases chances of a total or partial failure of the system.
- Key to overcoming this issue is maintaining open architecture principles for both hardware and software.
- There are multiple best practices which can contribute to a solution to this problem, these include but are not limited to:

- Making use of APIs for software packages, incorporating middleware software and I/O interfaces for the used hardware
- Reducing the hardware which is on-premise of the client's building
- Switching from a buy to a product as a service model, in which the hardware is rented from the vendor
- Making use of cloud based software solutions instead of on software running on-premise

Incorporating these best practices are no guarantee for success, and might be very difficult to even impossible for already installed legacy systems. They do, however, form a solid basis for yet to be installed systems and should enable the user to extend, upgrade and maintain the system for a longer period of time.

11. Discussion and Conclusion

This study aimed to explore the body of knowledge surrounding future proof non-intrusive authentication systems for use around the office or commercial real estate in general. A model was developed to create insight into the commonly and conceptual available technologies and be able to make a motivated choice between these technologies. Furthermore, a look was taken at how these technologies can be implemented in such a way that they can be properly maintained, extended and may be used for a long period of time.

11.1 Addressing the Research Questions

To come to these results, the following research question was posed:

"How and which non-intrusive authentication systems can best be applied in office buildings to increase the comfort of its users, while ensuring these authentication systems remain maintainable?"

To be able to answer this research question, several sub-questions were formulated. These questions were consequently answered through a literature review and multiple consultations with experts in the field of authentication systems. The first sub-question is as follows:

> **SQ1:** "Which technologies are available to support non-intrusive authentication systems in the office of the future?"

To answer this question, some background knowledge regarding the problem context and the definition of the concept of non-intrusive authentication was necessary. This body of knowledge was presented in Sections 3 and 4. This strong basis was consequently used to dive deeper into the matter of authentication technologies. Through the means of a literature review of popular and scientific literature as presented in Section 5, it was aimed to chart the broad range of (non-intrusive) authentication systems which could be applied in the context of commercial real estate. Technologies which are currently not yet commonly available were included as well, as these could become important in the nearby future. It was found that there are a multitude of solutions, maybe even too many to all include in this research. Each of these solutions seemingly has its own strengths and weaknesses, and many variations exist for each of these solutions. A slight alteration to a given technology can completely change the way it operates or may be used. Continuing, multiple technologies may be combined to create a more secure and versatile solution if this is deemed necessary. Such multi-factor authentication methods are becoming more and more common, and it is likely only a matter of time until we see these methods being applied for physical access control instead of logical access control.

To explore how the different characteristics of the identified techniques may be used in different contexts and to cater to different requirements and stakeholder goals, the stakeholders must first be identified. The following question was therefore posed:

> **SQ2:** "What are the main stakeholders that make use of commercial real estate and are involved in using this technology, and what are their requirements?"

Through logical analysis of users of commercial real estate, as presented in Section 6, a total number of four stakeholder groups were identified. The office workers, the real estate leaser, the property owner and an additional supporting stakeholder group. This last stakeholder group includes service providers such as catering, emergency services and maintenance personnel. It was found that, besides the basic legal requirements that have to be fulfilled, requirements vary significantly between different stakeholder groups but are all interconnected. Office workers mainly require a health work environment. This can be achieved by controlling environmental factors such as air quality, lighting and temperature. If possible, they wish to be able to control these things on a personal level. Preferably per area or desk. Comfort at the workplace is one of the prime concerns of this stakeholder group. This would directly increase productivity, which directly brings us to the requirements of the real estate leaser. The leaser is often the employer of the office worker, and therefore wishes to create an environment in which employees can thrive and be productive. Of course, this has to be done at minimal costs to ensure efficiency. However, due to the current war on talent for (primarily) employees with a technical background, the office may be used as an additional method to distinguish itself from the competition. In this respect differ the requirements only slightly from the property owner, which wishes to create an attractive building so that it can easily be rented out. Once again, minimizing costs is an important concern as well. Lastly, the service provider group benefits from proper flow of information. This relates to knowing how to get access to areas, as well as having information about the use of the building.

Regarding this use of the building, it is clear that a lot has changed due to the ongoing coronavirus pandemic. This is what sub-question three relates to:

> **SQ3:** "Which changes do major employers anticipate in respect to changed working habits due to the coronavirus pandemic, and how has this changed the requirements of them, their employees and third-party stakeholders?"

This question revolving around the recent developments involving the coronavirus pandemic was answered in Section 8. To do so, a mixed method approach was used. Literature was consulted to spot the main trends and expectations relating to office use during and after the pandemic. To support these findings, experts were asked about what they feel would happen to office use in the future and how this may possibly be accelerated due to the pandemic. Results from literature show that office use has changed, and will be changed for good. Employers and property owners see a decline in the amount of office space they need, as working from home has become more common. Due to the pandemic, the infrastructure necessary to be able to work from home has been set up for many organizations which previously did not support this. Research shows that productivity may increase significantly when working from home, although this is not the case for all employees since one's home-situation may differ drastically. Signs point towards the office being a central meeting point and place to increase creativity. Offices will be equipped with so-called hot-desks and meeting rooms. This results in different people visiting the office each day, consisting of employees of the organization, flex-workers and clients. Such a diverse flow of personnel could put significant extra stress towards hospitality employees such as front-desk employees. These are tasked with providing visitors access to rooms, provide them with directions around the building and consequently revoke access to areas within the building once they are leaving. Modernizing access control to make it more comfortable to both the visitor, property tenant and property owner may become more and more important.

Now that the stakeholder requirements are known, they can be combined with general requirements for authentication systems, which were identified and constructed in Section 7, to design a model to make a substantiated decision between available systems. These authentication requirements are constructed based on literature and completed through insights gathered from expert interviews. This leads us to the following question:

> **SQ4:** "What would a concept design for selecting and implementing non-intrusive authentication methods in the commercial real estate sector look like?"

It quickly became clear that a single one-size fits all solution does not exist. Therefore, a model had to be developed which made sure that the user can indicate which criteria are more important to differentiate between the various options. To achieve this goal, a weighted decision matrix was developed which includes 13 criteria and 20 authentication systems to choose from. This model was presented in Section 9. Each combination of system-criteria has been given a score, ranging from 1 (being the worst) to 5 (being the best). This score is based on insights as presented throughout this research. The user can indicate a weight, once again ranging from 1 to 5, to each of the criteria based on the importance of that criteria to the user. What results is a ranking of scores for each potential authentication system.

Designing a model is one thing, but ensuring it is correct is even more important. Therefore an evaluation of the model was conducted by consulting three experts in the field. The following question was posed:

> **SQ5:** "To what extent does this concept design fulfil the requirements of its primary users, and how can it potentially be improved?"

In this evaluation as presented and elaborated upon in Sections 9.4 and 9.5, the experts were asked to answer a total of eight questions relating to various aspects of the developed model. Through this evaluation some points of improvement were indicated, although the general response to the model was positive and the model was deemed correct and applicable. These mainly relate to usability aspects, since the model was often found to be quite overwhelming to use even though they were experts. It is therefore clear that, if the model is to be used by users which possess significantly less knowledge about authentication systems, it should be significantly altered in terms of UI and intuitiveness to make it useable. Insights were provided by the experts on how to achieve this. How this may be done is elaborated upon in the future work section.

Lastly, in Section 10, attention was paid to how the lifecycle of complex technologies such as authentication systems may be redesigned. The last question which needed answering was therefore as follows:

> **SQ6:** "How should the product lifecycle be redesigned so that these non-intrusive authentication systems can be applied in a maintainable way that benefits all stakeholder groups?"

The lifecycle of modern technologies was critically assessed, indicating problems relating to maintainability and longevity. Complex software and hardware interdependencies combined with the demand of users wanting products to constantly be improved and extended results in issues with stability of systems or hardware having to be replaced entirely. This while the product itself is not yet even a few years old, and physically can continue to work for many years to come. The same can be said about authentication systems, which are due to be extended by many extensions to improve the comfort of the user. Some things can be done to at least partially counter this. A set of best practices was presented, deduced from literature and expert consultations.

11.2 Key Findings

1. A research gap exists between the knowledge area of smart offices and authentication

While the knowledge base revolving around smart offices (or "the office of the future") is broad and includes many different topics, only little attention is paid to authentication or access control. This seems odd, as topics regarding personalization of environmental conditions, indoor positioning systems and meeting management platforms are discussed to great extent. Making use of this system requires some kind of authentication to ensure personalization. Therefore, additional attention to this topic seems obvious and necessary. Directions on how to do so are provided in Section 11.4.

2. Authentication is moving towards non-intrusiveness, although adoption is slow

Through inventorization of available authentication method, it has become clear that the recent focus of scholars and companies specializing in this area is put on biometrics. To be more precise, vision based authentication scanning one's face seems to be the future. This was also recognized by the experts which were consulted. Additional non-intrusive methods such as gait, heartbeat and brain activity were also mentioned in literature but are still in its infancy. Although the sector is moving towards these less intrusive authentication methods, adoption is still low. Most organizations still go for card reader systems. It will be interesting to see how fast this will develop.

3. The future of office use points to becoming hybrid, balancing between working from home and on-site, although a lot is still unclear

Literature and organizations feel that the future of office use will change, partially due to the pandemic. Working from home is there to stay, and the office will change towards becoming a meeting spot and accelerant for creativity. However, when experts were asked about these developments, no real consensus could be reached. Of course, organizations might be able to force these changes upon their employees through protocols or redesigning the office, but this takes time. It is therefore to be seen if these predicted changes will actually go through. If these anticipated changes indeed become reality, new solutions need to be adopted to support this new way of working.

4. The future of maintainable and long lasting technology is openness

Complex technologies consisting of multiple hardware elements connected through different layers of software may be difficult to maintain. Solution exist, and key in this is openness. This relates to creating an open hardware architecture, using standardized protocols and I/O interfaces. Furthermore, software should be connected to each other through the use of APIs or middleware software so that it can easily be swapped out if demand requires to do so.

11.3 Contributions

In this research a substantiated decision support model was presented for authentication systems which may be used in and around the office environment. Available and conceptual authentication systems were charted, stakeholders were identified and requirements for these stakeholders were consequently engineered. Lastly, it has contributed to the body of knowledge relating to durable, maintainable and sustainable technologies. Therefore the contributions of this research are as follows:

1. **Practice**: a model was presented to support potential buyers or sellers of authentication systems with choosing a solution without requiring any extensive knowledge of the topic in question
2. **Practice**: a set of best-practices were presented which may be used to redesign the product lifecycle of authentication/access control systems, or complex software-hardware systems in general
3. **Academic**: the need for additional attention and research to the use of authentication in and around the office of the future was demonstrated
4. **Academic**: through extensive literature research, an up-to-date overview of available and conceptual authentication systems was presented

11.4 Limitations

Inevitably, some limitations exist to this research. First of all, the number of authentication systems which is identified and elaborated upon throughout this research could possibly be incomplete. Developments in the world of authentication and access control move quickly, just as most other technological developments do in current day and age. To be completely up to date, one would have to be constantly watching developments in this area or scrape the web for anything related to authentication technologies. Furthermore, some authentication systems which were identified could possibly be decomposed into smaller sub-types of systems or variations of systems. For example, multiple smart card reader systems exist, as well as that mobile authentication systems can be implemented in several ways. Due to limitations in time and scope, it was chosen by the author to not do this, while this indeed might be possible when additional resources are spent on this.

Furthermore, the experts which were consulted for additional input throughout this research primarily came from one single organization. This could have limited their views on authentication systems, as the experience they have mostly comes from the set of products that they have on offering. Continuing, because only experts in the field of authentication systems were consulted, evaluation of the end product from a consumer point of view is lacking. Of course, the experts can shine their light on usability for laymen based on the experiences they have dealing with customers, but direct feedback from these users is lacking.

Lastly, the content relating to the coronavirus pandemic might not be up-to-date or accurate for all regions around the world. When writing this research, it was tried to make an assessment which is applicable to North America and Western Europe by combining sources from both areas of the world. Information regarding the impact of the pandemic on other areas of the world, mainly Asia and Africa, was not directly taken into account. Furthermore, the pandemic is still developing and having its impact all around the world, including North America and Western Europe. The severity of this impact is constantly changing, which makes it difficult to make a time accurate assessment over the course of six months of writing. This should be taken into account when reading the sections relating to this.

11.5 Future Work

Of course, future work should focus on trying to resolve the limitations as mentioned in previous section. First of all, the limitation regarding the completeness of the model could be resolved by diving into catalogues of providers authentication systems and decompose them even further. This would extend the model, making it more complete. It is however questionable if this would make the model more interesting, as the smaller differences in terms of characteristics between the different implementations are most likely vendor dependent. The model should therefore be include systems, makes and models which are on offer by an organization, or which are useful for a scholar to be included for research purposes.

Continuing, the model which was presented in this research should be evaluated by a broader set of experts and laymen users. This could be done by means of a larger survey, in which the number of participants may be significantly increased. If time and resource constraints would allow it, one could even opt for interviews to extend the body of knowledge even more. Organizations offering authentication technologies or access control systems as well as potential consumers from different areas of the world could be consulted. This way the model can be checked for broad applicability in various different contexts.

Lastly, the content presented in this research relating to the coronavirus pandemic should be updated based on the impact that it has had on the world. As of writing, some parts of the world are slowly opening up again and recovering from the pandemic while other parts are still in complete lockdown. Looking at the global infection rates, even in Western Europe or North America, there is no way to indicate when everything will go back to normal. Infection and hospitalization rates are fluctuating constantly, and so is government policy. Once the point of going back to normal has been reached, the statements which are made in this research in Section 8 should be evaluated based on the knowledge that is available at that moment to ensure that it remains correct.

11.6 Recommendations

A major recommendation which was brought up multiple times during the evaluations related to how the model could be made more usable, or in other words: the model should be improved by making it more user friendly. A brief discussion with the experts also gave some insights in how this could be achieved. It is recommended to transform the model to a web application which can be used by potential buyers of a new authentication system. This web application should guides the user through the process of selecting intended purpose, user demographics and important criteria through an intuitive web flow (or wizard). This web flow should intentionally be made not too difficult to understand by supporting it with relevant images and icons, and hiding the full contents of the overwhelming matrix. In the end, the user should be presented with a top five of most suitable systems between which a comparison of the primary characteristics can be made. This makes the model instantly commercially much more interesting.

Besides this commercialized model, it is recommended to keep a more extensive model on hand for internal use. This model could be used to train new employees, and compare different available options before proposing these to potential customers. It should be kept up-to-date with the newest developments, so that employees of the organizations specialized in authentication technologies are in the know about these new technologies. This to ensure that the organization maintains competitive within the respective market it is operating in.

APPENDIX A

	Cognitive	Gesture	Text passwords	Visual password	PIN	(Metal) Keys	Smart cards	Barcodes	OTP	Smart devices	Face Biometrics	Fingerprint	Knuckle	Palm	Iris	Gait	Brain activity*	Heartbeat*	Keystroke*	Location*
Security	3	3	2	4	2	2	3	1	4	4	5	4	4	4	4	5	5	5	4	2
Throughput	1	3	1	2	2	2	4	4	2	5	5	4	4	4	3	5	5	5	5	5
Budget	4	3	4	3	4	5	4	3	3	2	3	3	2	2	2	1	1	1	4	2
Installation	4	3	4	4	4	5	4	4	4	3	3	4	3	3	3	1	1	1	4	2
Service-ability	4	3	4	4	4	5	4	4	3	2	2	4	3	3	2	1	1	1	1	2
Accuracy	5	4	5	5	5	4	5	4	5	3	4	4	4	4	4	3	4	4	4	2
Efficiency	2	3	2	2	3	3	4	3	2	3	5	4	4	4	4	5	1	1	5	5
Skill	3	2	2	2	3	3	4	4	3	3	5	5	5	5	5	5	5	5	3	5
Touchless	1	2	1	1	2	2	4	4	2	4	5	2	1	1	5	5	5	5	1	5
Keyless	4	3	3	3	3	1	2	2	2	2	5	5	5	5	5	5	5	5	5	5
Effort	3	3	3	3	3	5	4	4	3	2	2	3	3	3	3	2	1	2	5	2
Privacy	4	4	5	5	5	5	5	5	5	4	1	3	3	3	2	1	2	2	1	2
Image	2	3	2	3	2	1	2	2	2	3	4	3	4	4	4	5	5	5	4	5

Appendix A: An overview of scores assigned to each criteria for each identified system

REFERENCES

Akbar et al. (2015). Contextual Occupancy Detection for Smart Office by Pattern Recognition of Electricity Consumption Data. 10.1109/ICC.2015.7248381.

Andrew et al. (2014). Fast forward 2030. Retrieved February 22, 2021, from https://www.cbre.com/research-and-reports/future-of-work

ApolloTechnical. (2020, September 3). Surprising working from Home productivity Statistics (2021). Retrieved March 11, 2021, from https://www.apollotechnical.com/working-from-home-productivity-statistics/

Barkadehi et al. (2018). Authentication systems: A literature review and classification. Telematics and Informatics, 35(5), 1491-1511. doi:10.1016/j.tele.2018.03.018

Barry, J., & Feucht, K. (2020, December 03). 2021 commercial real estate outlook. Retrieved February 04, 2021, from https://www2.deloitte.com/us/en/insights/industry/financial-services/commercial-real-estate-outlook.html

BBC News. (2020, February 07). Apple fined for slowing down old iPhones. Retrieved February 23, 2021, from https://www.bbc.com/news/technology-51413724

Blonder. (1995, May 21). Transaction authorization and alert system.

Bloom, N. (2020, June 01). How working from home works out. Retrieved February 04, 2021, from https://siepr.stanford.edu/research/publications/how-working-home-works-out

Borodavkin, M. (2019). Smart Office Solutions in Modern Workplace.

BSIA. (2016, April). A specifiers guide to access control systems. British Security Industry Association. https://www.bsia.co.uk/publications/access-control/.

Chambers et al. (1998). The War for Talent. The McKinsey Quarterly. 3. 44-57.

Chow, L. K. (2005). The New Intelligent Building Index (IBI) for Buildings around the World – A Quantitative Approach in Building Assessment and Audit Experience with the Hong Kong Tallest Building, Two International Finance Centre (420m and 88-storey High). Tall Buildings. https://doi.org/10.1142/9789812701480_0142

Clements-Croome, D. J. 2013. *Intelligent Buildings: Design, Management and Operation*. 2nd ed. London: ICE Publishing.

Davies, A. & Adams, C. (2015, July 13). To err is human: Human error and workplace safety. Retrieved March 05, 2021, from https://www.shponline.co.uk/common-workplace-hazards/to-err-is-human-human-error-and-workplace-safety/

Deloitte Canada. (2015, June 17). Digital disruption in commercial real estate. Retrieved February 04, 2021, from https://www2.deloitte.com/ca/en/pages/real-estate/articles/digital-disruption-in-commercial-real-estate.html

De Ondernemer. (2020, October 25). Einde kantoortuinen: Maar hoe zien werkplekken er straks dan wel uit? Retrieved April 17, 2021, from https://www.deondernemer.nl/corona/coronavirus/kantoortuinen-werkplekken-thuiswerken~2573607

Divya, R., & Lavanya, R. (2020). *A Systematic Review on Gait Based Authentication System. 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS).* doi:10.1109/icaccs48705.2020.9074361

EY Belgium. (2020, April 08). Why remote working will be the new normal, even after covid-19. Retrieved February 04, 2021, from https://www.ey.com/en_be/covid-19/why-remote-working-will-be-the-new-normal-even-after-covid-19

Fridman et al. (2017). Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location. IEEE Systems Journal, 11(2), 513–521. doi:10.1109/jsyst.2015.2472579

Future Workplace. (2019). Future workplace wellness study. Retrieved February 09, 2021, from https://futureworkplace.com/ebooks/future-workplace-wellness-study/

Gabbatiss, J. (2019, January 22). 'Endangered' elements used to make phones are 'running out fast'. Retrieved February 24, 2021, from https://www.independent.co.uk/news/science/mobile-phones-elements-periodic-table-endangered-chemicals-st-andrews-a8739921.html

Gafurov et al. (2007). Gait Authentication and Identification Using Wearable Accelerometer Sensor. 2007 IEEE Workshop on Automatic Identification Advanced Technologies. doi:10.1109/autoid.2007.380623

Ghaffarianhoseini et al. (2016) What is an intelligent building? Analysis of recent interpretations from an international perspective, Architectural Science Review, 59:5, 338-357, DOI: 10.1080/00038628.2015.1079164

Google. (2021, April 26). Authenticator - Android-apps on Google Play. Google. https://play.google.com/store/search?q=authenticator&amp;c=apps&amp;hl=nl&amp;gl=US.

Hadhazy, A. (2016, June 12). Here's the truth about the 'planned obsolescence' of tech. Retrieved February 22, 2021, from https://www.bbc.com/future/article/20160612-heres-the-truth-about-the-planned-obsolescence-of-tech

Hendrikman, M. (2016, November 23). Eerste smart-tv's van PHILIPS uit 2009 verliezen Smart-functionaliteit. Retrieved February 22, 2021, from https://tweakers.net/nieuws/118171/eerste-smart-tvs-van-philips-uit-2009-verliezen-smart-functionaliteit.html

Herhold, K. (2019, June 18). 83% of Employees Want Some In-Office Working Time Over Working Fully Remotely. 83% of Employees Want Some In-Office Working Time Over Working Fully Remotely | Clutch.co. https://clutch.co/press-releases/83-employees-want-some-office-working-time-over-working-fully-remotely.

Jll. (2020, July 14). What the future holds for flexible space in a fast-paced world affected by the pandemic. Retrieved December 10, 2020, from https://www.us.jll.com/en/trends-and-insights/research/the-impact-of-covid19-on-flexible-space

Kainda et al. (2010). Security and usability: Analysis and evaluation. 2010 International Conference on Availability, Reliability and Security. doi:10.1109/ares.2010.77

Kawamoto et al. (2017). Effectively Collecting Data for the Location-Based Authentication in Internet of Things. IEEE Systems Journal, 11(3), 1403–1411. doi:10.1109/jsyst.2015.2456878

Kotera, Y., & Correa Vione, K. (2020, July 14). Psychological impacts of the new ways of Working (NWW): A systematic review. Retrieved March 11, 2021, from https://www.mdpi.com/1660-4601/17/14/5080

Kivistö, N. (2020, February 04). Smart Office: 3 Critical Technologies to Implement in 2020. Retrieved January 10, 2021, from https://www.steerpath.com/blog/smart-office-critical-technologies-to-implement-in-2020

Leifer, D. (1988), "Intelligent Buildings: A Definition", Architecture Australia 77: 200–202.

Marsh, R. (2017, June 8). Building lifespan and function - Yes, it really does matter in the Circular Economy! Retrieved March 10, 2021, from https://www.linkedin.com/pulse/building-lifespan-function-sustainability-yes-really-rob-marsh/

Masood, H., & Farooq, H. (2017). A proposed framework for vision based gait biometric system against spoofing attacks. 2017 International Conference on Communication, Computing and Digital Systems (C-CODE). doi:10.1109/c-code.2017.7918957

McCann, A. (2020, June 16). Coronavirus and working from home: Almost 60% of Americans Think covid-19 has changed the way we work for the better. Retrieved February 04, 2021, from https://wallethub.com/blog/coronavirus-and-working-from-home-survey/75534

Memoori. (2019, October 07). Designing & building for the complex life cycle of smart buildings. Retrieved March 05, 2021, from https://memoori.com/designing-building-for-the-complex-lifecycle-of-smart-buildings/

Milasi et al. (2020, June 22). Coronavirus pandemic reveals large differences in the prevalence of telework across the EU. Retrieved March 11, 2021, from https://ec.europa.eu/jrc/en/news/coronavirus-pandemic-reveals-large-differences-prevalence-telework-across-eu

Miller, J. (2019, April 16). Workplace wellness programs yield unimpressive results in short term. Retrieved February 09, 2021, from https://news.harvard.edu/gazette/story/2019/04/workplace-wellness-programs-yield-unimpressive-results-in-short-term/

Moore, S. K. (2021, June 29). How and When the Chip Shortage Will End, in 4 Charts. IEEE Spectrum: Technology, Engineering, and Science News. https://spectrum.ieee.org/tech-talk/semiconductors/devices/how-and-when-the-chip-shortage-will-end-in-4-charts.

Mørch, A. (2019, January 07). The Most Important Features for Your Smart Office in 2019. Retrieved January 10, 2021, from https://www.askcody.com/blog/the-most-important-features-for-your-smart-office-in-2019

Motwani et al. (2021). Multifactor door locking systems: A review. Materials Today: Proceedings. doi:10.1016/j.matpr.2021.02.708

Nationale Onderwijsgids. (2020, June 30). 'Studenten volgen liever volledig fysiek onderwijs dan volledig online onderwijs'. Nationale Onderwijsgids. https://www.nationaleonderwijsgids.nl/hbo/nieuws/54774-studenten-volgen-liever-volledig-fysiek-onderwijs-dan-volledig-online-onderwijs.html.

Needhidasan et al. (2014). Electronic waste - an emerging threat to the environment of urban India. Journal of environmental health science & engineering, 12(1), 36. https://doi.org/10.1186/2052-336X-12-36

Nelson et al. (2017). De strijd om talent win je met de juiste uitrusting. Retrieved February 16, 2021, from https://www.cbre.nl/-/media/cbre/countrynetherlands/campaigns/healthy%20offices/pdfs/healthy-offices-research-war-for-talent-nl-pdf.pdf

NEN. (2010). NEN 1824:2010 nl. Retrieved February 09, 2021, from https://www.nen.nl/nen-1824-2010-nl-145544

NLTimes. (2021, February 05). Most Dutch employees afraid of GETTING Covid at work: Trade unions. Retrieved March 11, 2021, from https://nltimes.nl/2021/02/05/dutch-employees-afraid-getting-covid-work-trade-unions

NOS Nieuwsuur. (2021, January 31). Wat doen deze bedrijven MET hun kantoorruimte? Retrieved February 04, 2021, from https://nos.nl/nieuwsuur/artikel/2366750-wat-doen-deze-bedrijven-met-hun-kantoorruimte.html

OCC. (2020, March 05). Third-Party relationships: Frequently asked questions to Supplement Occ Bulletin 2013-29. Retrieved March 05, 2021, from https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html

OpenPath. (n.d.). Physical Access Control Systems: PACS. OpenPath. https://www.openpath.com/blog-post/physical-access-control#what-to-look-for-in-pacs.

Oxford Dictionary. (n.d.). Oxford Dictionary - authentication. authentication noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com. https://www.oxfordlearnersdictionaries.com/definition/english/authentication.

Oxford Dictionary. (n.d.). Oxford Dictionary - intrusive. intrusive adjective - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com. https://www.oxfordlearnersdictionaries.com/definition/english/intrusive.

Pearson IT Certification. (2011, June 6). Understanding the Three Factors of Authentication. Understanding the Three Factors of Authentication | Pearson IT Certification. https://www.pearsonitcertification.com/articles/article.aspx?p=1718488.

Porter, M. E., & Heppelmann, J. E. (2015, October). How smart, connected products are transforming companies. Retrieved March 05, 2021, from https://hbr.org/2015/10/how-smart-connected-products-are-transforming-companies

Pouwels, A. (2020). Open plan offices - the new ways of working. the advantages and disadvantages of open office space - think tank. Retrieved March 12, 2021, from https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_BRI%282020%29659255

Randstad. (n.d.). Dit zijn DE MEEST GEVRAAGDE BEROEPEN in Nederland. Retrieved February 15, 2021, from https://www.randstad.nl/werknemers/blog/de-meest-gevraagde-beroepen-in-nederland

Rhodes, B. (2014, July 1). Lifespan of electronic access control systems. IPVM. https://ipvm.com/reports/lifespan-of-typical-access-systems.

Rijksoverheid. (2012). Building regulations. Retrieved February 09, 2021, from https://business.gov.nl/regulation/building-regulations/

Robinson, B. (2020, June 19). Is working remote a blessing or burden? Weighing the pros and cons. Retrieved February 04, 2021, from https://www.forbes.com/sites/bryanrobinson/2020/06/19/is-working-remote-a-blessing-or-burden-weighing-the-pros-and-cons/

RS2 Technologies. (2008). Total Cost of Ownership (TCO)   for Access Control Systems. https://rs2tech.com/wp-content/uploads/RS2_WP_TCO.pdf.

RTL Nieuws. (2014, June 27). Kantoorpand Zuidas VOOR 200 Miljoen verkocht. Retrieved February 08, 2021, from https://www.rtlnieuws.nl/geld-en-werk/artikel/1800426/kantoorpand-zuidas-voor-200-miljoen-verkocht

Ryu et al. (2021). Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3061589.

Sánchez et al. (2019). Securing Smart Offices Through an Intelligent and Multi-device Continuous Authentication System. 10.1007/978-981-15-1301-5_7.

Schouten, E. (2020, October 16). Bierbrouwers gaan bij tweede Horecasluiting voor maatwerk. Retrieved February 22, 2021, from https://www.nu.nl/economie/6084338/bierbrouwers-gaan-bij-tweede-horecasluiting-voor-maatwerk.html

Sid, S. (2020, January 06). What do employees want from workplace? 6 shocking truths! Retrieved February 09, 2021, from https://101productivity.com/what-do-employees-want-from-their-workplace/

So et al. (1999), "A new definition of intelligent buildings for Asia", Facilities, Vol. 17 No. 12/13, pp. 485-491. https://doi.org/10.1108/02632779910293488

Someka. (2021, April 7). How to Make Decision Matrix in Excel to Make Better Decisions! Someka. https://www.someka.net/blog/how-to-make-decision-matrix-in-excel/.

Stanford. (1999, March 1). Sharing information to boost the bottom line. Retrieved March 05, 2021, from https://www.gsb.stanford.edu/insights/sharing-information-boost-bottom-line

Sudha, L. R., & Bhavani, D. R. (2011). Biometric authorization system using gait biometry. *arXiv preprint arXiv:1108.6294*.

Tao et al. (2012) Person Authentication and Activities Analysis in an Office Environment Using a Sensor Network. In: Wichert R., Van Laerhoven K., Gelissen J. (eds) Constructing

Tessares. (2020, July 14). Working from home, the importance of upload speed. Retrieved February 04, 2021, from https://www.tessares.net/working-from-home/

Twingate. (2020, June 15). Internet security research - cybersecurity in the age of coronavirus. Retrieved February 04, 2021, from https://www.twingate.com/research/cybersecurity-in-the-age-of-coronavirus/

US Bureau of Labor Statistics. (2020, June 25). AMERICAN TIME USE SURVEY —2019 RESULTS. Retrieved February 04, 2021, from https://www.bls.gov/news.release/pdf/atus.pdf

Van Barneveld. (2020). Peiling provincie: één op de tien Utrechtse ondernemers denkt failliet te gaan. Retrieved February 22, 2021, from https://www.ad.nl/utrecht/peiling-provincie-een-op-de-tien-utrechtse-ondernemers-denkt-failliet-te-gaan~a77d89e8/

Velásquez et al. (2018). Authentication schemes and methods: A systematic literature review. Information and Software Technology, 94, 30-37. doi:10.1016/j.infsof.2017.09.012

Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*. Springer. https://doi.org/10.1007/978-3-662-43839-8

Wolfswinkel et al. (2013). Using Grounded Theory as a Method for Rigorously Reviewing Literature. European Journal of Information Systems. 22. 10.1057/ejis.2011.51.

Wong et al. (2005). Intelligent building research: a review. *Automation in construction*, *14*(1), 143-159.