‘What’ you are to show ‘who’ you are
User Acceptance of Biometrics in eHealth Video Consultations

Bartjan L. Happel
October 19, 2017

Radboud Universiteit Nijmegen

Master Thesis
Science, Management & Innovation Master Track
Faculty of Science, Radboud University Nijmegen

Keywords
Video Call - Biometric Authentication - User Acceptance

Business Information
Philips Research
Marcel Quist

University Information
Supervisor - Raphaël Smals
2nd reader - Lilian Beijer

Student Information
Bartjan L. Happel, s4125916
Mathematics

Start date: February 1, 2017
Presentation date: TBA
Abstract

To determine the feasibility and user acceptance of biometrics as login for the Philips online audio-video consultation service, a mixed-method research strategy was used.

In-depth interviews with experts in security and biometrics revealed that biometrics may not be usable for foolproof evidence of identity, but it can be used for identity verification. During short, structured interviews healthcare professionals spoke about the need for approachable ways of communicating with patients, and showed their interest for user friendly, biometric means of identity verification. In a survey, patients showed little above average acceptance for three of the six asked biometric methods, provided enough safety measures are taken. While prior factors of innovativeness, trust in technology and concern for data privacy (as described in Miltgen, Oliveira and Popović (2013)) did not seem to impact acceptance, antecedent factors like compatibility, usefulness and facilitating conditions did. In conclusion, it is recommended to implement a biometric login into demonstrators, to show the possibilities to the end users. However, there are some conditions and requirements that must be met.
Executive Summary

Research Questions

The following questions created the basis for this study.

Main question

What are the biometric modalities that are considered acceptable by users, both healthcare professional and patient, for patient authentication during online audio/video consultations, and what do different experts think about the implementation of such a system?

Sub-questions

1. What is the opinion of experts on the use of biometrics as a means of patient authentication?
2. What are the methods of biometric authentication that can be used in the audio-video consulting service as the Philips team is designing it?
3. What is the level of user acceptance among healthcare professionals concerning biometrics, when used to authenticate patients during online consultations?
4. What is the level of user acceptance among patient concerning biometrics, when used to authenticate them in online consultations?
5. What factors are correlated to the patient user acceptance of biometric authentication in a healthcare context?

Research Methods

This study was conducted with a mixed-method research strategy, consisting of:

- Four in-depth, semi-structured interviews with experts in the areas of security, biometrics and information management,
- Seven structured interviews with healthcare professionals, differing in specialisation and amount of different patients,
- 126 filled out surveys, completed by participants who are familiar with the current, in-hospital consultations.

Interviews were first thematically analysed, after which they were coded inductively. Descriptive statistics were used to visualise the results of the survey, while calculations of several correlation coefficients were used to determine dependencies between factors of acceptance.
Results and Analysis

Results from Team Conversations
Through conversations with the Philips team, to find out the requirements and demands that a usable biometric modality needs to fulfil, a list of six usable biometrics was created. These six biometrics, included in the survey, are face recognition, speaker recognition, eye blood vessel recognition, hand geometry, ear geometry and fingerprint recognition.

Results from Interviews
Speaking with experts in security and biometrics, and after a study of available literature, it became clear that the usage of terms concerning identity (e.g. identification, verification and authentication) do not follow clear definitions when biometrics are concerned.

While in the field of biometrics, authentication and verification are used for the same action (comparing the biometrics of a person to that in a database), this action does not seem to produce enough proof to be called a true authentication attempt in a security context. Here, only some secret exclusively known by the person who is authenticating can be used to generate definitive proof. Meanwhile, the three pillars of authentication (something you know, have or are) clearly leaves room for biometrics in its definition. All except the security expert see a future for biometrics, albeit under some requirements on safety, fraud detection, minimised error rates and a fail-safe.

Most healthcare professionals were positive about the use of biometrics to create a more user friendly login for patients. They did create a similar list of requirements as the experts (safety and fail-safes), adding the preference of authentication done before the consultation starts (saves time) and simplicity for the healthcare professional (do not show an excess of information).

Results from Survey
The survey shows that the three most accepted methods are fingerprint recognition, face recognition and speaker recognition. Interestingly, out of the six included biometrics, these three are frequently used (e.g. fingerprint sensors in smartphones) or seen in popular media (e.g. TV shows). It seems that knowledge of (or familiarity with) biometric methods could have quite an influence on the acceptance.

When asking whether or not participants would accept these three biometrics, an average of 61.09% answers with ‘yes’, 26.44% answers with ‘maybe’ and 12.47% answers with ‘no’. In addition, participants had the opportunity to state requirements or demands for the usage of the system, and often stated categories are ‘fraud detection’, ‘security’, ‘ease of use’ and ‘trusted supplier’.

When calculating the presence and significance of correlations between different factors of acceptance, it shows that the three tested ‘prior factors’ (innovativeness, trust in technology and concern for data safety) have no significant correlation with acceptance. However, all ‘antecedent factors’ (compatibility, ease of use, usefulness, social influence, facilitating conditions and perceived risks) do show significant, either moderate or even strong correlations.

Conclusions

Conclusions
Experts see the potential benefit of using biometrics, but give warning that using only biometrics may lead to patients not being recognised (and getting frustrated with the system). They therefore recommend implementing a fail-safe (perhaps a password/-phrase) for those cases.

The six biometrics usable in the context of this study, and chosen to be tested in the survey,
are face-/speaker recognition, hand-/ear geometry, recognition of blood vessels in the sclera and fingerprint recognition. All of the above, except fingerprint recognition, can be implemented with the use of the camera and microphone on a patients device (either smartphone/tablet/laptop, or PC with webcam and microphone). Fingerprint recognition requires an additional sensor, which currently is available in multiple smartphones. Therefore, in the future it might be possible to use the fingerprint sensor on a smartphone as a ‘key’ to gain access to audio-video consultations.

Healthcare professionals would prefer a method able to work before the start of an consultation. For that reason they favour face-/ and fingerprint recognition, as they are easiest to use (and do not require the patient to speak to their device, without a second party being present). While ear-/hand geometry and sclera blood vessel recognition can be used before consultations, interviewees were more interested in the better known methods.

From the biometric modalities usable during audio-video consultations, face-, speaker- and fingerprint recognition scored highest on acceptance with the patient users. Hand- and ear geometry consistently scored lower, while sclera blood vessel recognition often scored between these two groups.

In this study there is no evidence found that prior factors influence the acceptance of biometric methods. However, it was shown that antecedent factors do influence acceptance, and should therefore be the focus when explaining biometric systems to patients. In addition, it seemed the ‘new’ antecedent factor of ‘knowledge of…/familiarity with…’ influenced acceptance as well.

Recommendations
I would recommend that the Philips team implements biometric authentication in the service, in demonstrators through ‘biometrics-as-a-service’ and in a final product by purchasing biometric software. Recommended modalities are face- and speaker recognition, as they both score high on acceptance, and are relatively easy to implement.

Furthermore, I suggest using both (or even more) modalities to create a multimodal system, increasing security and fraud detection. Look into the option to have authentication take place before the consultation start, nullifying additional duration for healthcare professionals.

I would advice putting a fail-safe (e.g. password/-phrase) in place, in case the system falsely records a non-match, and finally I would recommend giving the patient users the option not to use the biometric login (but another form of authentication), so patients do not feel like this system is forced upon them. This way, patients can more gradually get used to the idea of biometric logins, and later decide to start making use of the system.
# Contents

**Abstract**  
2

**Executive Summary**  
Research Questions .................................................. 5  
Research Methods ....................................................... 5  
Results ................................................................. 6  
Conclusions ............................................................... 6

**Acknowledgements**  
11

**Definitions**  
11

1 **Introduction**  
1.1 Background and Motivation for Research .......................... 15  
1.2 Role within Philips .................................................... 16  
1.3 Problem Definition .................................................... 16  
1.4 Relevance ............................................................... 17  
1.5 Research Objectives and Questions .................................. 17  
1.6 Reading Guide .......................................................... 18

2 **Literature and Theoretical Framework** ................................ 19  
2.1 Authentication ......................................................... 19  
2.2 Biometrics ............................................................... 19  
2.3 Safety, Ease of Use and Functionality ............................... 23  
   2.3.1 Safety ............................................................. 24  
   2.3.2 Ease of Use and Implementation ................................ 26  
   2.3.3 Functionality ...................................................... 27  
2.4 Acceptance .............................................................. 27  
   2.4.1 Technology Acceptance .......................................... 28  
   2.4.2 End User Acceptance Model .................................... 28

3 **Research Methods** ..................................................... 31  
3.1 Research Strategy ..................................................... 31  
3.2 Data Collection ....................................................... 32  
3.3 Data Analysis .......................................................... 34  
3.4 Research Ethics ........................................................ 35
4 Results and Analysis
  4.1 Results from Team Conversations .............................................. 37
     4.1.1 Requirements ............................................................. 37
     4.1.2 Potential Biometric Modalities ........................................... 37
  4.2 Results from Interviews .......................................................... 39
     4.2.1 Prior Factors Healthcare Professionals .................................... 39
     4.2.2 Expert Opinion and Healthcare Professional Acceptance ................. 41
  4.3 Results from Survey ................................................................ 46
     4.3.1 Patient User Acceptance .................................................... 46
     4.3.2 Correlations ..................................................................... 54

5 Conclusions and Recommendations ...................................................... 59
  5.1 Sub-questions ............................................................................ 59
     5.1.1 Sub-Question 1: Expert Opinion .............................................. 59
     5.1.2 Sub-question 2: Usable Biometrics in Philips Context ................. 60
     5.1.3 Sub-Question 3: Healthcare Professionals User Acceptance ........... 60
     5.1.4 Sub-Question 4: Patient User Acceptance .................................. 61
     5.1.5 Sub-Question 5: Factors for Patient User Acceptance .................. 61
  5.2 Main Question: Feasibility of Biometric Authentication ..................... 62
  5.3 Additional Conclusions ............................................................... 62
  5.4 Recommendations ..................................................................... 63
  5.5 Limitations ............................................................................... 64
  5.6 Possibilities for Further Research ............................................... 64

References ................................................................................. 67

Appendices .................................................................................. 70

A Outlines ................................................................................... 71
  A.1 Survey Outline ..................................................................... 71
  A.2 Interview Outline Healthcare Professionals ............................... 74

B Interviews .................................................................................. 75
  B.1 Interviewee List ..................................................................... 75
  B.2 Coding Experts ..................................................................... 76
  B.3 Coding Healthcare Professionals .............................................. 77

C Survey Results ........................................................................... 79
  C.1 Descriptive Statistics ............................................................... 79
  C.2 Survey Question 28 Answers ................................................... 83
  C.3 Acceptance Comparison ........................................................... 86
  C.4 Correlation Significance ............................................................ 87

D Sample Size Calculation .................................................................. 89

E Biometrics-as-a-Service ................................................................ 91
Acknowledgements

I would like to thank my university coach Raphaël Smals. You managed to teach me a lot about conducting societal research (which is quite the feat, because as a mathematician this was all quite new to me). Thank you Lilian Beijer, for being the second academic reader. Even though we have had no contact during this study, I hope the resulting thesis will live up to your standards.

I thank the TeleHealth team at Philips Research. Marcel Quist, Zoran Stankovic and Karin Klabunde, Daniëlle van Oers, Georgiana Manolache, Arjen Draisma and Kevin Sanders. I loved working as part of your team on a service we all believe in, and I hope to see it in practice soon! Furthermore, thank you all for your patience. Finishing the writing of this thesis took (a lot) more time than I expected, but I hope the final thesis is worth the wait.

Gijs Geleijnse, thank you so much for helping me with getting ICBE approval for this study. Without you I would probably still be filling out study documents.

In addition, I thank Janne Miltenburg who, even when my motivation was at its lowest, managed to kick me back into ‘writing mode’.

One big thanks to all interviewees and survey participants, without whom this study would not have been possible. I have learned a lot from you, and appreciate your input.
Definitions

**Biometric Modalities:** Also called *biometric factors* or, for short, *biometric*. A biometric modality is the set of systems depending upon a specific human trait, e.g. fingerprints.

From ‘The Guide to Data Protection’ (ICO., 2017):

**Personal Data:** “Personal data means data which relate to a living individual who can be identified either from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect to the individual.” (ICO., 2017)

**Data Subject:** “Data subject means an individual who is the subject of personal data.” (ICO., 2017)

**Sensitive (Personal) Data:** Sensitive personal data means personal data consisting information about the data subject, as to

(a) racial or ethnic origin,
(b) political opinions,
(c) religious beliefs or other beliefs of a similar nature,
(d) whether the data subject is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) physical or mental health condition,
(f) sexual life,
(g) the commission or alleged commission by the data subject of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

**Data Controller:** “Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.” (ICO., 2017)
Chapter 1

Introduction

1.1 Background and Motivation for Research

Philips N.V. is a diversified technological company that wants to improve the life of people by creating meaningful innovations in the areas of healthcare, consumer lifestyle and lighting. The healthcare branch of Philips is market leader in cardiological care, critical care and care at home.

This project takes place within the Philips Research department, a global organization that helps Philips introduce meaningful innovation that improve people’s lives. At Philips Research, technology options for innovations are provided in the area of health and well-being, targeted at both developed and emerging markets.

The topic of this thesis is the end user acceptance of biometric authentication in a healthcare context. In addition to being of interest to Philips, the acceptance of biometrics and biometric authentication has both societal and academic relevance. Now that the digital age is flourishing, and every day more information is stored in the cloud, one societal issue is the following: how can we properly secure access to personal information? The system most often used is the established username and password combination. For better security, you should not use your password on multiple places (once stolen, thieves have access to more of your information) and many businesses require you to change your password every (other) month. In addition, many account management systems still require at least one capital letter, one digit and one symbol. This means having ten user accounts would require you to remember 60 to 120 different passwords each year, every year. Due to the complex composition rules, this could lead to passwords left on sticky notes on desks. Can the use of biometrics contribute to the creation of a more user friendly, and potentially more secure system?

The demand for secure login systems often rises from the need to protect (sensitive) data. A specific location where access to data, both online and offline, must be well-guarded, is in the healthcare sector. Personal medical files often include sensitive information which should not be disclosed to unauthorized people. In addition, the quality of the data can be increased when the data can be retraced to the rightful owner. Due to the digitalization of the healthcare sector, video consults are starting to gain followers among both patients and physicians. The former will forego travel- and waiting times by simply conversing with their healthcare professional from the comfort of their own home, while the latter can now choose to work from home and

\footnote{However, research by Chiasson and Van Oorschot (2015) shows password expiration often means people use predictable transformations of old passwords, and states that \textit{“the security benefit of password ageing policies are at best partial and minor”} (Chiasson \& van Oorschot, 2105).}

\footnote{In a 2017 NIST document the focus changes, favouring longer passwords and user friendliness while foregoing composition rules and forced expiration.}
even outside of regular office hours.

However, Wildenborg (2017) states in her article for the Dutch newspaper ‘De Gelderlander’ that ‘the patient does not visit the digi-doctor’. A reason for this statement is that patients are ‘unaware of the possibility’, while patients who do make use of the service often stop because programs are not user friendly. “Patients have to login with DigiD and an SMS code, or have to gain permission from their physician to create an account. They quickly think: I’ll just phone them” (Wildenborg, 2017). This second part, about user unfriendly logins, plays in favour of biometrics, and shows the relevance of a study into biometric logins for patients. Dr. L.M. Visser (2017) concludes in her PhD thesis that a transformation is needed in ‘norms about abilities, knowledge, and expertise that patients and healthcare professionals need’. In addition, ‘changes in the education of healthcare professionals could, for example, play a large role in this transformation’ (Visser, 2017). This, however, lies outside the scope of this study.

In the context of the Philips team, biometric logins are used in telehealth consultations. During such E-Health video calls, there is a two way information stream, from the medical file to the patient and back from the patient to the medical file. To secure access to the information, and increase quality of said information, the healthcare professional must be sure that he is speaking with the correct patient. This is one of the reasons why the World Health Organization (WHO) considers “Patient Identification” as one of the top “Patient Safety Solutions” (World Health Organization, 2017), and the WHO mentions the use of biometrics to increase the security of patient identification multiple times (World Health Organization, 2007). Patient identification is important for (at least) two reasons. Firstly, correct identification results in a decrease of the amount of information given to the wrong person. Disclosing medical information to an unauthorized person is not only a breach of the privacy of the patient, it also breaks the Hippocratic oath (“I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know” (Lasagna, 1964)). Secondly, misidentification can cause the pollution of medical records. In a study by Imprivata it is seen that “the average [American] hospital loses $17.4 million per year in denied claims resulting from misidentification” (Imprivata, 2016). Is in this context the use of biometrics acceptable for both patients and healthcare professionals to increase the certainty of correct access? And what factors play a role in changing the user acceptance?

1.2 Role within Philips

The project is part of a larger innovation created within the TeleHealth Video Services team, which lies under the ‘Professional Health Solutions and Services’ specialization in Philips Research. The TeleHealth Video Services team drives innovation to market for video solutions, such as video communication between healthcare professionals and patients. The team is taking their current video solution to market, but they still seek to innovate upon their service. The assignment aims to determine if the addition of biometrics as an additional service, is accepted by end users. If biometric authentication is accepted by both end user groups, the team wants to build a demonstrator which enables them to show this service to potential clients.

1.3 Problem Definition

When looking at the topic from an academic point of view, relevance can be seen in determining of a way to ‘test’ user acceptance of biometrics. A lot of literature exists explaining technology acceptance testing, but much less is available for the specific technology of biometrics, even without considering the context of healthcare. The model proposed by Miltgen and others
(described later, (Miltgen, Oliveira, & Popović, 2013)), makes for a good starting point, but can it be used in a sensitive context such as healthcare, and do the same dependencies and correlations hold? Two limitations of Miltgen’s study are the usage of only one biometric and the restriction on the age of participants. The academic relevance of this thesis is to utilize the model from Miltgen and see if its application in healthcare, and usage on a wider age range and with more biometrics, gives rise to similar results. To summarize the academic problem this thesis aims to solve in one sentence:

What are the biometric modalities that are considered acceptable by users, both healthcare professional and patient, for patient authentication during online audio/video consultations, and what do different experts think about the implementation of such a system?

1.4 Relevance

The academical relevance of this thesis lies in the determination of factors that have an effect on the final acceptance of biometric technology in a healthcare context. While studies exist studying the acceptance of biometrics to gain access to banking applications, there is less literature available searching for the patient acceptance of biometric login to healthcare applications. In addition, there exists even less research into the factors that influence acceptance in such a particular scenario. No validation has been found that proves biometric access to (sensitive) medical information can be compared to biometric access to banking information, or that biometric technology can be compared to other access technology.

On a societal level, there is both a need for better protection of personal (and sensitive) information that is stored online, and there is an increasing call for fast access between healthcare professionals and patients.

For Philips, the relevance of this project is more biased towards the feasibility of implementation. For the team, the results of the user acceptance test are more important, paired with the opinions of the healthcare professional users and experts in security, data management and biometrics. The Philips team has created an audio-video consultation service, which they are pushing to the market at this very moment, and this research is aiming to show them whether implementing biometric authentication is a valid addition to their existing service.

1.5 Research Objectives and Questions

The following sub questions are defined to each answer part of the main problem:

1. What is the opinion of experts on the use of biometrics as a means of patient authentication?
2. What are the methods of biometric authentication that can be used in the audio-video consulting service as the Philips team is designing it?
3. What is the level of user acceptance among healthcare professionals concerning biometrics, when used to authenticate patients during online consultations?
4. What is the level of user acceptance among patient concerning biometrics, when used to authenticate them in online consultations?
5. What factors are correlated to the patient user acceptance of biometric authentication in a healthcare context?
1.6 Reading Guide

The following text exists out of various chapters. Chapter two describes the context of my role within the team in Philips, and the technological context that is useful to more easily read this thesis. Chapter three shows the literature and the theoretical framework, keystones of the research, in addition to the research methods of data collection and analysis. In chapter four, the reader can learn more about the ethics and the process of the Internal Committee for Biomedical Experiments passed before starting the study. The second part of chapter four describes all results gathered from all data sources, and their respective analyses. Directly following the results comes chapter five, where the results are discussed and their relevance is shown. This thesis is concluded with chapter six, where the reader can find the conclusion and recommendations for further research. After this last chapter the references can be found, and additional data in the appendices.
Chapter 2

Literature and Theoretical Framework

In this chapter, the main goal is to describe the theory and the approach used to tackle the problem. Sections include user acceptance and research models.

2.1 Authentication

In the world of security, the difference between identification and authentication lies in the question that needs answering. Identifying a person can be seen as asking ‘who are you?’, while authenticating a person can be seen as asking ‘how can you prove who you are?’. In the biometric context, the term authentication is often used for verification. Where authentication aims to prove, without a doubt, that a claim of identity is correct, verification simply verifies the claim, and states that the claim is (in)correct compared to some previously determined threshold (more on that later).

As described in Biometrics - Personal Identification in Networked Society (Jain, Bolle, & Pankanti, 2002), there are three ‘pillars’ that can be used for authentication. The first pillar is something you ‘know’ (the knowledge factor), which can be a password or pin code. The second pillar is something you ‘have’ (the possession factor), like a house key or a security badge. The third pillar is something you ‘are’ (the inherence factor), and it is at this place that biometrics come up. In addition to these three pillars, a fourth factor (the context factor, describing ‘where’ you are) can be used to strengthen the claim. Context can be provided by you IP-address, GPS location or even previous online purchases when using a mobile banking app.

2.2 Biometrics

The word ‘biometrics’ originates from the Greek words bios (life) and metrikos (measure), and can be interpreted as a measurable aspect of a life form, usually a human being. As mentioned above, biometrics represent the third pillar of authentication methods: something you ‘are’. Within biometric authentication, there are two main fields to consider: biological and behavioural aspects. The biological aspect splits up in morphological (also called randotypic or phenotypic) information, which is “completely random”, and genotypic information, which is “completely determined by genetics”. Behavioural information is “completely determined by training” In addition, ‘unchanging marks’ can be used to further identify a person, as stated
in the article *On the reconstruction of biometric raw data from template data* (Bromba, 2006). See Figure 2.1 below for a typology of biometric authentication methods.

**Figure 2.1:** Typology Biometric Authentication Methods (Bromba, 2006). Biometrics are divided into three categories: factors a person is born with (biological), factors developed throughout a person’s life (behavioural) and ‘unchanging marks’, which can be used to indirectly identify a person.

To determine whether or not a biometric factor can be used for authentication, there are seven requirements that must be met (Jain et al., 2002):

- **Universality**: the biometric should be possessed by as many people as possible,
- **Uniqueness**: the biometric should be different for (almost) everyone,
- **Permanence**: the biometric should not change (much) over time,
- **Collectability**: the biometric should be easy to see/collect,
- **Performance**: the biometric should achieve a high accuracy and low error rates,
- **Acceptability**: the biometric should be accepted by the public,
- **Hard to Circumvent**: it should be difficult (and costly, both in time and money) to ‘fool’ the system.
In Jain et al., a table is used to score several biometrics on these seven requirements:

### Table 2.1: Comparison of Biometric Factors.

<table>
<thead>
<tr>
<th>Biometrics</th>
<th>Universality</th>
<th>Uniqueness</th>
<th>Permanence</th>
<th>Collectability</th>
<th>Performance</th>
<th>Acceptability</th>
<th>Hard to Circumvent</th>
<th>Scoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>7</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>11</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>8</td>
</tr>
<tr>
<td>Keystrokes</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>3</td>
</tr>
<tr>
<td>Hand Vein</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>8</td>
</tr>
<tr>
<td>Iris</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>11</td>
</tr>
<tr>
<td>Retinal Scan</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>9</td>
</tr>
<tr>
<td>Signature</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>4</td>
</tr>
<tr>
<td>Voice Print</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>4</td>
</tr>
<tr>
<td>Face Thermograms</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>11</td>
</tr>
<tr>
<td>Odour</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>7</td>
</tr>
<tr>
<td>DNA</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>8</td>
</tr>
<tr>
<td>Gait</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>6</td>
</tr>
<tr>
<td>Ear</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>9</td>
</tr>
</tbody>
</table>

Note: The data is based on perception of three biometric experts. (Jain et al., 2002, page 16). The fourteen biometric are scored on the seven requirements. Total score uses high (two points), medium (one point) and low (zero points).

It is important to notice that this table originates from the year 2002. At that time, less research had been conducted into sclera vein recognition (which is why this factor is not included in the table). In addition, research in other factors has not been standing still, meaning that some values may be outdated. Moreover, anti-spoof measures have improved as well; increasing the amount of effort (both in time and in costs) it takes to circumvent the system. The scoring column assigns two points for every ‘high’ score, one point for every ‘medium’ score and zero points for every ‘low’ score. It does not differentiate or weigh the independent factors. Considering this score, the three ‘best’ biometrics would be fingerprints, iris scans and face thermograms (each eleven points). Ear geometry and retinal scans follow on the fourth place with nine points, after which hand geometry, hand vein and DNA are tied for sixth place with eight points each. Tied for ninth place are face recognition and odour, each seven points, on eleventh place is gait with six points. Both signature and voice print take twelfth with four points, and keystrokes takes last place with three points.
A biometric system works in the following way, as seen in Jain et al. (2002, page 20-21):

“**A biometric-based identification (authentication) system operates in two distinct modes: enrolment and identification (authentication).** During enrolment, biometric measurements are captured from a given subject, relevant information from the raw measurement is gleaned by the feature extractor, and (feature, person) information is stored in a database. Additionally, some form of ID for the subject may be generated for the subject (along with the visual/machine representation of the biometrics).

In addition, Jain explains how during authentication, the claimer of an identity presents both the ID (if generated) and the biometric. The system then extracts the features and tries to match these to the template. After this, the system can either accept or reject the claim. This essentially means each biometric system has to complete four steps. Step one is the enrolment (and creation of a template). During the authentication three steps are taken: the collection of a live sample, the comparison with the template, and the scoring of the comparison. The system itself can only score the comparison and needs a decision threshold (often a number between 0 and 100) to generate an accept or reject. When considering biometrics, even more so when comparing them to other forms of authentication (passwords, for example), it is important to take two error rates into account. The first one, the False Match Rate (FMR), is the probability that the system finds a match where it should not. The second, called False Non Match Rate (FNMR), is the probability of a system finding no match, where it should find one. The FMR represents the percentage of matched imposters, FNMR represents the percentage of non-matched ‘reals’. Deciding the location of the decision threshold depends on the trade-off between these two rates. Decreasing the FMR, and therefore decreasing the odds of an imposter gaining access, increases the FNMR and, consequently, the odds of a real match being denied access. It depends on the application which error rate is more important, as also seen in Figure 2.2. Here instead of the FMR and FNMR, the similar False Accept Rate (FAR) and False Reject Rate (FRR) are used respectively. These are very similar, but FMR and FNMR are the ISO terms.

![Detection Error Tradeoff Curve](image)

**Figure 2.2:** Detection Error Tradeoff Curve (Jain et al., 2002).

When FAR increases, FRR decreases (and vice versa). Equal Error Rate is the rate where FAR equals FRR.

To determine the performance of a biometric system, there are several metrics than can be used. One of the popular metrics is the Half Total Error Rate (HTER). This calculates half of the
sum of the FMR and the FNMR (and can be calculated by $\text{HTER}(\Delta) = \frac{\text{FMR}(\Delta) + \text{FNMR}(\Delta)}{2}$).

Another metric is the Equal Error Rate (EER). This is the point where the FNMR equals the FMR, and can be calculated by setting

$$\text{EER} = \text{FMR}(\Delta_*) = \text{FNMR}(\Delta_*), \text{ where } \Delta_* = \arg\min_{\Delta}(|\text{FMR}(\Delta) - \text{FNMR}(\Delta)|)$$

(Poh, Chan, Kittler, Fierrez, & Galbally, 2012). This means $\Delta_*$ equals the threshold where the difference between the FMR and the FNMR is minimal (equal to a small value $\epsilon$ that is negligible). Because indeed the difference between FMR and FNMR does not necessarily have to be zero, the EER is often set to $\text{HTER}(\Delta_*)$. “A metric becomes a performance criterion when it is used to obtain a threshold but not for performance reporting. In biometrics evaluation, it is common to use FMR as a performance criterion and report the system performance in FNMR, and vice versa.” (Poh et al., 2012). An elegant criterion is the Weighted Error Rate (WER), adding the additional variable $\beta$ to the mix:

$$\text{WER}_\beta(\Delta) = (1 - \beta)\text{FNMR}(\Delta) + (\beta)\text{FMR}(\Delta)$$

where $\beta \in [0, 1]$ adjusts the contribution between FMR and FNMR (Poh et al., 2012). As seen in Figure 2.2, forensic applications often have a high FAR and a low FRR. This is due to the fact that with forensics, the expert wants to find a match in a database, after which the (blood-)sample can be tested against this match for a more definitive result. On the other end of the spectrum are high security access applications, where the FRR is very high but the FAR very low. While employees may not like it to have to check in multiple times to be recognized, it is far more important that imposters do not get access to these buildings. Somewhere in the middle the civilian applications are found, who often balance the FAR and the FRR, sometimes leaning more towards either one.

The important take-away is that while different methods exist that show the performance of a biometric system, the outcomes of those methods are not identical. Therefore is may depend on the final application whether it is better to use the HTER or the EER.

### 2.3 Safety, Ease of Use and Functionality

Within authentication, there exists a practical tradeoff between three factors. The first factor is the security of a system, which deals with how secure information is stored and how secure communication takes place. The second factor is the ease of use, dealing with how fast a user can get used to a system and how easy they can work with it. The final factor is functionality, the number of actions the user can take with the system, and the number of functions the system can offer the user. As seen in Figure 2.3, increasing one factor has implications for the other factors. More functionality means more points of entrance for malicious attacks (less security), and may cause new users to get lost in the possibilities (less ease of use). More security may limit the points of entrance, therefore limiting functionality, while also requiring additional steps to safely connect (less ease of use). Finally, increasing ease of use may require less from the user, which potentially decreases safety, and does not give the user unnecessary information, decreasing functionality.
Figure 2.3: ‘Triad: Security, Functionality, Ease of Use’ (Waite, 2010). This picture shows the difficulty of maximizing the three aspects at the same time, as increasing two aspects is hypothesized to lead to a decrease in the third.

Now the challenge for every business operating in software and technology is the following:

_How to find balance between security, functionality and ease of use?_

Because of innovations, this question is slowly becoming easier to answer. Due to the fact that people are getting better at using technology, increasing functionality will not necessarily rapidly decrease the ease of use. At the same time, technological advancements may be able to create biometric authentication systems that are both easy to use and have an adequate level of security. Now, the three factors will be explored within the context of biometrics.

2.3.1 Safety

Safety (or ‘strength’) of an authentication method is defined as the ability of that method to protect your personal data from unauthorized access. Standards exist for the safety of authentication methods, such as the international ISO/IEC JTC 1/SC 37 Biometrics (Miller, 2002), the BS ISO/IEC 19794 Series (British Standards Institution, 2009), the Dutch NEN-ISO/IEC 24761:2009/C1:013en (van Zetten, 2013), the NEN 7510:2011nl (Commissie Informatievoorziening in de Zorg, 2011) and NEN 7512:2015nl (Nederlands Normalisatie-instituut, 2015). However, further investigation of the standards is out of scope for this study.

At this time, when patients want access to their EMR (Electronic Medical Record) in the Netherlands, they require to show a valid form of identification. However, as previous research has shown (Panis, 2015), out of forty consumers, five managed to get a copy of their medical dossier without showing any form of identification. Using biometrics for every access to medical records through audio-video consults would thus provide a more consequent way of authentication. There is also the Dutch standard eIDAS for e-recognition (eHerkenning, n.d.), going from a basic level, to substantial and to a high level, but as of October 19, 2017 this standard does not incorporate biometric authentication methods. The basic level requires only username/password, the substantial level requires a two-factor login, with username/password and text verification code and the high level requires PKI-certificate (Public Key Infrastructure). The intricacies of such systems are left out of scope.

Another example is the STORK project tries to create an European “Quality Authentication Assurance” system and is composed of four levels. The system generates the assurance level based on three aspects during registration (“quality levels of the identification procedure, of the credential issuing process, and of the entity issuing the credential”) and two aspects during the electronic authentication phase (“quality levels of the type and robustness of the credential, and of the security of the authentication mechanism”) (Hulsebosch, Lenzini, & Eertink, 2009).
Finally, a draft from the National Institute of Standards and Technology proposes the Strength of Function for Authenticators (SOFA) framework, with the purpose “to provide guidance for measuring, evaluating, and comparing the strength of authentication systems.” The draft “attempts to provide a starting point for the overall SOFA framework by identifying the ways in which biometric authenticator strength can be measured and evaluated. It focuses on three core concepts: False Match Rate, Presentation Attack Detection Error Rate, and Effort.” (NIST, 2016)

Besides the accuracy of a biometric authentication system, another important factor of safety is the protection of templates. There are several methods within cryptography to do so (Sutcu, n.d.; Nandakumar & Jain, 2015; Korte & Plaga, 2007), but this falls outside of the scope of this study. It is however important to know that the template that is stored is never an exact copy of the information taken from you. Specific information is extracted and encrypted, meaning that a stolen template does not necessarily mean that the system can be breached.

There is, of course, the question what happens when the user gets either sick or injured, leaving them unable to pass the biometric test (e.g. burning their fingertips or even losing an eye). In the best case, either the biometric will still work on other markers or other biometric methods can still provide enough security. In the worst case new templates have to be created - a process for which the user once again has to identify themselves on site. A final interesting point to consider is the fact that a user cannot simply ‘change’ their biometric ‘password’. On the one hand this means that this password cannot be forgotten, which erases the risk of the user leaving a sticky note somewhere with the password written on it. On the other hand this creates the risk that if a biometric factor is successfully copied, then the user does not have the possibility to alter the biometric factor.

Often the safety of biometrics is lower than that of, for example, a password. This is partly due to the fact that biometrics work with probabilities, therefore having less probative force compared to other forms of authentication. While a password is (supposed to be) secret, and should be changed every other month, both these facts do not hold for biometrics. This however does not mean that biometrics are not safe at all. The achieved level of safety is closely related to the FAR (False Accept Rate). A system is completely safe when there is an absolute 0% chance of an imposter getting access. By increasing the value of the decision threshold, and thus the sensitivity, the FAR decreases, as seen in Figure 2.4.
Figure 2.4: Error Rates (Gibson, 2011). A more sensitive system is prone to more Type 1 Errors (False Rejects), but will have less Type 2 Errors (False Accepts). Sensitivity can be chosen based on different factors, such as the system’s area of application.

In addition to the FAR and the FRR the image shows the Crossover Error Rate (CER), also called Equal Error Rate (EER). Effectively this means that increasing the decision threshold to almost 100, it is possible to achieve a near zero FAR. The distinctiveness can differ between different biometric modalities, and can be calculated as 100% minus the FAR (also called the True Reject Rate, the percentage of false claims that are rejected).

2.3.2 Ease of Use and Implementation

It is important to note that increasing the decision threshold also holds a negative effect; it increases the FRR (False Reject Rate). Now rejecting a user that should be accepted does not increase or decrease security, but it does impact the ease of use. If the FRR becomes too big, it means that every user will have to try authenticating multiple times before the system (rightfully so) recognizes them. This can result in user resenting the system, and refusing to work with it. Biometrics itself have ease of use as an advantage over other means of authentication.

On the other side are the healthcare professionals, who figuratively sit on the other side of the screen. For them, ease of use has a different meaning compared to a patient. It is often seen that medical professionals “typically have a good sense of patients privacy, but they mostly lack familiarity with information security. They are trained to help, and want IT-functionality to do so, [but] they have little patience for security measures [and] they don’t have the professional paranoia of security experts. [A] common attitude: why protect, we’re the good guys!” (Jacobs & Alpár, 2015). Therefore it is important to consider the healthcare professionals opinion considering the implementation of biometric authentication, and how much and what they get to see of it. The third group who have to be considered when looking at the ease of use and implementation is the product team, who will eventually make a demonstrator out of it. Here the ease concerns the requirements and expectations the team has when looking at the implementation.
2.3.3 Functionality

The functionality of an authentication method determines the number of options the user gets access to. This can range from little functionality (the patient has no choice about what biometric factor to show, only minimal information shown to the healthcare professional) to a great deal of functionality (the patient can determine per consult if and what biometric factors he or she wants to show, and the healthcare professional has access to detailed information and options to recheck the patient etc.). Because this study focuses on the tension between ease of use and security, and because during this study the implementation (and thus the choice of functionality) of the biometric authentication has not started, the functionality factor is left out of scope.

2.4 Acceptance

Acceptance comes in many flavours and on many levels. On the subject of social acceptance, Gigya commissioned a study entitled “2015 State of Consumer Privacy & Personalization”. The report is based on a survey of 2000 UK and 2000 US adults aged 18 and older. They found that “41% of US consumers have a high level of comfort logging in to a site or mobile app using a thumbprint biometric or face/eye biometric scan.” (Lee, 2015). While this may not be an accurate representation for Dutch adults, Philips serves a worldwide market, and the initial launch of the service may not take place in the Netherlands. In a 2002 paper from the Global Information Assurance Certification (GIAC) it is stated that “there can never be public acceptance of biometrics until the public feels their information is safe and won’t be misused. [...] Another key to public acceptance is education.” (Wolansky, 2002). Yet there seems to be a gap in the literature when looking at the current state of public/social acceptance regarding biometric authentication. This may very well differ from that of the public in 2002, since the use of biometrics in ‘everyday’ objects (smartphones with fingerprint scanners, PC’s with face and iris recognition) is much more prevalent.

In October and November of 2014, Accenture held an online survey among 24,000 consumers across 24 countries, concluding that “Consumers [are] willing to use biometric authentication methods” (Srivastava, 2015). In the past years, there were multiple opinion surveys conducted on the public perceptions of biometric (International Biometrics Identity Association, 2016). In a study by Ponemon Institute (2013), it is stated that “the majority of respondents believe it is acceptable for a trusted organization such as their [...] health care provider [...] to use the biometrics such as voice or fingerprints to verify their identity”. In another study by CTA (2016)(CTA, 2016), one of the key findings was that “U.S. adults view entities that currently handle (sensitive) personal information securely such as health care organizations [...] more favourably with managing biometric information”. These surveys show some positive results regarding the acceptance of biometric authentication methods. However, for the case at hand (audio-video calls between medical professional and patient) there is no specific information available.

According to Patrick (2004), “factors that are making the systems more acceptable include technical interest, concerns about identity theft, government border-control initiatives, securing critical infrastructures, and the opportunity to reduce memory demands by replacing memorized passwords.” Angela Sasse characterizes biometric security systems as ‘enabling tasks’, which differ from the actual work (‘production tasks’) that users are interested in. “If the enabling task is at all awkward, slow, or unusable, it is natural for users to try to avoid it. For biometrics, perceived convenience can be a bigger driver than any increase in security” (Patrick, 2004).

Another interesting viewpoint when looking at social acceptance is the view of religious
groups, for example some Christian splinter groups, who “believe that all forms of biometric ID constitute what the Christian Bible calls ‘the mark of the beast.’” (Elgan, 2012, John, 2016). These groups are opposed to all forms of biometric authentication, making it difficult to get acceptance from their ranks. At the same time, the size of these splinter groups is not huge, and it is uncertain how many Christians in the Netherlands share their beliefs. Therefore these groups are excluded from the scope of this research.

In this study the focus lies on user acceptance of technology, which is a research field on its own.

2.4.1 Technology Acceptance

The more specific kind of acceptance that is considered within this thesis is the acceptance of technology. One of the first models considering acceptance and human behaviour is called the Theory of Reasoned Action, using as core constructs the ‘Attitude Toward Behaviour’ (“an individual’s positive or negative feelings (evaluative affect) about performing the target behaviour” (Fishbein & Ajzen, 1975)) and the ‘Subjective Norm’ (“the person’s perception that most people who are important to him think he should or should not perform the behaviour in question” (Fishbein & Ajzen, 1975)).

An often used, and more recent, model to determine technology acceptance is the Technology Acceptance Model (TAM) proposed by Davis in 1989. This model uses two factors, ‘Perceived Usefulness’ (“the prospective user’s subjective probability that using a specific application system will enhance his or her job or life performance” (Davis, 1989)) and ‘Perceived Ease of Use’ (“the degree to which the prospective user expects the target system to be free of effort” (Davis, 1989)) to determine ‘User Acceptance’.

The TAM model has seen some revised versions, among which TAM2 (which reuses the core construct of ‘Subjective Norm’) and the Unified Theory of Acceptance and Use of Technology (UTAUT)(Venkatesh, Morris, Davis, & Davis, 2003). This model adds two ‘new’ factors on top of ‘Perceived Ease of Use’ and ‘Perceived Usefulness’:

- ‘Social Influence’: An adaptation of the ‘Subjective Norm’, incorporating ‘Social Factors’ (“what they [the users] think they should do” (Thompson, Higgins, & Howell, 1991)) and ‘Image’ (“the degree to which use of an innovation is perceived to enhance one’s image or status in one’s social system” (Moore & Benbasat, 1991)),
- ‘Facilitating Conditions’: Incorporating ‘Perceived Behavioural Control’ (“people’s perception of the ease or difficulty of performing the behaviour of interest” (Ajzen, 1991)), ‘Facilitating Conditions’ (“objective factors, ‘out there’ in the environment, that several judges or observers can agree make an act easy to do” (Thompson et al., 1991)) and ‘Compatibility’ (“the degree to which an innovation is perceived as being consistent with the existing values, needs, and past experiences of potential adopters” (Moore & Benbasat, 1991)).

2.4.2 End User Acceptance Model

The model, mentioned in the introduction, used to determine the end user acceptance (of patients in a survey and, to some degree, of healthcare professionals in an interview) is the model proposed by Miltgen, Oliveira and Popović. They do so in their article titled ‘Determinants of end user acceptance of biometrics: Integrating the “Big 3” of technology acceptance with privacy context’ (Miltgen et al., 2013). This model was chosen because of its direct application to the field of biometrics. The writers have proposed the framework as seen in Figure 2.5, where factors from three well known technology acceptance models are integrated and combined with additional factors, all in the context of biometrics. The three
models combined are the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT), discussed above, together with the Diffusion of Innovations model (DOI). Within this model, five attributes are described concerning the diffusion of innovations: the ‘Relative Advantage’ the innovation has over existing products, the ‘Complexity’ of the product, the ‘Trialability’, ‘Observability’ and ‘Compatibility’ (Rogers, 2003). Miltgen et al. consider ‘Relative Advantage’ closely connected with ‘Perceived Usefulness’ and ‘Complexity’ closely connected with ‘Perceived Ease of Use’. They do add the new attribute ‘Compatibility’, determining if an innovation is compatible with “the values, past experiences, and needs of potential adopters” (Rogers, 2003).


![Diagram showing factors and their correlations](image-url)

**Figure 2.5:** Factors End User Acceptance Biometrics (Miltgen et al., 2013)

The green arrows represent positive correlations, the two red arrows (with minus signs) represent the two negative correlations.

Adding on top of the mentioned models, the model by Miltgen considers several ‘Prior Factors’, to determine how users consider innovations as a whole, how much they trust technology and how concerned they are about the privacy of their data. In addition, they show the correlations (positive in green, negative in red) they have tested for.

From right to left, it is suggested that the ‘Behavioural Intention to Recommend’ is positively affected by only the ‘Behavioural Intention to Accept’. The ‘Intention to Accept’ correlates several other factors, both antecedent and prior. Both the prior factors ‘Innovativeness’ and ‘Trust in Technology’ show a positive effect on the ‘Intention to Accept’, as do the ‘Compatibility’, ‘Ease of Use’, ‘Usefulness’, ‘Social Influence’ and the ‘Facilitating Conditions’. ‘Intention to Accept’ is negatively affected by the ‘Perceived Risks’. Among the antecedent factors, the ‘Ease of Use’ is positively affected by the ‘Compatibility’, while the ‘Usefulness’ is positively affected by both the ‘Compatibility’ and ‘Ease of Use’. The prior factor ‘Innovativeness’ positively affects ‘Compatibility’, ‘Ease of Use’ and ‘Usefulness’, while ‘Trust
in Technology’ positively affects ‘Ease of Use’ and ‘Usefulness’, but negatively affects ‘Perceived Risks’. The ‘Perceived Risks’ are also positively affected by the ‘Concern for Data Privacy’.

However, these correlations were found in a study using only the biometric of iris scanning and were only tested on respondents of age between 15 and 25 years (Miltgen et al., 2013). To enable a participant to scan his or her iris, an additional device is needed, which makes it part of a specific category of biometrics that cannot instantly be scanned. Participants of age between 15 and 25 are often more familiar with innovations in technology, which may influence the results, and foregoing results from the labour force of age between 25 and 65.
Chapter 3

Research Methods

3.1 Research Strategy

The strategy utilized during this study is a mixed-method strategy. Both quantitative and qualitative tools were used to answer different questions. For the patient user acceptance, the question ‘how many patients find X’ comes to mind, and for these kind of questions Dawson (2009, p.20) suggests a quantitative methodology. However, for user acceptance of healthcare professionals and expert opinions, words as ‘experiences’ and ‘thoughts’ come to mind, which Dawson (2009, p.20) links to a qualitative methodology. In the study, three different research methods were applied. Semi-structured interviews (Dawson, 2009, p.28-29) with experts, structured interviews (Dawson, 2009, p.29) with healthcare professionals and a closed-ended questionnaire with one open question (Dawson, 2009, p.31) for the patients.

The first weeks of the internship, an in-depth literature study of mostly secondary research (Dawson, 2009, p.46) was conducted into, among others, the following topics:

- Biometrics,
- Authentication,
- Biometric authentication,
- Biometric factors,
- Safety of biometrics,
- Distinctiveness of factors,
- User acceptance,
- Acceptance of biometrics,
- Authentication in hospitals.

After some time, the process of the internal ethics committee (ICBE) at Philips was started (see Section 3.4) after which the actual study and primary research (Dawson, 2009, p.46) could begin. To complete the study, both a quantitative method (survey) and a qualitative method (interviews) were used to find answers to different sub-questions.

After the literature study the first outline of the survey was created in EFM (Verint, 2017), a survey-tool used by Philips. The survey contains, except for one, only closed-ended questions (Dawson, 2009, p.90). This decreased the risk of participants (unintentionally) leaving personal or sensitive information in these open questions. This lowered the ‘privacy impact assessment’ that needed to be taken during the ICBE section. The outline incorporated the prior, antecedent and consequent aspects as described by Miltgen et al. (2013). To ensure interest of participants was kept throughout the survey, most aspects were tested with up to three questions. Innovation was tested using the research by Craig and Ginter (1975). Questions about other aspects, such as ease of use, simply asks how easy (or hard) the participant views the use of certain methods, also in comparison to the most known methods of username-password and SMS code requirements. The first version of the survey included situation sketches about the consent protocol, in which participants would have to choose which situation they preferred. In later versions this part was deleted, due to its size and the lack of relevance for the main topic.
The main language of the survey was English, but the EFM tool allowed for easy, yet manual, translation in Dutch. The survey was sent to supervisor Raphaëls Vmals for review, and after alterations was sent to the Philips team for a pilot (Dawson, 2009, p.98). After incorporating the suggestions, it was sent to Janne for final review, as well as spell check. After the final changes, it was distributed to the participants (see Section 3.2).

The interviews with healthcare professionals were of a structured nature. The questions were partly taken from the survey. However, a part about audio-video consultations was added to provide the professionals with some context and background. This was done to ensure that the healthcare professionals were aware where the biometric authentication would be used, and why. In addition, because the role of healthcare professionals in the authentication process differs from that of patients, questions were added regarding the way the authentication should look (what should (not) be visible?, what information should the professional get?, and what should happen if an authentication fails?).

The interviews with experts in security, biometrics and information systems of hospitals had an semi-structured nature (Dawson, 2009, p.28-29), and the questions differed for each area of expertise. The reason semi-structured interviews were chosen is the need to have several topics discussed/several questions asked, but in no particular order, and the interviewee was free to discuss his or her personal opinions on what they deemed important to the subject. Questions for the security expert focussed on the security of biometrics as an authenticator, questions for both biometric experts focussed on requirements to set up a safe system, and the specific biometric factors that are usable. The questions for the information manager of a hospital focussed more on the implementation, and possible hurdles within a hospital that need to be taken before implementation is possible.

3.2 Data Collection

The data collection for the five sub-questions and the main question, posed in Section 1.5, took place as follows:

Sub-question 1: Expert Opinion
The answer to the first sub-question was produced by analysing the results of four interviews with experts, with the areas of expertise of security, information-management, academic biometrics and commercial biometrics:

<table>
<thead>
<tr>
<th>Code</th>
<th>Date</th>
<th>Time</th>
<th>Expertise</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXPInterviewee01</td>
<td>22-05</td>
<td>16:56</td>
<td>Security</td>
</tr>
<tr>
<td>EXPInterviewee02</td>
<td>31-05</td>
<td>17:21</td>
<td>Biometrics (commercial)</td>
</tr>
<tr>
<td>EXPInterviewee03</td>
<td>13-06</td>
<td>14:58</td>
<td>Biometrics (academic)</td>
</tr>
<tr>
<td>EXPInterviewee04</td>
<td>07-07</td>
<td>10:59</td>
<td>Information Manager</td>
</tr>
</tbody>
</table>

Note: Interviews were anonymous.

The areas of expertise were chosen by theoretical sampling (Dawson, 2009, p.51) to be able to determine the security and ease of implementation requirements, in addition to more practical information about biometric authentication itself. The interviewees were recruited by direct contact, searching in the literature for Dutch biometrics experts, while contact the security expert was recommended by a colleague within Philips. The information manager of the hospital was contacted by referral, by another information manager in
Sub-question 2: Usable Biometrics in Philips Context
To answer the second sub-question, the information from several conversations with team members was compiled, together with the reasoning behind requirements and expectations. In addition, the knowledge was used of the current state of the service, and the view for the future.

Sub-question 3: Healthcare Professionals User Acceptance
The third sub-question was answered by analysing interviews with seven healthcare professionals to determine their viewpoints of and whether or not they would accept the use of biometrics:

<table>
<thead>
<tr>
<th>Code</th>
<th>Date</th>
<th>Time</th>
<th>Expertise</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPIInterviewee01</td>
<td>26-06</td>
<td>17:30</td>
<td>Laboratory Clinical Medicine</td>
</tr>
<tr>
<td>MPIInterviewee02</td>
<td>27-06</td>
<td>12:24</td>
<td>Youth Healthcare</td>
</tr>
<tr>
<td>MPIInterviewee03</td>
<td>10-07</td>
<td>11:45</td>
<td>Institution for Protected Living</td>
</tr>
<tr>
<td>MPIInterviewee04</td>
<td>19-07</td>
<td>12:49</td>
<td>Communicable Disease Control and Forensic Medicine</td>
</tr>
<tr>
<td>MPIInterviewee05</td>
<td>20-07</td>
<td>11:02</td>
<td>Neurology</td>
</tr>
<tr>
<td>MPIInterviewee06</td>
<td>21-07</td>
<td>15:42</td>
<td>Guided Living</td>
</tr>
<tr>
<td>MPIInterviewee07</td>
<td>28-07</td>
<td>12:35</td>
<td>Psychological Help</td>
</tr>
</tbody>
</table>

Note: Interviews were anonymous.

These healthcare professionals were contacted by first making contact with different hospitals, and utilizing the snowball sampling (Dawson, 2009, p.50), asking each professional if they know a colleague who would want to be interviewed. They have different backgrounds, areas of expertise and they differ in the amount of contact with patients. The criteria used to determine if a healthcare professional is appropriate, is if the healthcare professional does have medical consults with patients. In specific, follow-up consultations (or similar consultations) that can potentially be replaced by either phone consults or, in the future, audio-video consults. There were multiple reasons to seek out a heterogeneous group of healthcare professionals. First of all, this could provide information about specific medical specialities where implementation of an audio-video consulting service is most wanted. Secondly, speaking with healthcare professionals both in hospitals and in ‘the neighbourhood’ could show differences in number of patients treated in a time interval, which potentially generates more (or less) need for (biometric) authentication. The interview schedule can be found in Appendix A.2. In total, seven of these interviews were conducted.

Sub-question 4: Patient User Acceptance
Surveys sent out to determine patient user acceptance towards the usage of biometric authentication, where participants were selected with convenience sampling (Dawson, 2009, p.51). The channels used to distribute the survey were outlined in the ICBE study overview. The survey was sent to the Philips SocialCast network (Philips employees), the Philips Intern Community (network of all interns working at Philips), the Radboud University ‘Studenten Prikbord’ and the Community as a Service group, a community of active (inter-)national
participants. The convenience here was the fact that access to all these databases was not restricted, while in general access to patient databases is restricted. Participants below the age of eighteen were excluded, as are participants who never in their lives had a consultation with a healthcare professional. The reason for this exclusion is that the aim is to find the opinions of patient users who are familiar with current consultation systems. An outline of the survey can be found in Appendix A.1. As an absolute bare minimum sample size to have some statistical relevance, 56 participants are needed. For the calculation, see Appendix B. In total, 126 participants completed the survey.

Sub-question 5: Factors for Patient User Acceptance
To answer this last sub-question, the same data used for sub-question four was used. However, where in sub-question four the precise outcomes were important, in sub-question five the focus lies more on correlations and dependencies between the scores on different aspects. Same as before, the participants were selected by convenience sampling.

Main Question
Finally, to answer the main question and to advice Philips on the potential implementation of biometric authentication in their service, the information gained in the first four sub-questions was combined.

3.3 Data Analysis

Sub-question 1: Expert Opinion
The interviews with experts in the fields of biometrics, security and information management are semi-structured. Here, a highly qualitative type of analysis (Dawson, 2009, p.119) was used, in particular thematic analysis (Dawson, 2009, p.119-120). The recurring themes found can be seen in Appendix C.1, and include biometrics, fail-safes/alternatives and requirements. As the reader can see, these topics are broad and change heavily per expert. However, the topics are used to distil the main opinions and viewpoints of these experts from the interviews, placing these in the context of their background, interest and expertise, and comparing these to literature and to each other.

Sub-question 2: Usable Biometrics in Philips Context
To analyse the data for the second question, the answers of the team members were compiled, after which the list of requirements and expectations was created.

Sub-question 3: Healthcare Professionals User Acceptance
The interviews with healthcare professionals have a structured form. This has made it easier to code the interviews with more specific topics, therefore using almost qualitative and highly qualitative (Dawson, 2009, p.119) types of analysis. First thematic analysis was used to generate recurring themes in the interviews, such as demands, hurdles and fail-safes. Content analysis (Dawson, 2009, p.122) was applied by coding the themes found. There was no prior existing coding scheme, but the scheme formed inductively (for a complete coding scheme, see Appendix C.2). For the coding of the interviews, the program QDA Miner Lite was used. This program allowed for easy coding and basic analysis by coding frequency. Later, the full program QDA Minder was used to run further analyses on the coding.

Sub-question 4: Patient User Acceptance
For the first analysis of the survey results, descriptive statistics are used. These give a clear
image of the answers of participants, and provide an answer to this sub-question. For each relevant survey question, the participants are divided into three groups: Top, Neutral and Bottom. Depending on the number of possible answer per question (Yes-Maybe-No, Very Easy-Easy-Neutral-Hard-Very Hard) the Top group contains the participants giving ‘positive’ answers (Yes, (Very) Easy), the Neutral group the Maybe and Neutral answers and the Bottom group the participants giving ‘negative’ answers (No, (Very) Hard).

**Sub-question 5: Factors for Patient User Acceptance**

The first tests used are the correlation tests of Pearson (1895, 240-242), Spearman (1987, 441-471) and Kendall (1938, 81-89). These correlation tests take the answer columns of different aspects, and calculates whether or not a significant correlation exists. The following nineteen correlations, also seen in Figure 2.5 with factors and implicated dependencies, were checked:

<table>
<thead>
<tr>
<th>Code</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>C01</td>
<td>Innovativeness</td>
<td>Compatibility</td>
</tr>
<tr>
<td>C02</td>
<td>Innovativeness</td>
<td>Ease of Use</td>
</tr>
<tr>
<td>C03</td>
<td>Innovativeness</td>
<td>Usefulness</td>
</tr>
<tr>
<td>C04</td>
<td>Innovativeness</td>
<td>Behavioural Intention to Accept</td>
</tr>
<tr>
<td>C05</td>
<td>Trust in Technology</td>
<td>Ease of Use</td>
</tr>
<tr>
<td>C06</td>
<td>Trust in Technology</td>
<td>Usefulness</td>
</tr>
<tr>
<td>X01</td>
<td>Trust in Technology</td>
<td>Perceived Risks</td>
</tr>
<tr>
<td>C07</td>
<td>Trust in Technology</td>
<td>Behavioural Intention to Accept</td>
</tr>
<tr>
<td>C08</td>
<td>Concern for Data Privacy</td>
<td>Perceived Risks</td>
</tr>
<tr>
<td>C09</td>
<td>Compatibility</td>
<td>Ease of Use</td>
</tr>
<tr>
<td>C10</td>
<td>Compatibility</td>
<td>Usefulness</td>
</tr>
<tr>
<td>C11</td>
<td>Compatibility</td>
<td>Behavioural Intention to Accept</td>
</tr>
<tr>
<td>C12</td>
<td>Ease of Use</td>
<td>Usefulness</td>
</tr>
<tr>
<td>C13</td>
<td>Ease of Use</td>
<td>Behavioural Intention to Accept</td>
</tr>
<tr>
<td>C14</td>
<td>Usefulness</td>
<td>Behavioural Intention to Accept</td>
</tr>
<tr>
<td>C15</td>
<td>Social Influence</td>
<td>Behavioural Intention to Accept</td>
</tr>
<tr>
<td>C16</td>
<td>Facilitating Conditions</td>
<td>Behavioural Intention to Accept</td>
</tr>
<tr>
<td>X02</td>
<td>Perceived Risks</td>
<td>Behavioural Intention to Accept</td>
</tr>
<tr>
<td>C17</td>
<td>Behavioural Intention to Accept</td>
<td>Behavioural Intention to Recommend</td>
</tr>
</tbody>
</table>

Note: Coding of the different correlations described by Miltgen et al. (2013). ‘C’ codes are expected positive correlations, ‘X’ codes expected negative correlations.

After the three correlation tests, the Goodman and Kruskal Gamma test (1954, 1959, 1963, 1972) was used to find the strength of relationships for each correlation.

### 3.4 Research Ethics

Before being able to conduct the interviews and send out the surveys, this study had to be approved by the internal ethics board of Philips (called ICBE, Internal Committee Biomedical Experiments). The submission includes a study overview, privacy notices, information letters and a privacy impact assessment.

Requiring to complete an ICBE submission forced me to take a close look at several aspects of the research. On the topic of privacy, it has been decided that for the interviews, audio
recordings will be made but will not be heard by anyone but me. Anonymised transcripts can be shared with Raphaël, but will not end up in the final report. Quotes in the final report will always be anonymised, and greatest care will be taken to make it impossible to connect possible quotes to a particular interviewee. The survey on the other hand does not save any personal information. The questions only concern opinions, and answers to inclusion/exclusion criteria will not be saved. In addition, before the study can be completed, two courses were completed. The first one is an online course named "Philips Privacy Rules (BCR)", focusing on the definition of personal information and in what situations the processing of personal information is allowed. The second course, named "Introduction to Ethics, ICBE Processes and Regulations for Research", is a four hour in-house course at Philips. Here, especially the ethics and regulatory aspects are of interest.

Getting the study accepted by Philips ICBE means that the study passes all requirements that Philips sets on the quality of research. At Philips there is, at this time, no student/intern ‘shortcut’ through the submission, resulting in a study submission of the same level as other human studies conducted at Philips.

Completing the ICBE courses and submission showed me the importance of conducting research in an ethical way. It also gave me the opportunity to create extensive information files, that enabled me to make sure all participants, to both interviews and the survey, were fully informed of their rights. During the survey, no personal information was gathered, and all personal information gathered during interviews was anonymised. Because of this, in combination with the absence of side-effects from the study (neither negative nor positive), minimized the impact on the participants.
Chapter 4

Results and Analysis

In the following chapter, the results and analyses of these results will be presented. This will be
done in three sections, beginning with the section describing the requirements for the biometric
authentication, for the audio-video consultation service as the Philips team is creating. The
second sections discusses the results of the interviews, both with the healthcare professionals
and with the experts in security, biometrics and information management. The last section will
focus on the survey results.

4.1 Results from Team Conversations

Through conversations with the team within Philips Research, a clear picture could be created
that shows some requirements which a biometric system would have to fulfil to be usable in the
audio-video consultation context.

4.1.1 Requirements

First of all, the service that is being developed, uses audio-video communication. Because the
team does not want to force patients to buy additional hardware (except for the mandatory
microphone and webcam), it would be useful to have biometric factors that can be authenticated
using these audio-video services. Secondly, one of the unique selling points of the service is the
one click access. This makes access to the service as easy as possible. To continue this trend
when looking at biometric authentication, there is a need for factors that are easy and fast to
use, requiring as little time from the patient as possible. Thirdly, the service should be usable
cross-device and cross-platform. This means that the biometric factor should be usable on PC,
tablet and smartphone, and on Windows, Android, Linux and iOS. This immediately limits the
available biometric factors that can be used. In addition, it excludes most of the biometrics that
score ‘high’ on performance in Table 2.1, namely DNA, iris scans and retinal scans. Fingerprints
are not excluded straight away, because many modern smartphones have fingerprint sensors
included, which can be used for further authentication. In addition, face thermograms (which
also scores high in Table 2.1) cannot be used either, because of the hardware restrictions.

4.1.2 Potential Biometric Modalities

The previous requirements result in a list of six biometric factors that could be feasible for use
in an audio-video service:

- Face recognition. This system can operate in many ways, but the most simple way to
  think about it is a set of points on your face (also called knots) and the distances between
these points. Now the template is an encrypted version of these distances which the life 
sample can be compared to. Difficulties are, according to EXPInterviewee03:

> With face recognition there are a few important factors. Indeed the pose, 
so how straight do you look into the camera? Modern face recognition 
systems often have ways to adjust if you do not look completely straight. 
A second factor is, how uniform is the light? Now a little omniform is 
not a big problem, but too much difference and nothing can be done to 
fix it. When a part of the face is covered with hair or big sunglasses, is 
a factor, and so are emotions. Those are the problems.

However, because patients (participants to the system) are mostly cooperative and want 
to be authenticated/recognised, many of these problems boil down to asking the patient to 
look and sit straight, and turn the camera until the light is of sufficient quality. However, 
demanding a patient to keep the same size beard or same hairstyle will most likely not 
get the cooperation of patients, implicating that even in this scenario total complete 
cooperation does not exist.

- Speaker recognition. Interestingly, as the reader can also see in Figure 2.1, the voice is 
both a biological and a behavioural biometric. Some behavioural aspects are accent and 
the speed at which a person speaks. Biological aspects can be the size of your lungs, or 
the shape of your vocal tract. While the sound of your voice may change, during a cold 
for example, these biological aspects do not. Therefore speaker recognition may also work 
during sickness. Within speaker recognition, both text dependent and text independent 
systems are operational. While the first shows somewhat better results, the latter is 
preferable, not requiring the patient to memorize a passphrase. However, again because 
of the cooperation of the patient, remembering a passphrase may not be considered a 
large decrease in usability.

- Ear geometry. While, as stated by EXPInterviewee03,

> Geometry of the ear is used mainly in forensic applications. There is 
nowhere close the amount of research done in that field, compared to the 
distinctiveness of fingerprints.

an interesting fact about ears is that while it grows in size, the actual shape does not 
change significantly after birth (Ross & Abaza, 2011). This means that, while at this time 
the research about using ear biometrics is lacking, they may hold a future proof way of 
identifying and authenticating people during a lifetime.

- Hand geometry. Other than ear geometry, more research has been done into hand 
geometry, and it is already deployed in several contexts. Usually this requires a device 
to ‘aim’ the hand (see Figure 4.1), companies are set to create a system usable by 
showing your hand to your phone camera (de Santos Sierra & Ávila, 2011). Future 
implementation might see a patient waving to a camera, and their authentication attempt 
is strengthened with the size and shape of their hands.
Figure 4.1: Hand Aiming for Hand Geometry (360 Biometrics, 2011).

- Recognition of blood vessels in the sclera (white part of the eye). While retinal scans require special eye scanners, and iris scans require infrared pictures, the blood vessels in the sclera can be recognized with a regular (phone) camera. The company EYEVERIFY (EYEVERIFY, 2017) even offers a free phone app, allowing users to try this method themselves, as long as they have a smartphone with at least a 2MP camera.

- Fingerprint recognition. This specific biometric requires an additional device to scan the fingerprints. While it is not preferred to require patients to buy new devices, fingerprint recognition is still included because the amount of mobile phones that come with fingerprint scanners increases. This means that if the patients owns such a smartphone, they can authenticate themselves by using the phones scanner. EXPInterviewee03 sees a bright future for biometrics on smartphones, stating:

  "In the short term, you will see biometrics being closely linked to your smartphone. [...] In identity and access the focus will be on ‘what can I do with my smartphone?’; for example you could use the fingerprint sensor to authenticate yourself to other applications. Your smartphone is going to be a token, which negotiates with systems and proves your identity. This is the ‘bring your own ID’ concept."

4.2 Results from Interviews

After analysing the interviews, some overlap was found between topics discussed with healthcare professionals and experts. These topics include ‘demands/requirements’, ‘hurdles’, ‘fail safes’ and ‘alternatives’.

First the broader scope of the interviews with healthcare professionals will be discussed, which includes questions about the audio video service itself, after which the overlap with the interviews with experts will be discussed, ending with the final analysis of the experts interviews.

4.2.1 Prior Factors Healthcare Professionals

First the results are shown of the ‘prior factors’ statements, as described in the methodology, ranking the healthcare professionals on ‘most’ to ‘least’ accepting of new technology based solely
on prior factors. These factors are ‘innovativeness’, ‘trust in technology’ and ‘concern for data safety’ (Miltgen et al., 2013). The ten statements used are the following:

(a) Innovativeness  
   i. New is generally better  
   ii. I like to take risks  
   iii. I am glad if something works ‘well enough’  
   iv. I am interested in innovations within healthcare  

(b) Trust in Technology  
   i. I trust the safety of technology  
   ii. I trust the privacy protection in technology  
   iii. I trust the ‘honesty/transparency’ of technological companies  

(c) Concern for Data Safety  
   i. I am concerned about the safety of online, non-medical data  
   ii. I am concerned about the safety of online, medical data  
   iii. I am concerned about the safety of my own online medical data  

The healthcare professionals were asked to give themselves a number between zero and ten for each question. The total score was calculated by summing up the scores of the questions with an expected positive correlation to acceptance ((a)i,ii,iv,(b)i-iii), then adding (10 - score) for the questions with an expected negative correlation to acceptance ((a)iii,(c)i-iii). The results are shown below:

Table 4.1: Acceptance Scoring Prior Factors MPIInterviewees

<table>
<thead>
<tr>
<th>Topic Question</th>
<th>(a) Innovativeness</th>
<th>(b) Trust in Techn.</th>
<th>(c) Concern Data</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(i)</td>
<td>(ii)</td>
<td>(iii)</td>
<td>(iv)</td>
</tr>
<tr>
<td>MPInterviewee01</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>MPInterviewee02</td>
<td>6</td>
<td>7</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>MPInterviewee03</td>
<td>7</td>
<td>7</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>MPInterviewee04</td>
<td>6</td>
<td>10</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>MPInterviewee05</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>MPInterviewee06</td>
<td>6</td>
<td>7</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>MPInterviewee07</td>
<td>7</td>
<td>8</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

Note: Scores as answered by healthcare professional interviewees, including average score. Highest scores per column are coloured green, lowest red. The average scores are quite close, leading to the conclusion that these prior factors do not provide a clear distinction between healthcare professionals who accept new technology, and those who do not.

This gives an average score of 5.75, where MPInterviewee02, -03, 04 and -05 score well above average. For the questions in category (a) and (b), answers are relatively close, with the exception of MPInterviewee04, who stated during the interview that he always tried to score such questions in absolutes (three scores of ten and a score of zero). The biggest differences are seen in question (c)iii, which can be due to the interpretation of the question. Some interviewees considered their own online medical data as ‘not interesting’, and are therefore not concerned about its safety. However, other interviewees were as concerned about their own data as they were about general online medical data, as they had no idea how that data was stored or protected. These two interpretations lead to a greater diversity in answer scores. The same pattern can be seen in the answer scores of question (c)i, where a similar reason can be given. Interviewees who consider online, non-medical data as less interesting will score low on concern.
Other interviewees score higher, as they are concerned for all data that is stored online, no matter the sensitivity.

However, when comparing the total scores, the margins are small. As stated, the average is 5.75, the lowest score being 4.6 and the highest 6.7. This means that, when only taking the prior factors into account, the seven healthcare professionals seem to be neither very accepting of new technology, nor highly against it. It is noteworthy that all interviewees are (very) interested in innovations within healthcare, though most seem to be reasonably glad when things work ‘well enough’. This can be due to the fact that technological changes often go hand in hand with bugs, which need to be fixed. A healthcare professional may rather see a system that works (well enough) and leave it at that, than needing to go through a tedious circle of implementing, updating and fixing. In addition, the fact that these healthcare professionals were willing to be interviewed about this topic speaks for their interest in new technological applications. This indicates that the total score may not be an optimal way to indicate acceptance of technology based on prior factors.

4.2.2 Expert Opinion and Healthcare Professional Acceptance

Audio-video consultations

As noted, the interviews with healthcare professionals did not only contain questions about their opinions on biometric authentication, but to sketch the context in which this authentication would be used, questions were included regarding audio-video consultations. All seven interviewees were interested in the technology of audio video consultations. Three of the interviewees named the ability to see the patient as a benefit over the use of telephone consults and the use of the mobile messaging application ‘WhatsApp’. Interestingly enough, the use of WhatsApp as a means of talking with patients is not allowed, as one of the interviewees admitted, but it is still used because of how easy it is to remain in contact. Later we will circle back to the fact that healthcare professionals sometimes trust their own judgement over that of their managers. Two of the interviewees named not being physically present at the patient as a negative. The reason for this was, according to interviewee03:

“The small view you get from the camera may show a tidy house, but the rest may as well be a big mess. Another thing you cannot see is if the client takes care of their personal hygiene. Their face may seem clean, but you cannot smell whether they have taken a shower in the past days. If during these video calls the client wants to hide something, you will not see it.”

Interviewee02 added: “There will always be people saying ‘the baby is very ill, but you will not be able to feel, see or smell that’. Those are new risks. You will never have access to all information.” It seems that audio video consultations are, for all intents and purposes, the ‘next best thing’ to actually seeing a patient face to face during follow-up appointments. However, even during audio video consultations vital information can be missed, stressing the need for (periodical) face to face consultations, as well as when relaying important (bad) news. Interviewee07 also states that having audio video consultations greatly decreases travel time of healthcare professionals making house calls.

The most important reason why audio video consultations are not often used, even though all interviewees are interested in the technology, is because of technological hurdles. Interviewee02 states that he never used teleconsults simply because ‘the technology is not
present at this time’. An important requirement, as stated by MPIInterviewee05, is that

“It is important that teleconsults are seen as ’consultations’, and we get compensated the same way. Because for us, the amount of work when comparing teleconsults and regular consults does not change. While we may not have to walk to the waiting room, we will still have to make notes and process the information. Therefore, if teleconsults are not being compensated, nobody will use them.”

Biometric authentication
Because of the reasonably large difference in knowledge about biometrics and security, it is interesting to compare the opinions about biometric authentication, in general or during audio video consultations, between those of healthcare professionals and experts. While the healthcare professionals, and with them many people unfamiliar with the intricacies of biometrics, can either be hesitant to use this technology, or as EXPInterviewee03 stated, can be interested because the usage of such systems in crime television series, it is based solely on their own feelings, without facts. In addition, it is also interesting to see the difference in opinion about biometrics between a security expert and biometric experts.

Starting with this last comparison, security expert EXPInterviewee01 states:

“In my lectures, and as a general standard, identifying means ‘saying who you are’, while authenticating means ‘proving who you are’. […] Authentication is important for the proof.”

In this definition, the act of authenticating lies with the person. However, when talking about biometric authentication, the act of authenticating lies with the biometric system, and the act is also called ‘verification’, as stated “A synonym for verification is authentication” (Poh et al., 2012). Within biometrics, EXPInterviewee03 defines identification as ‘having a large database with biometric information, when someone places their fingerprint on a sensor it picks the entry from that database that is most likely to be you.’ With biometric authentication, or verification, the fingerprint is only compared to one template. In short:

“So identifying is more about ‘who am I seeing here?’
Verifying means ‘am I the one I say I am?’”

While these definitions of identification and authentication seem similar, the biggest problem lies in the so called ‘probative force’. What are the odds that an imposter enters a system, when the authentication happens with a password, or biometrics? EXPInterviewee03 states that security experts rather want error margins of the order $10^{-6}$, which are really small. Error margins in biometrics are higher. Therefore EXPInterviewee01 considers biometrics as a ‘dead end’, and completely unsuitable for the act of authentication, basically stating that biometric authentication is a scam, or fraud. Biometric experts EXPInterviewee02 and EXPInterviewee03 disagree, stating that it all depends on the usage, and cost/benefit analyses of the companies using this kind of authentication. The literature seems to favour the opinion of the biometric experts. The simple fact that so many sources use the term ‘biometric authentication’ (Jain et al., 2002; Wayman, Jain, Maltoni, & Maio, 2005; Tuyls et al., 2005; Mitra, Savvides, & Brockwell, 2006; Jain, Ross, & Pankanti, 2006; Wang, Rane, Draper, & Ishwar, 2012) shows that the concept of authentication can (and is) used in the context of biometrics. There is, however, a source that states why biometrics cannot (and should not) be
used as authentication (Riley, 2006). Here, it is stated that any authenticator should be secret (only known to the person who it belongs to) and does not necessarily need to be unique. A password fits, as long as you keep it a secret. However, biometrics are generally not a secret, as you leave your fingerprints everywhere you go, and in general everyone can see your face. The counterargument is that this definition of an authenticator seems to mean that only a secret password can be used for authentication. A house key or keycard can be stolen and are no real secrets, and neither is your passport. In conclusion, in security a password/-phrase seems to be the only acceptable means of really proving ones identity. Therefore, when biometrics are used, it may not be a bad idea to couple it with a ‘secret code’. While copying the biometric factors of a specific person is quite a costly and personal attack, having another layer (even something simple like date of birth) can again increase security. And indeed, the benefits of biometric authentication may not lay in its small error margin, but in the ease of use and user friendliness.

When specifically asking EXPInterviewee03 how the implementation of a biometric system should take place, the expert answered that the best course of action would be to buy the software, not develop it. "Developing it yourself would leave you at a huge disadvantage. Some suppliers sell incredible software". About biometrics-as-a-service the expert was clear:

"I think it would be safer to buy the software. Just for a demonstrator it might work, [...] but you do give them information about the users, which is something that does not fit with the context of medical records. The software however does not have to be expensive. It could be rather affordable."

Searching for prices of biometric software shows that there are many providers providing free services up to a number of comparisons a month. In this case being bound by such a maximum is unwanted, therefore the paid versions of the software are preferred. However, many biometric software suppliers do not show their prices online. VeriLook by NEUROtechnology (2017) does show pricing, charging 859 euro for one extended Software Development Kit (SDK) license. EyeFace by Eyedea Recognition (2017) can be acquired for 599 euro for one expert SDK license. Fulcrum Biometrics (2017) shows prices for several SDK’s, ranging from anywhere between 400 USD for a standard VeriFinger SDK to 3000 USD for the MegaMatcher SDK. The issue with these prices are, that it is unknown at this point how many licenses are needed.

Looking at the opinion of EXPInterviewee04, an information manager in a hospital, and the opinions of the healthcare professionals, we see that they do not doubt the existence of biometric authentication. They often seem to favour biometrics over a system with password protection or SMS code, for two main reasons. Firstly, biometrics are easier in use, not having to either remember a password or requesting that SMS code. Secondly, they tend to think that biometrics are safer compared to a password, because stealing a password is quite simple. In fact, a strong password, of sufficient length and containing enough symbol variety, can be a good ‘key’. However, remembering such a password can be difficult, resulting in people writing it down. Biometrics on the other hand seem very easy in use, and because our biometric features seem so distinct, the healthcare professionals see it as a good alternative. This is a point where the cost benefit analysis is important. Your fingerprint, in comparison to a password, is no secret. You leave it everywhere you go, and it is rather easy to take a copy of it. After that, creating a fake fingerprint that passes state of the art biometric authentication systems is doable, but costly. So the question becomes, is the medical information of a single person so valuable, that an imposter would go through the trouble of getting a copy of the biometric factor, creating a fake factor that passes the authentication, and uses this to gain
access to an audio video consultation? This question can only be answered when weighing the costs, and risk, of fraud against the benefits of the biometric system. When using audio-video consultations, using biometric authentication will be better than using no authentication (which seems to be the status quo). While using passwords or SMS codes may provide a smaller error margin, they seem to create a hurdle which some patients do not want to (or cannot) pass. This results in telehealth consults not being available to all patients.

It also became clear that not all healthcare professionals are instantly positive about using biometric authentication within the audio video consultations. While some requirements they set can be seen further below, MPIInterviewee02 suggested that “you could just use the same common practice, basic trust, that we now do for phone calls. I also mail to parents without having authentication, and I’ve never had any legal problems with that”. At this time, MPIInterviewee02 does not stand alone in using only trust as an authenticator. MPIInterviewee05 explains:

“Now see, at this time, when I call someone for a phone consultation, then I do not ask for any form of authentication. Sometimes people pick up saying their full name, sometimes just their first name or they just pick up with ‘hello?’. At that point I do ask ‘is this Mr. Jansen?’, to which they respond with ‘yes’. After that, I just assume I am talking to the correct patient.”

The pattern that shows here is that healthcare professionals do not want to increase the difficulty of having contact, by using elaborate authentication schemes. They often only use trust, or the simplest ‘password’ (e.g. date of birth) as authenticator. Here it really depends on the situation how much damage a misidentification can do. For a simple consult the damage may be low, but for an invasive surgery the implications may be much more severe.

Requirements and demands
To increase the quality of a biometric authentication system, both the experts and healthcare professionals have posed some requirements or demands. EXPInterviewee02 generated a list, stating:

“A couple of known requirements are the following:
1. A maximal False Reject Rate (FRR) with a given False Accept Rate (FAR),
2. A maximal Failure to Enrol Rate,
3. The level in which quality control of the biometrics system is possible,
4. The level of supervision during registration and authentication,
5. The quality and performance of the chosen modalities, algorithms and sensors.”

To which EXPInterviewee03 adds the ‘presentation attack detection’. The first demand regards a static FAR, which can be seen as the decision threshold. EXPInterviewee03 explains this has its uses in radar technology, where you want a definitive (small) chance of false attacking a friendly airplane. Given this static FAR, you look to minimize your FRR. Another method to choose your FAR and FRR, as EXPInterviewee03 draws on a whiteboard in his office, is to create a DET-curve (Detection Error Trade-off). Minimizing Total Costs, given by

\[ TC = (C_{FM} \times FMR \times P_{FM}) + (C_{FNM} \times FNMR \times P_{FNM}), \]

gives rise to a threshold value. Here the costs of a false match \( C_{FM} \), the costs of a false non match \( C_{FNM} \) and prior chances of false (non) match \( P_{FM} \) and \( P_{FNM} \) are known, as are the dependencies between FAR and FRR. Now indeed minimizing TC by choosing the right FAR
and FRR gives a threshold. While the first method may not lead to the lowest total costs, it
does have a FAR chosen by the company. The second method may have a much higher FAR, but
lower costs. However, both methods boil down to choosing a decision threshold, and choosing
a method depends heavily on the company in question. In the case of authentication during
audio video consultations, I would suggest choosing a maximal FAR, then seeing if the total
costs can be minimized while keeping the FAR under the maximum. If so, choose that as the
decision threshold, if not, choose the maximal FAR as the decision threshold.

The second demand, as EXPInterviewee03 explained, is mostly important if the enrolment is
completed online. The reason for this is the fact that if the online enrolment is too difficult,
and the failure to enrol rate is too high, then people would not use the system. However, in the
case of enrolment in the hospital, the professional overseeing the enrolment can immediately
see if something is going wrong, and help where needed. So it is recommended to have the
enrolment supervised, which also fits with requirement four. While the authentication itself
does not happen under the eye of a biometrics expert, it does happen in front of the healthcare
professional. This supervision can at least make sure that ‘easy’ forms of fraud (simple
masks, band recorder for voice) cannot be used, as the healthcare professional will spot them.
Requirement three, the level of quality control, deals with how well the system can be checked. If
the system is transparent enough, catching flaws will become easier, making necessary updates
less difficult to spot. The final requirement considers the quality of the software, hardware
and biometrics and speaks for itself. The demand added by EXPInterviewee03, regarding
presentation attack detection, is explained as:

“[...] spoof detection, or presentation attack detection, is important. That
includes liveliness detection, to see if that finger belongs to a living person or
if it has been cut off. You do not even want to consider what may happen with
iris. It is all part of presentation attacks, you see it in the name, you present
a biometric and the attack is focused on that.”

Indeed, being able to spot basic imposters, and spot biometrics that ‘do not live’ (fake finger,
paper mask) can decrease the FAR, by giving a very low score to fake comparisons.

This list of practical requirements or demands is very alike the theoretical list as described in
Section 2.2. Some practical points look like copies of the theory, while other are combinations
of more than one theoretical requirement. First of all, the first practical requirement asks for ‘a
maximal FRR with a given FAR’. Now both FRR and FAR depend on how unique the biometric
factor is, how permanent it is over time and with the performance of the system. Hence this
ties in with the theoretical requirements of ‘Uniqueness’, ‘Permanence’ and ‘Performance’. The
second practical requirement, ‘a maximal Failure to Enrol Rate’, goes hand in hand with the
percentage of participants who ‘posses’ the biometric factor, and with how difficult (or easy) it
is to ‘collect’ the factor. Therefore this ties in with the ‘Universality’ and the ‘Collectability’
requirements. The practical requirement of ‘a certain level of quality control’ does not
automatically tie in with any of the seven theoretical requirements. This is due to the fact that
this practical demand considers the biometric system (software, hardware) as a whole, while the
theoretical requirements focus only on the biometric factors. The same can be said regarding the
practical requirement of ‘the level of supervision during registration and authentication’, which
focuses on the processes of registration and authentication. These processes are important in
practice, but less so in theory based only on biometric factors. ‘The quality and performance
of the chosen modalities, algorithms and sensors’ does tie in with the theoretical requirements,
namely the ‘Performance’. The final practical requirement, the ‘presentation attack detection’,

45
goes together with the theoretical requirement of 'Hard to Circumvent', because detecting presentation attacks (including liveliness detection) makes a system much harder to circumvent.

The healthcare professionals have their own ‘list of demands and requirements’. The most frequent answers were safety and choice of whether or not to use biometric login up to patient. To convince healthcare professionals to use the system, they want to know that it is safe and cannot be compromised (or is, at least, not easy to compromise), and even if it is safe, the use should still be optional for the patient. Another demand is simplicity, where MPInterviewee05 stated that “if it does not make things easier, then no one will use it”. This simplicity also counts towards the amount of information the healthcare professionals sees when an authentication attempt is in progress, or is completed, and towards the time an authentication attempt takes. The healthcare professionals agree that the time they get for medical consultations is already short enough, so this form of authentication should not make this time even shorter. Sadly, this does mean that, while many biometric authentication devices are built to authenticate a user fast, if a better method arises that takes longer, it will not be used.

Fail-safes
As for fail-safes, there are different viewpoints between all interviewees. In short, there are three main directions. The first is the usage of a second method of authentication. This could either be a password, like date of birth or mother’s maiden name, or even an SMS code verification. Personally I tend to like this option, because the biometric authentication will still authenticate the patient faster than using a password, and even if it does not work the patient can gain access to the consultation. The second group thinks the healthcare professional should have final say, and have the ability to overrule the decision of the biometric authentication. While many healthcare professionals agree with this option, this sort of beats the purpose of biometric authentication. If the service says ‘yes’, the consultation can take place, and if the service says ‘no’, the healthcare professional can still have the consultation take place. Then why have biometric authentication in the first place? The final option is to stop the consultation, and shut down the access to the patient file. However, this could lead to a bigger problem, because the consultation cannot take place. This could certainly create negative experiences, for both patients and medical professionals, who would no longer want to use the system.

4.3 Results from Survey

From the surveys, there are two parts of relevant information that will be discussed. Starting with the descriptive results of the acceptance of biometric authentication in the given setting and ending with correlation tests between given factors in the model.

4.3.1 Patient User Acceptance

First the results of the patient user acceptance will be discussed. The most interesting questions for patient user acceptance are the ones concerning the antecedent factors (13 through 19) and consequent factors (26 through 29) of the survey (full survey can be found in Appendix A.1).

The first question (question 13) reads: *I feel like authentication through the following methods is compatible with my needs.* The results (blue means ‘yes’, yellow means ‘maybe’ and red means ‘no’) and proportions can be seen in Figure 4.2:
This question means to represent the factor ‘compatibility’, as seen in Figure 2.5. It is seen in these results that most respondents find authentication based on fingerprints the most compatible with their needs. This can be explained by the fact that fingerprint sensors become more seen on mobile devices. In addition, 84% of the respondents answered ‘yes’ to the question I am familiar with, and (would want to) own, a smartphone with fingerprint sensor. This shows that the number of people who would be able to authenticate themselves with the fingerprint sensor on their smartphone keeps increasing.

The questions 17, 18 and 19 follow a similar answering pattern, essentially having three ‘groups’. The first being face recognition and speaker recognition, the second eye blood vessel recognition, hand geometry and ear geometry and the third containing only fingerprint recognition. Question 17 focusses on general usefulness, while questions 18 and 19 compare the usefulness of biometrics against that of username/password and against requesting an SMS code, respectively. The results can be seen in Table 4.2 below:

Table 4.2: Answer Percentages Question 17, 18 and 19

<table>
<thead>
<tr>
<th>Question</th>
<th>17</th>
<th>18</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td>Yes</td>
<td>Maybe</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>53.77</td>
<td>31.75</td>
<td>14.29</td>
</tr>
<tr>
<td></td>
<td>45.24</td>
<td>37.30</td>
<td>17.46</td>
</tr>
<tr>
<td></td>
<td>49.21</td>
<td>32.54</td>
<td>18.25</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>50.79</td>
<td>34.92</td>
<td>14.29</td>
</tr>
<tr>
<td></td>
<td>40.48</td>
<td>38.10</td>
<td>21.42</td>
</tr>
<tr>
<td></td>
<td>48.41</td>
<td>30.16</td>
<td>21.43</td>
</tr>
<tr>
<td>Sclera Blood Vessels</td>
<td>39.68</td>
<td>34.92</td>
<td>25.40</td>
</tr>
<tr>
<td></td>
<td>34.13</td>
<td>34.92</td>
<td>30.95</td>
</tr>
<tr>
<td></td>
<td>38.83</td>
<td>29.37</td>
<td>31.75</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>35.71</td>
<td>38.89</td>
<td>25.40</td>
</tr>
<tr>
<td></td>
<td>26.98</td>
<td>41.27</td>
<td>31.75</td>
</tr>
<tr>
<td></td>
<td>33.33</td>
<td>32.54</td>
<td>34.13</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>30.95</td>
<td>35.71</td>
<td>33.33</td>
</tr>
<tr>
<td></td>
<td>23.02</td>
<td>38.89</td>
<td>30.95</td>
</tr>
<tr>
<td></td>
<td>30.75</td>
<td>31.75</td>
<td>37.30</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>74.53</td>
<td>20.75</td>
<td>4.72</td>
</tr>
<tr>
<td></td>
<td>67.92</td>
<td>27.36</td>
<td>4.72</td>
</tr>
<tr>
<td></td>
<td>66.95</td>
<td>26.42</td>
<td>6.50</td>
</tr>
</tbody>
</table>

Note: Colouring per question, high (green) to low (red) percentages.

Once again, the reason for this distribution might be found in how much biometric methods are used (either in real life, like fingerprint sensors in smartphones, or in media). The usage of face and speaker recognition in series and films can explain why people feel more comfortable with these methods, and see them more useful. Other methods, especially hand and ear geometry, are less trusted, which might be due to the fact that they are far less known. The difference between the scores of questions 17 and those of questions 18 and 19 are the more moderate scores on ‘yes’ on the latter (an average of 47.61% at Q.17 versus 39.63% at Q.18 and 44.63% at Q.19), and the higher scores on ‘no’ (an average of 19.57% at Q.17 versus 24.07% at Q.18 and 24.91% at Q.19). This can be due to the fact that, even though respondents see biometric methods as useful, when comparing to two other methods (username/password and SMS code)
they are not necessarily more useful. There is also a slight difference between question 18 and 19, where in question 19 the ‘yes’ scores are somewhat higher compared to question 18. This can be explained by the difference between the methods compared. If username/passwords are seen as more useful than an SMS code, then that can lead to the shift in scores.

More interesting results follow from the questions 14, 15 and 16, which do not follow the two-three-one grouping. First consider question 14, these biometrics are easier in use compared to using a login name and a password. The proportions can be seen in Figure 4.3:

<table>
<thead>
<tr>
<th>Topic</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Top</th>
<th>Neutral</th>
<th>Bottom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>68.95%</td>
<td>61.65%</td>
<td>51.69%</td>
<td>40.44%</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td></td>
<td></td>
<td></td>
<td>51.69%</td>
<td>40.44%</td>
<td>31.2%</td>
<td>22.26%</td>
<td>13.79%</td>
</tr>
<tr>
<td>Eye Blood Vessel Recognition</td>
<td></td>
<td></td>
<td>78.29%</td>
<td>68.93%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hand Geometry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>78.29%</td>
<td>68.93%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ear Geometry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>78.29%</td>
<td>68.93%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>78.29%</td>
<td>68.93%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4.3:** Answer Percentages Question 14: These biometrics are easier in use compared to a login name and a password.

Here the answer that stands out is the one for eye blood vessel recognition. The reason why this is scored more favourable in this question, can be that in the information given with the survey, the scanning of the blood vessels in the sclera is described as an easy process, doable with a smartphone camera. Because of this, the biometric is scored closer to face recognition and higher than speaker recognition, which requires the participant to actual speak to a device. While it is true that a smartphone camera can see the blood vessels in the sclera, it may not have been clear enough in the survey that one would have to hold the phone at a ten centimetre distance from the face. This might have influences the answers in this question.

Question 15, stating these biometrics are easier in use compared to requesting and inputting an SMS code, follows the same pattern as question 14, presumably for the same reason. Ratios are in Figure 4.4:

<table>
<thead>
<tr>
<th>Topic</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Top</th>
<th>Neutral</th>
<th>Bottom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>68.95%</td>
<td>61.65%</td>
<td>51.69%</td>
<td>40.44%</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>78.29%</td>
<td>68.93%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eye Blood Vessel Recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>78.29%</td>
<td>68.93%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hand Geometry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>78.29%</td>
<td>68.93%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ear Geometry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>78.29%</td>
<td>68.93%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>78.29%</td>
<td>68.93%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4.4:** Answer Percentages Question 15: These biometrics are easier in use compared to requesting and inputting an SMS code.

Again, there is a grouping of three-two-one instead of two-three-one, which might indeed be due to the explanation of the scanning of blood vessels in the sclera.
Question 16 shows something completely different. It states *I think the use of the following methods will be*, and could be answered with very/a little easy, neutral or a little/very hard. Results are in Figure 4.5:

![Figure 4.5: Answer Percentages Question 16: I think the use of the following methods will be](image)

Strangely enough, when comparing eye blood vessel recognition to using passwords or SMS codes, it scores rather high, while asking participants how difficult they think it is to use, they score it much lower. Hand geometry however can be grouped with face recognition and speaker recognition as relatively easy methods, sclera vessel recognition with ear geometry as relatively hard, while fingerprint recognition ‘takes the cake’, with only a total of 7.54% finding it not easy to use. This is probably due to the fact that many people have already tried using a fingerprint sensor, either on their smartphone, laptop, or some forensic application. This leads to the assumption that participants who have already used a certain method will score it higher. By implementing a biometric authentication, and allowing participants to familiarize themselves with it, may swiftly increase the acceptance.

Question 26 (*I would accept the use of the following methods to get access to data that is personal, but not sensitive*) scores pretty similar to questions 13, 17, 18 and 19. Question 27 (*I would accept the use of the following methods to get access to data that is sensitive*) however scores more similar to questions 14 and 15. The results are shown in Table 4.3 below:

![Table 4.3: Answer Percentages Question 26 and 27](image)

When comparing these percentages of acceptance with the indicators from Table 2.1 (Jain et al., 2002), where acceptability is defined as *‘to what extent people are willing to accept the biometric system’* (Jain et al., 2002, page 4), the following results are gained and displayed in Table 4.4:
Table 4.4: Acceptability (Jain et al., 2002) and Acceptance (Q.26 and Q.27).

<table>
<thead>
<tr>
<th>Biometric</th>
<th>Acceptability</th>
<th>Acceptance Q.26 Only ‘Yes’</th>
<th>Incl. ‘Maybe’</th>
<th>Acceptance Q.27 Only ‘Yes’</th>
<th>Incl. ‘Maybe’</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td>High</td>
<td>62.70%</td>
<td>82.29%</td>
<td>57.14%</td>
<td>78.26%</td>
</tr>
<tr>
<td>Voice Print</td>
<td>High</td>
<td>53.97%</td>
<td>78.16%</td>
<td>48.41%</td>
<td>71.76%</td>
</tr>
<tr>
<td>Sclera Vessels</td>
<td>Low*</td>
<td>49.21%</td>
<td>69.67%</td>
<td>50.79%</td>
<td>71.10%</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>43.65%</td>
<td>65.47%</td>
<td>41.27%</td>
<td>61.18%</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>High</td>
<td>40.48%</td>
<td>60.72%</td>
<td>37.30%</td>
<td>55.29%</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Medium</td>
<td>73.58%</td>
<td>92.85%</td>
<td>70.76%</td>
<td>92.60%</td>
</tr>
</tbody>
</table>

Note: Under Q.26 and Q.27 first only the ‘yes’ percentage, second the ‘yes’ and (to ratio) part of ‘maybe’ percentage. (* = there is no such biometric described by Jain et al. (2002). However, both iris scans and retina scans are present, and both score low in Table 2.1.)

In the book of Jain et al. (2002) there is no indication of the percentage value of low/medium/high answers. Therefore, three different colourings of the percentages have been created to enable comparison. The first colouring used red (low) for values below 33%, yellow (medium) for values between 33% and 66% and green (high) for values above 66%. In this colouring (seen in Table C.1 in Appendix C) there are eight matches. The second colouring used red below 55%, yellow between 55% and 75% and green above 75%. This colouring (seen in Table C.2 in Appendix C) had nine matches. The third colouring, shown in Table 4.4 above, used the same proportion as in the book of Jain et al. (2002), where out of the fourteen biometrics three scored low, five scored medium and six scored high. Out of six, this means one low score, two medium scores and three high scores. In Table 4.4, there are eleven matches. Face- and speaker recognition often score high, as they do in Table 2.1. In addition, hand geometry scores medium, as in Jain et al. (2002). Sclera blood vessel recognition (not present in Table 2.1) scores higher than expected. However, since blood vessels in the sclera can be detected without eye-/iris scanner, the ‘low’ score in acceptability may as well be a ‘medium’ score, making the percentages as expected. The interesting cases are ear geometry and fingerprints. Fingerprints obtain the highest percentage scores, while having only a medium acceptability in Table 2.1. This can be due to the fact that Table 2.1 was created in the year 2002, when fingerprint sensors on smartphones (or even smartphones as a whole) where non-existent. Nowadays, the abundance of smartphones with fingerprint sensors has increased the acceptance, which explains the higher percentages.

The reverse is true with ear geometry. While a high acceptability is expected, the percentages are consistently the lowest of the six. While the method is non-invasive, participants are unfamiliar with the technology, and do not trust the results. This leads to ear geometry scoring lower than expected. However, Table 4.4 may give a distorted image of ear geometry, as in Table C.11 all ear geometry scores are classified as ‘medium’, while in C.12 only two out of the four ear geometry scores are ‘low’ (the other two being ‘medium’). While this still is lower than the expected ‘high’ score, it does show that even though ear geometry is the lowest scoring biometric of the six in question, it still does not have an abysmally low score (under 33% or even lower).
Question 28 states “I would only accept the usage of biometric authentication if...” This was an open question and was answered by 63 participants. These answers were divided into eight categories:

- Always,
- Never,
- Spoof and misuse detection,
- Security and (independent) testing results,
- Ease of use,
- Trusted supplier,
- Specific methods,
- If no other option available.

See Appendix A.3 for all answers. Here follow short summaries of each of the eight categories:

**Always** (seven responses)
Respondents say they would use all authentication methods mentioned, and consider biometric authentication better than what is used now.

**Never** (four responses)
These respondents would never consider using biometric authentication, for example because they do not trust the technology, or do not like the idea of being identified by eyes or hands.

**Spoof and misuse detection** (fourteen responses)
Respondents would consider using biometric authentication, but only if they are assured that pretending to be somebody else is rather difficult. In addition, these respondents want to be sure their biometric information is only used in the healthcare context, and misuse or use by third parties (government, police, telephone companies etc.) is detected and prevented.

**Security and (independent) testing results** (twenty-one responses)
Respondents who fall in this category want to be sure the authentication methods are thoroughly tested, and would like to see research done by independent (scientific) parties. Before they would consider using a biometric authentication system, they would like to see proof of its security, accuracy, reliability and safety.

**Ease of use** (five responses)
Respondents with answers falling in this category want to be sure the process of logging in becomes easier with biometrics. It should be faster than current methods, less prone to errors compared to typing in a highly complex password, and safer than current methods.

**Trusted Supplier** (two responses)
These two participants find it important that a trusted source or trusted company is in charge of the program.

**Specific methods** (three responses)
These respondents either only want to use fingerprints, because they have prior experience with such products, or are willing to try most except for the shape of the ear.

**If no other option available** (seven responses)
The respondents in this category would, in the beginning, not make use of biometric authentication. But if they are forced to, if it was required or strictly necessary, then they would consider using the service. But while it is not strictly mandatory, they would choose to opt out.
When comparing these ‘demands’ with those set by the experts and healthcare professionals, the overlap becomes apparent. First of all, the categories ‘always’, ‘never’ and ‘if no other option available’ are less interesting, because they do not offer any real demands. The ‘spoof and misuse detection’ combines well with the presentation attack detection, with liveliness detection, as described by EXPInterviewee03. Security and testing results sounds like requirement five from EXPInterviewee02, stating “the quality and performance of the chosen modalities, algorithms and sensors.” Ease of use compares well to the simplicity as noted by the healthcare professionals. Interesting new additions are the ‘trusted supplier’ and ‘specific methods’. The latter may be seen as trivial (of course people would not want to have an invasive DNA test before taking part in an online consult), but it is not that easy. It differs strongly per person what someone finds comfortable and will use. An interesting example is speaker recognition. While it sounds simple, it does require the participant to actually speak to a device, with no second person on the other end of the line. As EXPInterviewee04 says, “For face recognition, you do not have to do anything, while for speaker recognition you would have to speak to your device. For some people this is another barrier.” The other addition, ‘trusted supplier’, shows that more and more people start to distrust (big) data giants. They would only consider using a biometric authentication service if they trust the company that stores the templates and makes the comparison. Participants seem not to trust the government with that information, and would like to see an independent company having this information. In this case, it may be favourable if the hospital is the storage place of templates. It would also require rules and regulations about the usage, storage and exchange of this personal information.

The final questions, question 29, asks whether the respondents would recommend using a specific biometric method to friends and/or family. It is answered as follows:

<table>
<thead>
<tr>
<th>Topic</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Top</th>
<th>Neutral</th>
<th>Bottom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td>46.0%</td>
<td>34.53%</td>
<td>19.84%</td>
<td>68</td>
<td>46.03%</td>
<td>43</td>
<td>34.15%</td>
<td>25</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>42.06%</td>
<td>34.13%</td>
<td>23.91%</td>
<td>63</td>
<td>42.00%</td>
<td>43</td>
<td>34.15%</td>
<td>20</td>
</tr>
<tr>
<td>Eye Blood Vessel Recognition</td>
<td>35.54%</td>
<td>32.54%</td>
<td>30.96%</td>
<td>46</td>
<td>36.54%</td>
<td>41</td>
<td>32.54%</td>
<td>39</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>39.37%</td>
<td>38.55%</td>
<td>34.76%</td>
<td>37</td>
<td>29.37%</td>
<td>49</td>
<td>38.89%</td>
<td>40</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>36.05%</td>
<td>38.08%</td>
<td>34.43%</td>
<td>33</td>
<td>26.19%</td>
<td>60</td>
<td>39.68%</td>
<td>65</td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td>66.04%</td>
<td>22.44%</td>
<td>70</td>
<td>66.04%</td>
<td>24</td>
<td>22.64%</td>
<td>12</td>
<td>11.32%</td>
</tr>
</tbody>
</table>

Figure 4.6: Answer Percentages Question 29: I would recommend the use of the following methods to my friends and family.

These results show that, while the percentage of acceptance is rather high, the number of participants that would actually recommend others to use biometric authentication is somewhat lower. It could be hypothesised that this is due to the fact that a participant would only recommend something he or she really understands. However, the same grouping of biometric methods can be seen as in question 14. Eye blood vessel recognition is slightly closer to speaker recognition than it is to hand geometry, creating the three-two-one pattern.

When comparing the results with the results seen in the study from Ponemon Institute (2013, page 21), where it can be calculated that on average 71% of the respondents think that a trusted organization can use biometrics to authenticate consumers (as long as the biometric data is not accessible to the organisation), the results gained seem on the low side. Table 4.5 shows the
averages of positive (‘yes’) answers for each dichotomous question (13, 14, 15, 17, 18, 19, 26, 27 and 29):

Table 4.5: Answer Averages Dichotomous Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Avg. ‘Yes’</th>
<th>Question</th>
<th>Avg. ‘Yes’</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>52.63%</td>
<td>19</td>
<td>44.63%</td>
</tr>
<tr>
<td>14</td>
<td>52.10%</td>
<td>26</td>
<td>53.93%</td>
</tr>
<tr>
<td>15</td>
<td>47.30%</td>
<td>27</td>
<td>50.95%</td>
</tr>
<tr>
<td>17</td>
<td>47.61%</td>
<td>29</td>
<td>41.03%</td>
</tr>
<tr>
<td>18</td>
<td>39.63%</td>
<td>Total Avg.</td>
<td>47.76%</td>
</tr>
</tbody>
</table>

Note: Separate ‘maybe’ category, lowering the ‘yes’ scores.

As stated, these scores are at least 17.07% lower (question 26) and on average 23.24% lower than the result of Ponemon Institute. However, this can be due to the fact that the ‘maybe’ answer category is an odd one, generally never used in dichotomous questions, and perhaps a poor design choice. If we distribute the participants who answer with ‘maybe’ between the ‘yes’ and ‘no’ answers (to ratio: ‘new yes’ % = (‘old yes’ %)/(100% - ‘maybe’ %)), the results shown in Table 4.6 are gained:

Table 4.6: Answer Averages Dichotomous Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Avg. ‘Yes’</th>
<th>Question</th>
<th>Avg. ‘Yes’</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>74.43%</td>
<td>19</td>
<td>63.85%</td>
</tr>
<tr>
<td>14</td>
<td>72.85%</td>
<td>26</td>
<td>74.86%</td>
</tr>
<tr>
<td>15</td>
<td>67.75%</td>
<td>27</td>
<td>71.70%</td>
</tr>
<tr>
<td>17</td>
<td>69.79%</td>
<td>29</td>
<td>60.78%</td>
</tr>
<tr>
<td>18</td>
<td>61.18%</td>
<td>Total Avg.</td>
<td>68.58%</td>
</tr>
</tbody>
</table>

Note: Distributed ‘maybe’ category over ‘yes’ category, showing increased percentages.

Both tables are coloured with the same conditional colouring, showing that even the lowest average in Table 4.5 gives a higher result than the highest average in Table 4.4. In addition, the total average lies much closer to the results of Ponemon Institute, with only an average distance of 2.42%, and for some questions the average even exceeds 71% (13, 14, 26 and 27).

From these results it can be seen that, on average, participants are open to the idea of biometric authentication during audio-video consultations. While Table 4.5 shows a very positive picture (because the ‘maybe’ category is divided to ratio in ‘yes’ and ‘no’ answers), even Table 4.4 shows that the total average of positive answers comes close to 50% at 47.76%. While this may seem as insufficient, the total average of negative answers over these same questions equals 20.95%. This means that on average, for every twenty participants who have negative views regarding biometric authentication, there are 47 patients who have positive views about such systems, and another 33 patients who may be persuaded to see the benefits of such systems. In addition, if the focus shifts to the top three methods (speaker-/face- and fingerprint recognition), the results in Table 4.7 are seen:
Again, it is obvious the scores when distributing the ‘maybe’ category are better, but note that now the average percentage of positive answers when including the ‘maybe’ category never drops below 50%. On top of that, the total average of negative answers decreases to 6.84%, never going over 10% for any question.

### 4.3.2 Correlations

The second use of the survey is to test the correlations as they are described by Miltgen et al. (2013). When comparing the user acceptance survey in Appendix A.1 with the model by Miltgen in Figure 2.5, the questions can be linked to their respective factor, and the factors are numbered:

1. ‘Innovativeness’: questions one through seven,
2. ‘Trust in Technology’: questions eight and nine,
3. ‘Concern for Data Privacy’: questions ten and eleven,
4. ‘Compatibility’: question thirteen,
5. ‘Ease of Use’: questions fourteen through sixteen,
6. ‘Usefulness’: questions seventeen through nineteen,
7. ‘Social Influence’: questions twenty and twenty-one,
8. ‘Facilitating Conditions’: questions twenty-two through twenty-four,
9. ‘Perceived Risks’: question twenty-five,
10. ‘Behavioural Intention to Accept’: questions twenty-six through twenty-eight,
11. ‘Behavioural Intention to Recommend’: question twenty-nine.

The correlations that will be checked first are those described in Figure 2.5, and again below in Table 4.8:
Table 4.8: Correlations Between Factors

<table>
<thead>
<tr>
<th>To \ From</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>C01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>C02</td>
<td>C05</td>
<td>C09</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>C03</td>
<td>C06</td>
<td>C10</td>
<td>C12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>X01</td>
<td>C08</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>C04</td>
<td>C07</td>
<td>C11</td>
<td>C13</td>
<td>C14</td>
<td>C15</td>
<td>C16</td>
<td>X02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C17</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Tested Correlations as Shown in Figure 2.5 and Table 3.1.

where the C marks represent correlations, and X marks represent the inverse correlations. As described in the methodology, three correlation tests are performed (Pearson, Spearman $\rho$ and Kendall $\tau$) after which the strength of the relationships are determined with the Goodman and Kruskal $\gamma$. The complete results can be found in Appendix D.3.

In the Pearson Correlation test, the following correlations have no significance and small correlation: C01, C02, C06, C08. Correlations C09 through C17 and X02 all have significance at $\alpha=0.01$, and a large correlation. The interesting cases are shown below. C03, C04 and X01 have no correlation at all, which are the only ones not even gaining a small correlation. C05, while having only a small correlation, does have significance for $\alpha=0.5$. This can be explained by the fact that the ‘trust in technology’ factor contains questions about how well people trust their own skills in technology, and if the answers there grow, then it would be logical that those participants find technology easier to use. C07 has a small correlation which is only significant at $\alpha=0.1$. As seen below in Table 4.9, this is the only test in which this happens, so there is no good explanation for this occurrence.

Table 4.9: Pearson Correlation

<table>
<thead>
<tr>
<th>Corr</th>
<th>R-score</th>
<th>p-value</th>
<th>Significant at 0.1?</th>
<th>0.5?</th>
<th>0.01?</th>
<th>Correlation?</th>
</tr>
</thead>
<tbody>
<tr>
<td>C03</td>
<td>0.0874</td>
<td>0.33048</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>None</td>
</tr>
<tr>
<td>C04</td>
<td>0.0158</td>
<td>0.86061</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>None</td>
</tr>
<tr>
<td>C05</td>
<td>0.1873</td>
<td>0.03572</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td>Small</td>
</tr>
<tr>
<td>X01</td>
<td>0.0126</td>
<td>0.89391</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>None</td>
</tr>
<tr>
<td>C07</td>
<td>0.1483</td>
<td>0.09747</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>Small</td>
</tr>
</tbody>
</table>

Note: $R_{X,Y} = \frac{cov(X,Y)}{\sigma_X \sigma_Y}$, only deviant values shown.

For both the Spearman $\rho$ (Table 4.10) and the Kendall $\tau$ (Table 4.11) Correlation tests, the only interesting correlation is C05. C01 through C04, C06 through C08 and X01 all have no significance, while C09 through C17 and X02 have significance at $\alpha=0.01$. C05 again has significance for $\alpha=0.05$ (but not for $\alpha=0.01$), which can be explained by the logical correlation between the themes ‘how good are you with technology’ and ‘how easy do you find it to use technology’.

Table 4.10: Spearman $\rho$ Rank Correlation

<table>
<thead>
<tr>
<th>Corr</th>
<th>$\rho$-score</th>
<th>p-value</th>
<th>Significant at 0.1?</th>
<th>0.05?</th>
<th>0.01?</th>
</tr>
</thead>
<tbody>
<tr>
<td>C05</td>
<td>0.195105</td>
<td>0.02857</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Note: $r_s = \frac{cov(r_{X,Y})}{\sigma_{r_X} \sigma_{r_Y}}$, only deviant values shown.
Table 4.11: Kendall τ Rank Correlation

<table>
<thead>
<tr>
<th>Corr</th>
<th>τ-score</th>
<th>p-value</th>
<th>Significant at 0.1?</th>
<th>0.05?</th>
<th>0.01?</th>
</tr>
</thead>
<tbody>
<tr>
<td>C05</td>
<td>0.13980</td>
<td>0.026010</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Note: $\tau = \frac{(#\text{ Concordant Pairs}) - (#\text{ Discordant Pairs})}{n(n-1)/2}$, only deviant values shown.

The Goodman and Kruskal Gamma test shows some more interesting results. While C01 through C08 and X01 are only weak relationships (with C04 not being a relationship at all), the relationships in the group C09 through C17 and X02 are not all strong. Even more so, most of them are moderate, with only four (C11, C14, C16 and C17) being strong relationships.

Table 4.12: Goodman and Kruskal Gamma test

<table>
<thead>
<tr>
<th>Corr</th>
<th>γ-score</th>
<th>Relationship?</th>
</tr>
</thead>
<tbody>
<tr>
<td>C01</td>
<td>0.369644</td>
<td>Weak</td>
</tr>
<tr>
<td>C02</td>
<td>0.377150</td>
<td>Weak</td>
</tr>
<tr>
<td>C03</td>
<td>0.287564</td>
<td>Weak</td>
</tr>
<tr>
<td>C04</td>
<td>0.155823</td>
<td>None</td>
</tr>
<tr>
<td>C05</td>
<td>0.304976</td>
<td>Weak</td>
</tr>
<tr>
<td>C06</td>
<td>0.324746</td>
<td>Weak</td>
</tr>
<tr>
<td>X01</td>
<td>0.283114</td>
<td>Weak</td>
</tr>
<tr>
<td>C07</td>
<td>0.382727</td>
<td>Weak</td>
</tr>
<tr>
<td>C08</td>
<td>0.456538</td>
<td>Weak</td>
</tr>
<tr>
<td>C09</td>
<td>0.658189</td>
<td>Moderate</td>
</tr>
<tr>
<td>C10</td>
<td>0.691087</td>
<td>Moderate</td>
</tr>
<tr>
<td>C11</td>
<td>0.823259</td>
<td>Strong</td>
</tr>
<tr>
<td>C12</td>
<td>0.703534</td>
<td>Moderate</td>
</tr>
<tr>
<td>C13</td>
<td>0.577567</td>
<td>Moderate</td>
</tr>
<tr>
<td>C14</td>
<td>0.798351</td>
<td>Moderate</td>
</tr>
<tr>
<td>C15</td>
<td>0.709222</td>
<td>Moderate</td>
</tr>
<tr>
<td>C16</td>
<td>0.809524</td>
<td>Strong</td>
</tr>
<tr>
<td>X02</td>
<td>-0.67323</td>
<td>Moderate</td>
</tr>
<tr>
<td>C17</td>
<td>0.773459</td>
<td>Strong</td>
</tr>
</tbody>
</table>

Note: $G = \frac{(\#\text{ Concordant Pairs}) - (\#\text{ Discordant Pairs})}{\#\text{ Concordant Pairs} + (\#\text{ Discordant Pairs})}$.

Figure 4.8 below shows the information found in the statistical in the same picture as Figure 4.7. The ‘none/weak correlation’ distribution of the Pearson correlation is used, with the ‘moderate/strong correlation’ from the Goodman and Kruskal Gamma test, to differentiate between very low/low scores and high/very high scores. Thicker lines represent stronger correlations, a green line represents a positive correlation, while the red line (with minus sign) represents a negative correlation. Dotted lines represent correlations presented in the paper by Miltgen et al. (2013), but were not found in these results.
Here it shows that the factors used in the established models (UTAUT, TAM and DOI) have significant correlations with acceptance, with moderate to strong relationships. The prior factors, however, have either only weak relationships with no significance (with the only exception being C05) or no relationships at all. During this study, no evidence was found to support the addition of prior factors as Miltgen et al. suggested.

The reason that less correlations with the prior factors can be found, can be due to the way Miltgen et al. (2013) tested their hypothesis. They used a short scenario in which they provided very specific context (the person-bound, non-remote service of queueing for a driving simulator) for the use of one specific biometric method (iris scans). In addition, the participants of this survey were all between fifteen and twenty-five years of age, and of them, 91% had access to internet for at least three years, and 94% browsed the internet at least once per day (80% even multiple times per day). This seems to be a group of people for whom chances are they are proficient in using current technology and adapting to new technology. This differs from the participants of this survey, as the target group included all ages above eighteen, including respondents who are less proficient with technology.

In addition, the effect of prior factors on antecedent (and consequent) factors may be difficult to pin down. For example, prior knowledge of biometric methods can lead to person A having reservations and person B accepting the technology. If the knowledge is obtained through news outlets reporting that biometric sensors are ‘hacked’ or ‘fooled’, person A would understandably be negative. However, if information is gained through entertainment media (e.g. crime scene TV shows), biometric access management might seem to work near flawless and fast. Person B might then have a positive attitude regarding biometric authentication. While both person A and B claim to have prior knowledge of biometrics, it affects their acceptance very differently.
Chapter 5

Conclusions and Recommendations

In this chapter, the results shown in Chapter 4 will be used to answer the research questions and to advice the team within Philips Research on how to proceed.

5.1 Sub-questions

In this section, we will come back to the different research questions that guided this research and attempt to formulate answers to them based on the analyses in the previous chapters. We will first focus on the five sub-questions.

5.1.1 Sub-Question 1: Expert Opinion

Of the four experts, the professor in biometrics and the commercial biometrics expert are both in favour of using biometrics as a means of authentication. They have set some demands, or requirements, to test for the quality of such a system. The professor in security states that biometrics cannot, and should not, be used to authenticate people. While minimizing error margins does increase the safety of a system, and is something security experts strive for, the benefit of a user friendly system must not be underestimated. A very secure system that does not get used because it is not user friendly, nor easy to use, it not by definition a ‘solid’ system. The information manager from a hospital agrees, stating that the usage of ‘more difficult means of authentication’ (an SMS code) has decreased the amount of unique visitors to their online hospital platform by 25%.

I conclude that while security is very important in the current digital age, a certain degree of user friendliness and ease of use is necessary to keep people involved and to keep them from not using any form of authentication at all. In addition, combining multiple kinds of biometrics (creating a multimodal biometric system) will increase safety, and decrease the chance of imposters getting access (Jain, Hong, & Kulkarni, 1998; Ross & Jain, 2004). There are several reasons why multimodal systems are considered more secure. First of all, they decrease the False Reject Rate and the False Accept Rate. If there is a 1% chance of an imposter passing either of two biometric systems, the chance of him passing both in a row is one in ten-thousand, or 0.01%. In addition, when working with multiple different sensors, multiple instances of one biometric (e.g. both eyes, or three fingers) or multiple biometric factors, it becomes more difficult for imposters to gain access to all this information. While gathering one thumbprint might be manageable, requiring two different fingerprints, a voice recording and an high resolution picture of an eye makes things more difficult.
5.1.2 Sub-question 2: Usable Biometrics in Philips Context

Due to the requirements from Philips, and the restrictions of using the biometric authentication during audio-video consultations, some biometrics are disregarded immediately. Some for being invasive, such as DNA tests, some for requiring additional hardware, such as iris and retina scans, and others for the fact they are unusable during teleconsults, such as a signature, odour (smell) or gait (walking/moving pattern). While this does exclude some thoroughly tested methods, the methods that are left can still create a ‘good’ system. Here, ‘good’ indicates a system of biometric factors that are either already being used, or are expected to be usable at the time that technology (both hardware and software) catches up. Of these, both fingerprints and speaker recognition are already implemented in several mobile apps. As an example, they can be used to login to mobile banking apps, and even to transfer money. While some seem to trust this method, and others doubt its safety, comparing it to the five digit passcode used before may reveal an improvement. A five digit passcode allows for 100 000 different codes, and without prior knowledge and five ‘tries’ an imposter would have just 0.005% chance of getting access. However, one look over a shoulder could significantly increase this chance, while more effort is needed to gain access with a false fingerprint or voice recording. Adding face recognition, creates a system such as already described by Jain et al. (1998), where it is stated to it might be able to “overcome the limitations of individual biometrics” and “the experimental results show that our system performs very well”.

While other methods are becoming available, some of which might be usable during teleconsults, the testing results should first show their strength. Some of these methods, hand-/ear geometry and sclera vein recognition, were added to the patient user acceptance survey, to see if lesser known methods would still be accepted. This, however, does not seem to be the case at this moment (as will be further explored in sub-question four), and knowledge about (or familiarity with) a specific biometric method seems to be an indicator for acceptance. As more testing is done regarding lesser known methods, and companies will start using them, these biometrics (as well as soft biometrics) may become new authenticators.

5.1.3 Sub-Question 3: Healthcare Professionals User Acceptance

While all healthcare professionals applaud the use of audio-video consultations, provided that it is seen as a ‘regular’ consultation and paid in the same way, not all interviewees were enthusiastic about using biometric authentication. Some were reluctant because of what they knew about biometrics, other would rather not see an additional form of authentication during audio-video consultations at all. These professionals would rather trust the person on the other side of the line to be who they say, and see implementing (biometric) authentication as a precedent for using this authentication in all current communications with patients. Another healthcare professional saw using biometric authentication during teleconsults as the perfect way to bill his hours. The patient is authenticated, so there is proof that you have spoken with the patient, and there is a call log stating how long the call lasted, making billing per minute a possibility. In conclusion, two important factors to consider when wondering which healthcare professionals would be interested in using such a system, are the number of patients a professional sees (in a certain amount of time), and the amount of times the professional sees that particular patient. For professionals who see lots of patients only once or twice, this kind of authentication could prove to be helpful, while for professionals who see only ten patients very often, their own experiences may be just as usable to authenticate a patient.

When looking at the information that the healthcare professional sees of the authentication, simplicity is key. In conclusion, most professionals would rather only see a pop-up stating ‘authentication successful’, or a color light with at most three colors. One color for ‘success’,
one for ‘failure’ and one for ‘inconclusive’. Or, as one interviewee stated, the authentication could take place in a virtual waiting room, meaning the patient is already authenticated before the consultation starts.

5.1.4  Sub-Question 4: Patient User Acceptance

From the six methods that are usable during audio-video consultations, and were tested in the survey, fingerprint recognition is by far the most accepted by the patients. As stated before, this can be due to the fact that many people have fingerprint sensors on their smartphones, therefore knowing how to work with them (and, through experience, trust them more). However, using fingerprint recognition would require the patients to have a smartphone with fingerprint sensor, and while the penetration of smartphones with fingerprint sensors grows worldwide, to approximately 67% in 2018 (Statista, 2017), this may not reach enough patients. On top of that, Philips would have to create contracts with the suppliers of smartphones with said sensors, to enable the Philips app to use the sensor for authentication.

As seen in the results of the survey, face- and speaker recognition is the second group after fingerprints. These can easily be used during audio-video consultations, and it has been suggested that prices for these kinds of software are affordable. While exact pricing is difficult without more intimate knowledge about future implementation, the prices found are within reason. With no need for additional devices (or device specific requirements, such as the fingerprint sensor), these methods are the most usable biometrics in this context.

The third group, existing out of eye blood vessel recognition, ear- and hand geometry, were the least accepted methods. A reason for this is the current public knowledge about these methods, or the lack thereof.

5.1.5  Sub-Question 5: Factors for Patient User Acceptance

In this research is can be seen that the prior factors, as described by Miltgen et al. (2013), do not achieve similar significant correlations. While this may depend on the questions asked, and the amount of participants, I cannot proof the existence of significant relationships between the prior factors and the antecedent factors.

However, the results did show significant correlations between the antecedent factors and the intention to accept. This shows that the established models (TAM (Davis, 1989), UTAUT (Venkatesh et al., 2003) and DOI (Rogers, 2003)) also work for the technology of biometrics, in the field of healthcare. The strongest relationships were found between ‘compatibility’ and ‘acceptance’, ‘usefulness’ and ‘acceptance’ and between ‘facilitating conditions’ and ‘acceptance’. In addition, a strong relationship was found between ‘acceptance’ and ‘recommendation’, from which can be concluded that a higher acceptance leads to more people willing to recommend the technology to friends and family. In addition, the correlation between ‘social influence’ and ‘recommendation’ is higher than between ‘social influence’ and ‘acceptance’. This shows that participants who are more willing to recommend the technology to others, are also more inclined to listen to others about what technology to use.
5.2 Main Question: Feasibility of Biometric Authentication

What are the biometric modalities that are considered acceptable by users, both healthcare professional and patient, for patient authentication during online audio/video consultations, and what do different experts think about the implementation of such a system?

After answering all sub-questions, the results can be combined in an answer to the main question. First of all, using sub-question two, it is seen that several biometric modalities can be used in online consultations. Requirements for such modalities are, for example, the ability to use them without the need to purchase additional sensors and the non-invasive nature of the biometric modality. Six of these were selected and presented to the patient user in the survey, namely fingerprint-/speaker-/face- and blood eye vessel recognition, hand- and ear geometry.

The top three choice consists of fingerprint recognition, face recognition and speaker recognition, due to the answers of participants and their ease of implementation in audio-video consultations. Considering the opinion gained in the structured interviews of healthcare professionals, of whom some want the authentication to take place before the consultation starts, fingerprint recognition and face recognition would be the best options. This is due to the fact that both fingerprint recognition and face recognition requires little effort from the patient (place your finger on a sensor and look into the camera). However, speaker recognition requires the patient to talk to the device, and when authentication takes place before the consultation starts, this means the patient will have to talk to the device while there is no person ‘on the other side’. This may feel awkward, and is therefore the least favourable method of the three to use in authentication before the consultations starts. Considering the fact that the service should be usable with all devices (some of which may not possess a fingerprint sensor), face recognition seems to be the best fitting single biometric modality.

Experts stated during the interviews that the implementation would best done with bought software, and that using multiple biometrics (either as a combined, multimodal system, or as fail-safes) are preferred. This leads to the conclusion of using the two highest scoring and easiest to implement methods, face recognition and speaker recognition, with the possibility to add fingerprint recognition if implementation with smartphones is possible.

5.3 Additional Conclusions

Healthcare professionals, according to this research, appeared to often not use any form of authentication at all when conducting non-physical consultations (for example through telephone or instant messaging). Therefore, the introduction of a mandatory authentication system will provide more security. This is due to the fact that it will stop more fraudulent access attempts than the healthcare professional only. This decreases the amount of medical information shared with wrong patients, and decreases the amount of ‘pollution’ of medical records. Healthcare professionals and a hospital information manager agreed that increasing the security with often used methods (username/password or SMS code) also increases the threshold for patients to enter the service. At this point, biometrics can shine as form of authentication, as one of its main benefits is the user friendliness.

However, biometric authentication also has its negative sides. Examples are the higher error rates when compared to passwords and the fact that your biometrics are no secret (and therefore can be more easily stolen). Therefore such a system can only work if its safety can be guaranteed, and only then can there be hope for widespread (user) acceptance. As many patients noted...
in the survey, they would only use the system if methods are safe, their biometric templates cannot be accessed by third parties and the error rates are low.

5.4 Recommendations

Based on the results, the following recommendations are left to the Philips team, to help them with their choice whether or not to implement biometric authentication:

- I would recommend the use of biometrics, as this stays true the most to the idea of a single-click login, whilst adding a layer of security not present before. This provides a combination of safety and user friendliness, enhancing the experience of the users.
- If the choice is made to introduce a biometric authentication system:
  - Try to leave the option for patients not to use it. This ensures innovators and the early majority gain access to the new methods, whilst keeping the service without biometrics available for patients who, at first glance, do not want to use biometric authentication. This way, patients can more gradually get used to the idea of biometric logins, and later decide to start making use of the system,
  - Try to employ a secondary method as fail-safe (I recommend a password/-phrase, not overly complex, but not as simple as date of birth). This works in two ways. Firstly, if the system/authentication fails, a password can proof the identity and the consultation can take place. Secondly, a patient who distrusts biometric authentication on its own now has a trump card in the form of a passcode/-phrase/-word.
  - See if authentication can be done before the healthcare professional enters the audio-video consultation. This decreases (or even nullifies) the amount of time a healthcare professional has to spend dealing with the authentication. If it costs them more time, they will not be using it.
  - Consider using the name ‘biometric verification’. Whilst verification and authentication are used for the same action by biometric experts, security experts consider them widely different. Using the term ‘verification’ may make it easier to introduce to the target groups.
- Regarding biometric factors usable:
  - The most accepted is fingerprint recognition. This method can be used before the consultation starts, and the comparison can be made within the patients device (foregoing storage of templates). However, this may require contracts with smartphone manufacturers,
  - Both face recognition and speaker recognition are usable and score high on the acceptance test. Both can be used before the consultation starts, however, participants would rather use face recognition (passive, look at device) than speaker recognition (active, speak at device) when no healthcare professional is present,
  - If possible, combine multiple biometrics, creating a more solid multimodal system. I recommend starting with face- and speaker recognition, as implementation does not rely on additional sensors (usage of the service already requires a camera and microphone). Both these methods are well tested, software is widely available and a list of ‘as-a-service’ providers is added in Appendix E,
  - In the first version, I would advice against using unknown methods, such as sclera blood vessel recognition, as they may be much more difficult to ‘sell’ to potential users, e.g. patients. When such methods gain more popularity, they may be introduced to the system.
• Regarding the decision threshold:
  – I recommend putting the threshold somewhat higher than the EER. While this means more false negatives, and thus less ease of use, this will better protect the sensitive medical information against imposters. However, to get illegal access to the consultation of a patient, the imposter would need to have access to the mail account of the patient, as have copies of the patient’s biometric factors. Having a false accept rate of 1% means that out of one thousand imposters trying to get illegal access to a consultation, each of them having access to the mail account and biometrics of the patient, only one gets to see a healthcare professional.

• Regarding implementation:
  – For demonstrators, biometrics-as-a-service APK’s could be used to easily show the possibilities of biometrics,
  – However, for real implementation, it is not ethical to send a patient’s biometric information to as-a-service providers. In this case, purchasing algorithms is the better option, also providing more freedom when it comes to building the system.
  – Be very careful how to handle the biometric templates. While these templates may be (and should be) encrypted, making it impossible to recreate a picture of a face from its template, each template is still a ‘password’. Therefore, be very certain of the safety of the location where these templates are stored.

5.5 Limitations

Below, some of the limitations of this study are mentioned. The first one is the context of acceptance. Acceptance is a broad principle, and can be considered on many different levels. In this study the focus lies on end-user acceptance. Public acceptance or corporate acceptance are not considered, because of the exploratory nature of the study. This study has not gained enough participants to make significant statements on public acceptance of a larger group of people, and corporate acceptance was left out of scope. Secondly, a substantial part of the participants of the survey do not live in the Netherlands. Because no data on exact countries of residence were asked, no definite amounts are available. However, the Philips team does not aim to make a service strictly for the Netherlands, so the opinions of non-Dutch participants is just as valuable. The addition of the ‘maybe’ answer category in the dichotomous questions in the survey may have, to some degree, altered the results. In hindsight, a ‘I do not know’ category might have been better, allowing to focus solely on the participants who had an opinion.

The addition of too many possible biometric methods to the survey may have impacted the results. As three ‘well known’ and three ‘lesser known’ methods are added, the scores of the latter may pull down the scores of the former.

5.6 Possibilities for Further Research

Because this study was very exploratory of nature, one recommendation that comes to mind is to actually create a test setting, in which several biometric authentication methods can be tested by a target group. This would enable the researcher to give the participants more detailed and specific information about the methods used, and would make sure the participants know what they are talking about when they answer questions about those methods.

Best would it be, in the above case, to create test scenarios for the three most promising methods (face recognition, speaker recognition and fingerprint recognition). This could allow participants to better understand the context of an audio-video consultation where the
biometrics can be used. Additionally, a lower scoring yet promising method (sclera blood vessel recognition) can be provided, to make participants aware of such lesser known methods and its intricacies. Because knowledge of (or familiarity with) biometrics seems to influence acceptance, 'spreading the word' about lesser known methods may increase the user acceptance of such methods.

Furthermore, it can be beneficial to converse with professionals in multiple biometric methods about their practical opinions about (and experiences with) the use of biometrics in a wider context. According to a Dutch professor in biometrics, these professionals are scarce in the Netherlands. Therefore, a more international study can be conducted, speaking with more international biometrics professors or professionals. While there are both positive and negative results to be found in the literature regarding biometrics, the practical implications of such systems find less representation.

In addition, someone more proficient in programming could create a demonstrator, showing the possibilities of biometrics in the healthcare context. This ties in both with the first suggestion, where patients could try the demonstrator and form a better opinion about biometrics, as well as healthcare professionals. They could get a better view of what this authentication would do for them, and whether they are interesting in using such technology.

As for the survey used during this study, it was kept rather short on purpose, to get the highest amount of participants from the different sources. However, if bigger databases of patients would be available for survey distribution, more questions can be added for the different factors (either including or excluding prior factors). This could give even more clear answers about the interdependence of different acceptance factors. Moreover, it might be interesting if a survey is conducted using only prior factors and acceptance (excluding antecedent factors), delving deeper into these prior factors. Then the correlation between these factors and acceptance may either be seen, or may potentially be proven to be absent.

Alternatively, one could take the model of Miltgen et al. (2013), without the prior factors, and search for more influences between antecedent factors. While from Figure 4.7 it can be deduced that all antecedent factors (compatibility, ease of use, usefulness, social influence, facilitating conditions, perceived risks) have a moderate to strong correlation with ‘intention to accept’, further study may reveal that, for example, there are facilitating conditions that greatly increase compatibility and ease of use. Additionally, social influence from friends and family may show a person greater usefulness. By mapping the correlations between antecedent factors, this may provide an ordering in importance of those factors, revealing what businesses should focus on to successfully introduce biometric methods into their services.

Finally, it can be interesting to look deeper into the exact influence of knowledge of / familiarity with biometrics on acceptance. As stated multiple times before, it seems methods that are more often used, seen or heard of score higher on acceptance, with fingerprint recognition being at #1 because of its frequent implementation in smartphones. But further testing is needed to confirm the hypothesis that there exists a significant correlation between knowledge/familiarity and acceptance. This could add (or even replace an existing) antecedent factor when speaking about specific biometric methods.
References


Appendix A

Outlines

A.1 Survey Outline

User Acceptance of Biometrics Survey
- (Compact) Privacy Notice with Informed Consent Click-through
- Residency of the Netherlands
- Part 1: Prior Factors
- Innovativeness
  1. New is Never Wasteful (Likert 5-item scale)
     - I like to spend my time working with new ideas
     - I would still buy a product, even if its benefits are not yet proven
  2. Social Desirability (Likert 5-item scale)
     - I am always nice, even to people who are disagreeable
     - I have never been annoyed when people expressed ideas very different from my own
     - No matter who I am talking to, I am always a good listener
     - I am always willing to admit it when I make a mistake
  3. Novelty Seeking (Likert 5-item scale)
     - I like to experiment with new ways of doing things
     - I like to try new and different things
     - When I see a new device/service, I often buy it just to see what it is like
  4. Risk Aversion (Likert 5-item scale)
     - I like to take a chance
     - When it comes to taking chances, I would rather be safe than sorry
  5. ‘Style’ Consciousness (Likert 5-item scale)
     - I enjoy looking at new technological product or services as soon as they are released
     - Fast changing products and services in technology are a waste of time and money
  6. Satisfaction with Status Quo (Likert 5-item scale)
     - If something is good enough, people should not try to improve it
     - If people would quit wasting their time experimenting, we would get more accomplished
  7. Other-Directedness (Likert 5-item scale)
     - Whenever I have an idea, I find it important to know how others think about it
     - I would like to know what my friends and neighbours think of a product before I try it
- Trust in Technology
8. Self-confidence: I am confident that I can use... (Tiered)
   – Longer existing technology (telephone, TV)
   – Established technology (PC, mobile phones)
   – All the above, and current technology (tablets, smartphones)
   – All the above, and new technology (VR/AR, smart watches)
   – All the above, and future, unreleased technology

9. Personality: I trust... (Dichotomous with middle option)
   – The safety of existing technology
   – The safety of existing technology that gathers personal data
   – The safety of existing technology that stores personal data
   – That non-personal data is well protected
   – That my online data is well protected
   – That new technologies are thoroughly tested to see if they are well protected

• Concern for Data Privacy

10. General, Non-Personal Data: It is my opinion that... (Likert 5-item scale)
    – Non-personal offline data is stored safely
    – Non-personal online data is stored safely
    – Non-personal offline data is better secured compared to general online data

11. Personal Data: It is my opinion that... (Likert 5-item scale)
    – My offline data is stored safely
    – My online data is stored safely
    – My offline data is better secured compared to my online data

• Part 2: Antecedent and Consequent Factors

• Basic/Additional Information Sheet Biometrics. Six biometric factors asked (Face, Speaker, Eye Blood Vessel, Fingerprint, Hand Geometry and Ear Geometry)

• Smartphone with Fingerprint Sensor (Dichotomous)

12. I am familiar with smartphones that have fingerprint sensors, and either own one or would be interested in owning one in the future

• Compatibility (Dichotomous with middle option, answer per biometric factor)

13. I feel like authentication through the following methods is compatible with my needs

• Ease of Use

14. Using this method is easier compared to a login and password (dichotomous)
15. Using this method is easier compared receiving and inputting an SMS code (dichotomous)
16. I think the use of the following methods will be... (Likert 5-item scale, very hard - very easy)

• Usefulness

17. I feel like I would use the following methods, if they were implemented in an online consult service (dichotomous)
18. I feel like I would rather use the following methods than a login name and a password (dichotomous)
19. I feel like I would rather use the following methods than requesting, receiving and inputting an SMS code (dichotomous)

• Social Influence

20. If my friends and family used the online consult service with the following methods, then so would I (dichotomous)
21. If my friends and family trust the safety of the following methods in an online consult, then so would I (dichotomous)

• Facilitating Conditions
22. I would be more inclined to use the following methods if they are supported by trusted companies (government, healthcare institutions, banks) (dichotomous)
23. I would be more inclined to trust and use the following methods if they are admissible in the court of law to identify a criminal (dichotomous)
24. I would be more inclined to use the following methods if I could do so without having to make any purchases to enable me to use it (camera, scanning device) (dichotomous)
• Risks
25. I feel like the following methods can, when compared to the way I currently identify myself at a hospital, more safely secure access to my personal data (dichotomous)
• Intention to Accept
26. I would accept the use of the following methods to get access to data that is personal, but not sensitive (dichotomous)
27. I would accept the use of the following methods to get access to data that is sensitive (dichotomous)
28. I would only accept the use of biometric authentication if (optional open question)
• Intention to Recommend
29. I would recommend the use of the following methods to my friends and family (dichotomous)
• End Page
A.2 Interview Outline Healthcare Professionals

Encryption Code Participant - Stop Time (30 minute interviews)

Profile:

1. Rate from 0 to 10:
   (a) Innovativeness
      i. New is generally better
      ii. I like to take risks
      iii. I am glad if something works ‘well enough’
      iv. I am interested in innovations within healthcare
   (b) I trust
      i. The safety of technology
      ii. The privacy protection in technology
      iii. The ‘honesty/transparency’ of technological companies
   (c) I am concerned about the safety of
      i. Online, non-medical data
      ii. Online, medical data
      iii. My own online medical data

2. What is the most interesting innovation within healthcare?

3. Have you ever been part of an online consultation?
   (a) If so, opinions? If not, why? What should change?

4. Do you see benefits of adding biometrics? What are the positive and/or negative aspects?

5. After implementation, what should the system do?

6. What happens with rejects?

7. Are there any demands that must be met?

8. Do you have any further questions or remarks?
Appendix B

Interviews

B.1 Interviewee List

<table>
<thead>
<tr>
<th>Code</th>
<th>Date</th>
<th>Time</th>
<th>Category</th>
<th>Expertise</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXPInterviewee01</td>
<td>22-05</td>
<td>16:56</td>
<td>Expert</td>
<td>Security</td>
</tr>
<tr>
<td>EXPInterviewee02</td>
<td>31-05</td>
<td>17:21</td>
<td>Expert</td>
<td>Biometrics (commercial)</td>
</tr>
<tr>
<td>EXPInterviewee03</td>
<td>13-06</td>
<td>14:58</td>
<td>Expert</td>
<td>Biometrics (academic)</td>
</tr>
<tr>
<td>EXPInterviewee04</td>
<td>07-07</td>
<td>10:59</td>
<td>Expert</td>
<td>Information Manager</td>
</tr>
<tr>
<td>MPInterviewee01</td>
<td>26-06</td>
<td>17:30</td>
<td>Healthcare Professional</td>
<td>Laboratory Clinical Medicine</td>
</tr>
<tr>
<td>MPInterviewee02</td>
<td>27-06</td>
<td>12:24</td>
<td>Healthcare Professional</td>
<td>Youth Healthcare</td>
</tr>
<tr>
<td>MPInterviewee03</td>
<td>10-07</td>
<td>11:45</td>
<td>Healthcare Professional</td>
<td>Institution for Protected Living</td>
</tr>
<tr>
<td>MPInterviewee04</td>
<td>19-07</td>
<td>12:49</td>
<td>Healthcare Professional</td>
<td>Communicable Disease Control and Forensic Medicine</td>
</tr>
<tr>
<td>MPInterviewee05</td>
<td>20-07</td>
<td>11:02</td>
<td>Healthcare Professional</td>
<td>Neurology</td>
</tr>
<tr>
<td>MPInterviewee06</td>
<td>21-07</td>
<td>15:42</td>
<td>Healthcare Professional</td>
<td>Guided Living</td>
</tr>
<tr>
<td>MPInterviewee07</td>
<td>28-07</td>
<td>12:35</td>
<td>Healthcare Professional</td>
<td>Psychological Help</td>
</tr>
</tbody>
</table>

Note: Interviews were anonymous.
B.2 Coding Experts

Table B.2: Interview Coding Scheme Experts.

<table>
<thead>
<tr>
<th>Topics</th>
<th>Sub-topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric Authentication</td>
<td>‘Does not Exist’</td>
</tr>
<tr>
<td></td>
<td>Not Safe</td>
</tr>
<tr>
<td></td>
<td>Exists (Called ‘Verification’)</td>
</tr>
<tr>
<td></td>
<td>Fast</td>
</tr>
<tr>
<td></td>
<td>Easy to Use</td>
</tr>
<tr>
<td></td>
<td>User Friendly</td>
</tr>
<tr>
<td>Requirements</td>
<td>Max. FRR with given FAR</td>
</tr>
<tr>
<td></td>
<td>Max. Failure to Enrol Rate</td>
</tr>
<tr>
<td></td>
<td>Quality Control</td>
</tr>
<tr>
<td></td>
<td>Supervision Enrolment/Authentication</td>
</tr>
<tr>
<td></td>
<td>Performance Biometrics, Software, Hardware</td>
</tr>
<tr>
<td></td>
<td>Presentation Attack Detection</td>
</tr>
<tr>
<td></td>
<td>Fast Working Time</td>
</tr>
<tr>
<td>Hurdles</td>
<td>Level of Technology in Hospitals</td>
</tr>
<tr>
<td></td>
<td>Creating Routines for Staff</td>
</tr>
<tr>
<td></td>
<td>Set Up Enrolment at Hospitals</td>
</tr>
<tr>
<td></td>
<td>Acceptance of Patients and Staff</td>
</tr>
<tr>
<td>Fail-safes/Alternatives</td>
<td>IRMA (I Reveal My Attributes)</td>
</tr>
<tr>
<td></td>
<td>Additional Password</td>
</tr>
<tr>
<td></td>
<td>Login at MyHospital (I/O at Consultation)</td>
</tr>
</tbody>
</table>
## B.3 Coding Healthcare Professionals

<table>
<thead>
<tr>
<th><strong>Topics</strong></th>
<th><strong>Sub-topics</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric Authentication</td>
<td>Ease of Use</td>
</tr>
<tr>
<td></td>
<td>Proof of Contact</td>
</tr>
<tr>
<td></td>
<td>Secure Feeling</td>
</tr>
<tr>
<td>Hurdles</td>
<td>Age Dependent</td>
</tr>
<tr>
<td></td>
<td>Technological</td>
</tr>
<tr>
<td></td>
<td>Learning/’Getting Used’</td>
</tr>
<tr>
<td></td>
<td>Insert in Routine</td>
</tr>
<tr>
<td></td>
<td>First Visit for Template</td>
</tr>
<tr>
<td>Demands/Requirements</td>
<td>Safety</td>
</tr>
<tr>
<td></td>
<td>Simplicity</td>
</tr>
<tr>
<td></td>
<td>Few Details Shown to Physician</td>
</tr>
<tr>
<td></td>
<td>Short Working Time</td>
</tr>
<tr>
<td></td>
<td>Choice up to Patient</td>
</tr>
<tr>
<td></td>
<td>Low False Reject Rate</td>
</tr>
<tr>
<td></td>
<td>Clear Rules</td>
</tr>
<tr>
<td></td>
<td>No Interruptions</td>
</tr>
<tr>
<td></td>
<td>Good Integration</td>
</tr>
<tr>
<td></td>
<td>Set Boundaries on Authentication</td>
</tr>
<tr>
<td></td>
<td>Paid as Regular Consult</td>
</tr>
<tr>
<td></td>
<td>Well Tested</td>
</tr>
<tr>
<td>Fail-safes/Alternatives</td>
<td>Professional in Control</td>
</tr>
<tr>
<td></td>
<td>Shut off Access EMR</td>
</tr>
<tr>
<td></td>
<td>Stop Consultation</td>
</tr>
<tr>
<td></td>
<td>Ask to Reposition</td>
</tr>
<tr>
<td></td>
<td>Additional Password</td>
</tr>
<tr>
<td></td>
<td>New Physical Appointment</td>
</tr>
<tr>
<td></td>
<td>MyHospital Environment</td>
</tr>
<tr>
<td></td>
<td>Trust the Patients Identity Claim</td>
</tr>
<tr>
<td>Audio-Video Consultations</td>
<td>No Travel Time</td>
</tr>
<tr>
<td></td>
<td>See the Patient</td>
</tr>
<tr>
<td></td>
<td>No Physical Presence (Negative)</td>
</tr>
</tbody>
</table>
Appendix C

Survey Results

C.1 Descriptive Statistics

<table>
<thead>
<tr>
<th>Topic</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Top</th>
<th>Neutral</th>
<th>Bottom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td>64.76%</td>
<td>28.57%</td>
<td>7.78%</td>
<td>16.67%</td>
<td></td>
<td>69</td>
<td>36</td>
<td>21</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>61.69%</td>
<td>33.33%</td>
<td></td>
<td></td>
<td></td>
<td>66</td>
<td>47</td>
<td>19</td>
</tr>
<tr>
<td>Eye Blood Vessil Recognition</td>
<td>47.62%</td>
<td>30.16%</td>
<td>22.22%</td>
<td></td>
<td></td>
<td>60</td>
<td>47.62%</td>
<td>38</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>42.00%</td>
<td>36.51%</td>
<td>21.43%</td>
<td></td>
<td></td>
<td>53</td>
<td>42.00%</td>
<td>40</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>40.48%</td>
<td>31.75%</td>
<td>27.75%</td>
<td></td>
<td></td>
<td>51</td>
<td>40.48%</td>
<td>35</td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td>78.26%</td>
<td></td>
<td>18.11%</td>
<td></td>
<td></td>
<td>84</td>
<td>79.26%</td>
<td>21</td>
</tr>
</tbody>
</table>

**Figure C.1:** Question 13: I feel like authentication through the following methods is compatible with my needs.

<table>
<thead>
<tr>
<th>Topic</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Top</th>
<th>Neutral</th>
<th>Bottom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td>55.96%</td>
<td>38.95%</td>
<td></td>
<td></td>
<td></td>
<td>70</td>
<td>55.96%</td>
<td>17</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>48.41%</td>
<td>34.13%</td>
<td>17.46%</td>
<td></td>
<td></td>
<td>61</td>
<td>48.41%</td>
<td>22</td>
</tr>
<tr>
<td>Eye Blood Vessil Recognition</td>
<td>81.53%</td>
<td>26.19%</td>
<td>22.22%</td>
<td></td>
<td></td>
<td>65</td>
<td>81.53%</td>
<td>28</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>40.48%</td>
<td>36.51%</td>
<td>22.02%</td>
<td></td>
<td></td>
<td>54</td>
<td>40.48%</td>
<td>29</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>37.39%</td>
<td>30.85%</td>
<td>31.75%</td>
<td></td>
<td></td>
<td>47</td>
<td>37.39%</td>
<td>48</td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td>79.25%</td>
<td>15.98%</td>
<td></td>
<td></td>
<td></td>
<td>84</td>
<td>79.25%</td>
<td>4</td>
</tr>
</tbody>
</table>

**Figure C.2:** Question 14: These biometrics are easier in use compared to using a login name and a password.
Figure C.3: Question 15: These biometrics are easier in use compared to requesting and inputting an SMS code.

<table>
<thead>
<tr>
<th>Topic</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Top</th>
<th>Neutral</th>
<th>Bottom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td>62.38%</td>
<td>28.67%</td>
<td>19.60%</td>
<td>66</td>
<td>62.38%</td>
<td>36</td>
<td>30.57%</td>
<td>24</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>46.41%</td>
<td>50.95%</td>
<td>28.63%</td>
<td>61</td>
<td>46.41%</td>
<td>39</td>
<td>30.95%</td>
<td>26</td>
</tr>
<tr>
<td>Eye Blood Vessel Recognition</td>
<td>46.83%</td>
<td>27.78%</td>
<td>25.40%</td>
<td>56</td>
<td>46.83%</td>
<td>35</td>
<td>27.79%</td>
<td>32</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>33.33%</td>
<td>41.27%</td>
<td>25.40%</td>
<td>42</td>
<td>33.33%</td>
<td>32</td>
<td>41.27%</td>
<td>25.40%</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>34.82%</td>
<td>34.82%</td>
<td>20.16%</td>
<td>44</td>
<td>34.82%</td>
<td>44</td>
<td>34.92%</td>
<td>38</td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td>67.92%</td>
<td>22.64%</td>
<td>0.00%</td>
<td>72</td>
<td>67.93%</td>
<td>24</td>
<td>22.64%</td>
<td>10</td>
</tr>
</tbody>
</table>

Figure C.4: Question 16: I think the use of the following methods will be ((Very) Easy - Medium - (Very) Hard)

Figure C.5: Question 17: I feel like I would use the following methods, if they were implemented in an online consult service.
Figure C.6: Question 18: I feel like I would rather use the following methods than a login name and a password.

<table>
<thead>
<tr>
<th>Topic</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Top</th>
<th>Neutral</th>
<th>Bottom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td>46.24%</td>
<td>37.30%</td>
<td>17.46%</td>
<td>67</td>
<td>48.24%</td>
<td>47</td>
<td>37.30%</td>
<td>22</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>40.48%</td>
<td>30.10%</td>
<td>21.43%</td>
<td>54</td>
<td>40.48%</td>
<td>48</td>
<td>30.10%</td>
<td>27</td>
</tr>
<tr>
<td>Eye Blood Vessel Recognition</td>
<td>34.13%</td>
<td>34.93%</td>
<td>30.50%</td>
<td>42</td>
<td>34.13%</td>
<td>42</td>
<td>34.93%</td>
<td>39</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>26.89%</td>
<td>41.12%</td>
<td>31.76%</td>
<td>28</td>
<td>26.89%</td>
<td>29</td>
<td>41.12%</td>
<td>40</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>23.03%</td>
<td>38.89%</td>
<td>38.10%</td>
<td>29</td>
<td>23.03%</td>
<td>49</td>
<td>38.89%</td>
<td>48</td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td>67.92%</td>
<td>27.36%</td>
<td>27.36%</td>
<td>72</td>
<td>67.92%</td>
<td>29</td>
<td>27.36%</td>
<td>5</td>
</tr>
</tbody>
</table>

Figure C.7: Question 19: I feel like I would rather use the following methods than requesting, receiving and inputting an SMS code.

<table>
<thead>
<tr>
<th>Topic</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Top</th>
<th>Neutral</th>
<th>Bottom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td>49.21%</td>
<td>32.54%</td>
<td>18.25%</td>
<td>62</td>
<td>49.21%</td>
<td>41</td>
<td>32.54%</td>
<td>23</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>46.41%</td>
<td>30.16%</td>
<td>21.43%</td>
<td>61</td>
<td>46.41%</td>
<td>30</td>
<td>30.16%</td>
<td>21</td>
</tr>
<tr>
<td>Eye Blood Vessel Recognition</td>
<td>38.89%</td>
<td>25.37%</td>
<td>31.75%</td>
<td>49</td>
<td>38.89%</td>
<td>37</td>
<td>25.37%</td>
<td>40</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>33.33%</td>
<td>32.64%</td>
<td>34.13%</td>
<td>42</td>
<td>33.33%</td>
<td>41</td>
<td>32.64%</td>
<td>43</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>30.85%</td>
<td>31.75%</td>
<td>31.75%</td>
<td>29</td>
<td>30.85%</td>
<td>40</td>
<td>31.75%</td>
<td>47</td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td>66.38%</td>
<td>28.42%</td>
<td>28.42%</td>
<td>74</td>
<td>66.38%</td>
<td>26</td>
<td>28.42%</td>
<td>7</td>
</tr>
</tbody>
</table>

Figure C.8: Question 26: I would accept the use of the following methods to get access to data that is personal, but not sensitive.
Figure C.9: Question 27: I would accept the use of the following methods to get access to data that is sensitive.

<table>
<thead>
<tr>
<th>Topic</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Top</th>
<th>Neutral</th>
<th>Bottom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td>67.14%</td>
<td>26.84%</td>
<td>18.82%</td>
<td>72</td>
<td>57.14%</td>
<td>34</td>
<td>26.84%</td>
<td>15.82%</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>48.41%</td>
<td>32.64%</td>
<td>18.82%</td>
<td>61</td>
<td>48.41%</td>
<td>41</td>
<td>32.64%</td>
<td>24</td>
</tr>
<tr>
<td>Eye Blood Vessel Recognition</td>
<td>50.79%</td>
<td>28.57%</td>
<td>20.63%</td>
<td>64</td>
<td>50.79%</td>
<td>36</td>
<td>20.63%</td>
<td>20</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>41.27%</td>
<td>32.64%</td>
<td>26.19%</td>
<td>63</td>
<td>41.27%</td>
<td>41</td>
<td>32.64%</td>
<td>26</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>57.33%</td>
<td>33.33%</td>
<td>26.19%</td>
<td>47</td>
<td>37.33%</td>
<td>41</td>
<td>32.64%</td>
<td>38</td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td>78.75%</td>
<td>25.69%</td>
<td>25.69%</td>
<td>76</td>
<td>70.76%</td>
<td>25</td>
<td>25.69%</td>
<td>8</td>
</tr>
</tbody>
</table>

Figure C.10: Question 29: I would recommend the use of the following methods to my friends and family.

<table>
<thead>
<tr>
<th>Topic</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
<th>Top</th>
<th>Neutral</th>
<th>Bottom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face Recognition</td>
<td>46.03%</td>
<td>34.12%</td>
<td>19.04%</td>
<td>59</td>
<td>46.03%</td>
<td>43</td>
<td>34.12%</td>
<td>25</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>42.06%</td>
<td>34.12%</td>
<td>23.81%</td>
<td>53</td>
<td>42.06%</td>
<td>43</td>
<td>34.12%</td>
<td>38</td>
</tr>
<tr>
<td>Eye Blood Vessel Recognition</td>
<td>36.64%</td>
<td>32.64%</td>
<td>20.63%</td>
<td>46</td>
<td>36.64%</td>
<td>41</td>
<td>32.64%</td>
<td>39</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>29.37%</td>
<td>38.09%</td>
<td>21.75%</td>
<td>37</td>
<td>29.37%</td>
<td>49</td>
<td>38.09%</td>
<td>48</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>26.19%</td>
<td>38.09%</td>
<td>24.43%</td>
<td>33</td>
<td>26.19%</td>
<td>60</td>
<td>38.09%</td>
<td>45</td>
</tr>
<tr>
<td>Fingerprint Recognition</td>
<td>68.84%</td>
<td>22.64%</td>
<td>22.64%</td>
<td>70</td>
<td>68.84%</td>
<td>24</td>
<td>22.64%</td>
<td>12</td>
</tr>
</tbody>
</table>

82
C.2 Survey Question 28 Answers

Total of 63 answers in eight categories:

1. Always, 5. Ease of use,
2. Never, 6. Trusted supplier,
3. Spoof and misuse prevention, 7. Specific methods,
4. Security and (independent) testing results, 8. If no other option available.

1. Always (seven responses):
   - I would use it all.
   - I see this as a good thing in most cases.
   - No ifs. All of these are better than what we have now.
   - I am okay with biometric identification and already use fingerprint ID on my phone. I would like to see more than one protocol used or at least available.
   - I think it is a great idea.
   - I would always accept biometric authentication.
   - It was personal information.

2. Never (four responses):
   - Doubt it.
   - Sorry: I would not accept the use of biometric authentication for any reason whatsoever, or under any circumstance. The distinction you’ve drawn between identification and authentication is utterly irrelevant, in that individual personal records (used, in theory, for strictly comparison purposes) will still be compiled into a database including mass numbers of individuals. If/when that data storage device gets hacked, all of those individual records can then be used for nefarious identification purposes. I will never allow my biometrics to be recorded as long as I can control that particular set of circumstances.
   - Frankly I don’t give a diddly-damn about all this "privacy" crap! It all happened because of the AIDS stigma, and I think it is a total waste of time and resources! AND got implemented despite the threat posed to the general population from AIDS!
   - I wouldn’t. This is getting creepy and reminds me of movies about the future where you are identified by eyes or hands and I don’t like it. It’s like we are becoming robots and the whole thing makes me uneasy.

3. Spoof and misuse prevention (fourteen responses):
   - It is proven very difficult to fake the biometric (I’m less worried about false rejection, than false acceptance). Fingerprints can easily be re-created. Combining several biometrics is probably safest.
   - It is in some way made impossible for people to impersonate me through showing the system a photo or using recorded audio.
   - 99.99% accuracy is achieved and fail-safes are included. Fingerprints can be easily stolen and used fraudulently. Facial recognition cannot tell the difference between a real face and a mask. Speaker recognition can be beaten with high quality recording.
   - Could not be duplicated or ghosted.
   - I knew it could not be replicated.
   - They can guarantee that it is private, will not be able to be duplicated by others and completely safe.
   - I know without a doubt that the factor uses is only used for this purpose, and is well secured. I do not want the police or my phone company to be able to ask my
hospital to send over a picture of my fingerprint.

- Misuse of biometric data is prevented by design (e.g. only local processing).
- I would only accept it if it was used only for that one facility. For example, if my doctor’s office were to use one of the methods mentioned, I would allow it for that office only. If it was put into some sort of database that any facility or government could access it, then no, I would not accept or use it.
- The use of the authentication protocol seemed commensurate to the potential need for and subsequent usage of the data. I am not a big fan of having additional identification characteristics stored in random sites for their own authentication purposes.
- I was assured the database that stored the information had the highest security.
- I was assured that my information was only shared with the people or places I wanted.
- I might use it if it were only used for medical records and nothing else. Government already has way more than they need access to.
- Only if I knew for certain that Big Brother was not watching everyone.

4. **Security and (independent) testing results** (twenty-one responses):

- I feel like this could be super important for online/video consultations. I would accept it if it has been beta and real world tested to be secure.
- It is proven infallible.
- I would like to see some independent research on biometrics, research that is NOT done by companies that want to sell a system to collect biometric information. I would like to see whether government agencies accept that ear shape or palm shape or whatever is an acceptable method of identification.
- I would accept it if entities that I trust (such as scientific communities and/or research universities) generally feel that particular methods of biometric authentication is accurate and trustworthy.
- It was more secure than an alternative method.
- It was adequately tested.
- I was convinced that a strict security protocol was in place and followed carefully.
- If the technology is proven and is secure.
- It is more secure.
- It was proven safe.
- I was totally convinced it was foolproof.
- I would only accept biometric authentication if it is proven to be the most protective and they develop a stronger protection on my medical information and my voting registration records.
- If it is proven to be safer and able to keep my info private.
- It is reliable and fool proof.
- I had faith and confidence that it is secure.
- It was proven to be accurate and reliable.
- It was safe.
- I felt it was safe and that it was secure and being used in the right way. I think I showed that in my answers but hopefully that spells it out.
- It is proven to be accurate.
- It was proven to be safe and secure.
- If I could be sure my personal information is secure.

5. **Ease of use** (five responses):

- If the error rate - rejection of measure - was no higher than that associated with mis-typing highly complex passwords.
• I could be sure it was safe and it wasn’t too much trouble to use.
• It wasn’t a longer process to succeed. If a password or getting a code takes 20 seconds, but the eye blood vessel recognition would take 30 or more seconds, I prefer the lesser time.
• I knew it would make actions happen more quickly.
• It was easy to use, free of charge and always worked the first time.

6. **Trusted supplier** (two responses):
   • It was used by a trusted source.
   • If a trustworthy company was in charge of the program. One not associated with a government. I am concerned about how the information could be used against people.

7. **Specific methods** (three responses):
   • I have used and designed products that use fingerprint technology. I accept and trust this method of identification.
   • I now use an account with my hospital and doctors office, where I can see my test results before I even go. I love this, I think all except the ear shape would just be more security and you know that’s what we need. But at what price, how much to set all of this in place? I like all except the ear shape.
   • It were a fingerprint.

8. **If no other option available** (seven responses):
   • I was forced to do so. I do not want to use this, I understand (read about a court case) the police can make me open my phone if I use biometrics but not if I use a password or a code so I am less likely to use this to keep my information private.
   • It was required.
   • It was the only way offered.
   • If it was forced upon me to get medical care, I would be forced to either do without the care or give the data. My choice would depend upon how much whatever ailment hurt or inconvenienced me. At present, for my current ailments, I would forgo care rather than submit my data (beyond my fingerprint) for electronic storage.
   • Is strictly necessary.
   • I felt it was a secure site and necessary to prevent fraud.
   • It was mandatory to get my personal information.
### C.3 Acceptance Comparison

Table C.1: Comparison between acceptability (Jain et al., 2002) and acceptance in Q.26 and Q.27.

<table>
<thead>
<tr>
<th>Biometric</th>
<th>Acceptability</th>
<th>Acceptance Q.26</th>
<th>Acceptance Q.27</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Only ‘Yes’</td>
<td>Incl. ‘Maybe’</td>
</tr>
<tr>
<td>Face Recognition</td>
<td>High</td>
<td>62.70%</td>
<td>82.29%</td>
</tr>
<tr>
<td>Voice Print</td>
<td>High</td>
<td>53.97%</td>
<td>78.16%</td>
</tr>
<tr>
<td>Sclera Vessels</td>
<td>Low*</td>
<td>49.21%</td>
<td>69.67%</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>43.65%</td>
<td>65.47%</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>High</td>
<td>40.48%</td>
<td>60.72%</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Medium</td>
<td>73.58%</td>
<td>92.85%</td>
</tr>
</tbody>
</table>

Note: Low < 33%, High > 66%. Eight matches found.

Table C.2: Comparison between acceptability (Jain et al., 2002) and acceptance in Q.26 and Q.27.

<table>
<thead>
<tr>
<th>Biometric</th>
<th>Acceptability</th>
<th>Acceptance Q.26</th>
<th>Acceptance Q.27</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Only ‘Yes’</td>
<td>Incl. ‘Maybe’</td>
</tr>
<tr>
<td>Face Recognition</td>
<td>High</td>
<td>62.70%</td>
<td>82.29%</td>
</tr>
<tr>
<td>Voice Print</td>
<td>High</td>
<td>53.97%</td>
<td>78.16%</td>
</tr>
<tr>
<td>Sclera Vessels</td>
<td>Low*</td>
<td>49.21%</td>
<td>69.67%</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>43.65%</td>
<td>65.47%</td>
</tr>
<tr>
<td>Ear Geometry</td>
<td>High</td>
<td>40.48%</td>
<td>60.72%</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Medium</td>
<td>73.58%</td>
<td>92.85%</td>
</tr>
</tbody>
</table>

Note: Low < 55%, High > 75%. Nine matches found.
## C.4 Correlation Significance

### Table C.3: Pearson Correlation

<table>
<thead>
<tr>
<th>Corr</th>
<th>R-score</th>
<th>p-value</th>
<th>Significant at 0.1?</th>
<th>0.5?</th>
<th>0.01?</th>
<th>Correlation?</th>
</tr>
</thead>
<tbody>
<tr>
<td>C01</td>
<td>0.1392</td>
<td>0.12006</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>Small</td>
</tr>
<tr>
<td>C02</td>
<td>0.1350</td>
<td>0.13176</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>Small</td>
</tr>
<tr>
<td>C03</td>
<td>0.0874</td>
<td>0.33048</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>None</td>
</tr>
<tr>
<td>C04</td>
<td>0.0158</td>
<td>0.86061</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>None</td>
</tr>
<tr>
<td>C05</td>
<td>0.1873</td>
<td>0.03572</td>
<td>-</td>
<td>Yes</td>
<td>No</td>
<td>Small</td>
</tr>
<tr>
<td>C06</td>
<td>0.1005</td>
<td>0.26284</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>Small</td>
</tr>
<tr>
<td>X01</td>
<td>0.0126</td>
<td>0.89391</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>None</td>
</tr>
<tr>
<td>C07</td>
<td>0.1483</td>
<td>0.09747</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>Small</td>
</tr>
<tr>
<td>C08</td>
<td>0.1469</td>
<td>0.10071</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>Small</td>
</tr>
<tr>
<td>C09</td>
<td>0.5640</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Large</td>
</tr>
<tr>
<td>C10</td>
<td>0.6304</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Large</td>
</tr>
<tr>
<td>C11</td>
<td>0.6611</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Large</td>
</tr>
<tr>
<td>C12</td>
<td>0.7096</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Large</td>
</tr>
<tr>
<td>C13</td>
<td>0.6202</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Large</td>
</tr>
<tr>
<td>C14</td>
<td>0.7556</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Large</td>
</tr>
<tr>
<td>C15</td>
<td>0.6933</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Large</td>
</tr>
<tr>
<td>C16</td>
<td>0.7027</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Large</td>
</tr>
<tr>
<td>X02</td>
<td>-0.801</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Large</td>
</tr>
<tr>
<td>C17</td>
<td>0.7103</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Large</td>
</tr>
</tbody>
</table>

### Table C.4: Spearman ρ Rank Correlation

<table>
<thead>
<tr>
<th>Corr</th>
<th>ρ-score</th>
<th>p-value</th>
<th>Significant at 0.1?</th>
<th>0.05?</th>
<th>0.01?</th>
</tr>
</thead>
<tbody>
<tr>
<td>C01</td>
<td>0.106525</td>
<td>0.23515</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C02</td>
<td>0.093905</td>
<td>0.29561</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C03</td>
<td>0.03966</td>
<td>0.65927</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C04</td>
<td>-0.017</td>
<td>0.85014</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C05</td>
<td>0.195105</td>
<td>0.02857</td>
<td>-</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>C06</td>
<td>0.083216</td>
<td>0.35424</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>X01</td>
<td>0.033834</td>
<td>0.70684</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C07</td>
<td>0.105282</td>
<td>0.24069</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C08</td>
<td>0.07477</td>
<td>0.40536</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C09</td>
<td>0.55232</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>C10</td>
<td>0.623723</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>C11</td>
<td>0.642457</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>C12</td>
<td>0.703188</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>C13</td>
<td>0.627123</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>C14</td>
<td>0.709379</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>C15</td>
<td>0.634159</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>C16</td>
<td>0.671042</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>X02</td>
<td>-0.78944</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>C17</td>
<td>0.67558</td>
<td>0.00001</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table C.5: Kendall $\tau$ Rank Correlation

<table>
<thead>
<tr>
<th>Corr</th>
<th>$\tau$-score</th>
<th>p-value</th>
<th>Significant at 0.1?</th>
<th>Significant at 0.05?</th>
<th>Significant at 0.01?</th>
</tr>
</thead>
<tbody>
<tr>
<td>C01</td>
<td>0.08101</td>
<td>0.20233</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C02</td>
<td>0.06560</td>
<td>0.28278</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C03</td>
<td>0.02699</td>
<td>0.66193</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C04</td>
<td>-0.0106</td>
<td>0.86674</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C05</td>
<td>0.13980</td>
<td>0.02601</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>C06</td>
<td>0.06086</td>
<td>0.33684</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>X01</td>
<td>0.02313</td>
<td>0.72513</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C07</td>
<td>0.07904</td>
<td>0.22027</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C08</td>
<td>0.05790</td>
<td>0.38513</td>
<td>No</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>C09</td>
<td>0.43123</td>
<td>0.00001</td>
<td>-</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>C10</td>
<td>0.48619</td>
<td>0.00001</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>C11</td>
<td>0.51949</td>
<td>0.00001</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>C12</td>
<td>0.54921</td>
<td>0.00001</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>C13</td>
<td>0.47661</td>
<td>0.00001</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>C14</td>
<td>0.54453</td>
<td>0.00001</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>C15</td>
<td>0.49303</td>
<td>0.00001</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>C16</td>
<td>0.52748</td>
<td>0.00001</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>X02</td>
<td>-0.65408</td>
<td>0.00001</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>C17</td>
<td>0.54519</td>
<td>0.00001</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
</tbody>
</table>

### Table C.6: Goodman and Kruskal Gamma test

<table>
<thead>
<tr>
<th>Corr</th>
<th>$\gamma$-score</th>
<th>Relationship?</th>
</tr>
</thead>
<tbody>
<tr>
<td>C01</td>
<td>0.369644</td>
<td>Weak</td>
</tr>
<tr>
<td>C02</td>
<td>0.377150</td>
<td>Weak</td>
</tr>
<tr>
<td>C03</td>
<td>0.287564</td>
<td>Weak</td>
</tr>
<tr>
<td>C04</td>
<td>0.155823</td>
<td>None</td>
</tr>
<tr>
<td>C05</td>
<td>0.304976</td>
<td>Weak</td>
</tr>
<tr>
<td>C06</td>
<td>0.324746</td>
<td>Weak</td>
</tr>
<tr>
<td>X01</td>
<td>0.283114</td>
<td>Weak</td>
</tr>
<tr>
<td>C07</td>
<td>0.382727</td>
<td>Weak</td>
</tr>
<tr>
<td>C08</td>
<td>0.456538</td>
<td>Weak</td>
</tr>
<tr>
<td>C09</td>
<td>0.658189</td>
<td>Moderate</td>
</tr>
<tr>
<td>C10</td>
<td>0.691087</td>
<td>Moderate</td>
</tr>
<tr>
<td>C11</td>
<td>0.823259</td>
<td>Strong</td>
</tr>
<tr>
<td>C12</td>
<td>0.703534</td>
<td>Moderate</td>
</tr>
<tr>
<td>C13</td>
<td>0.577567</td>
<td>Moderate</td>
</tr>
<tr>
<td>C14</td>
<td>0.798351</td>
<td>Strong</td>
</tr>
<tr>
<td>C15</td>
<td>0.709222</td>
<td>Moderate</td>
</tr>
<tr>
<td>C16</td>
<td>0.809524</td>
<td>Strong</td>
</tr>
<tr>
<td>X02</td>
<td>-0.67323</td>
<td>Moderate</td>
</tr>
<tr>
<td>C17</td>
<td>0.773459</td>
<td>Strong</td>
</tr>
</tbody>
</table>
Appendix D

Sample Size Calculation

When determining the sample size, the general size can be found by using the following values (Berenson, Levine, & Szabat, 2013):

- The error margin $e$ of the confidence interval. This error margin shows how much the true mean of a population may differ from the found mean. A lower error margin means a higher number of respondents needed.
- The $z$-score of the confidence level. The confidence level shows what the chance is that the real mean falls within the confidence interval. A higher confidence level means more respondents (the $z$-score is the value of a standard normal distributed function at a certain percentage).
- The probability $p$, which shows how answers are distributed (if respondents are expected to answer 50/50, $p = 0.5$, but if there is a bigger change people respondents answer one way, $p$ may be 0.4).

Using these three values, the general population size $n_0$ can be determined by setting

$$n_0 = \frac{z^2 \times p \times (1 - p)}{e^2}$$

Now for the calculations, an error margin of 10% is chosen ($e = 0.1$), with a confidence level of 90% (matching $z$-score equals 1.645). Using the study from Ponemon Institute (2013), where in figure 20 it is stated that on average 71% of the respondents think a trusted organization can use biometrics to authenticate consumers (as long as the biometric data is not accessible to the organization), $p$ is set on 71% ($p = 0.71$). This means that the sample size equals

$$n_0 = \frac{1.645^2 \times 0.71 \times 0.29}{0.1^2} = \frac{0.557}{0.01} \approx 56$$

This means, to have a 90% chance that the real mean $\mu$ lies between our found $\bar{x}$ minus 10% and $\bar{x}$ plus 10%, there need to be at least 56 respondents. After this, the finite population correction factor can be applied. This corrects the general sample size, when the population is not too large. The correction works as follows, for a finite population size $N$:

$$n = \frac{n_0 \times N}{n_0 + (N - 1)}$$

This correction factor however only makes a real difference when the population is quite small, in fact smaller than ten times the general sample size (560 persons). This will not be the case, so the final sample size will be $n = 56$ respondents. However, according to the FluidSurveys Team (2014), the average response rate for email surveys equals 24.8%. This means that in total, at least $\frac{56}{0.248} \approx 226$ surveys need to be send out to acquire sufficient respondents. Increasing
this number will likely also increase the number of respondents, which will lead to a higher confidence level and smaller confidence interval.

Ending up with **126** participants, we can use a margin of error of 6.63% with a confidence level of 90%, a margin of error of 10% and a confidence level of 98.6% or a margin of error of 7% and a confidence level of 91%.
Appendix E

Biometrics-as-a-Service

The following list states (in no particular order) some providers of biometrics-as-a-service. While using such services in the final product may, because of the sensitive nature of the data protected, not be ideal, for demonstrators they can be useful:

- **BioID** at https://www.bioid.com/
  - Provides “anonymous face & voice biometric authentication as a service”,
  - Is stated to be Cloud-based and secure by design, and states to offer privacy by design,
  - Provides a free trial.
- **Aware** at https://www.aware.com/
  - Only face recognition,
  - Claimed to have “market-leading spoof detection and liveness detection”.
- **Jumio** at https://www.jumio.com/
  - Service that combines ID (passport/ID card) check with face recognition.
- **SecureIdentity** at http://secureidentity.nl/
  - Dutch service, created by OT-Morpho, for authentication in Idensys,
  - Requires one-time registration with ID card, claims not to leave any trace of personal information and allows users to “login with a smile”.
- **SmilePass** at https://smile-pass.com/
  - Is a “Free Open access proof of concept, Face and Voice Biometrics Matching & Authentication Service for developers”,
  - Offers both speaker and face recognition,
  - Offered free of charge for low usage.
- **EyeVerify** at https://www.eyeverify.com/
  - Uses the ‘EyePrint ID’, which “uses regular front-facing smartphone cameras to create a cryptographic key used to authenticate users based on the micro features in and around their eyes, the most important of which are the blood vessels visible in the whites of the eyes”,
  - Only available sclera blood vessel recognition service,
  - Claimed on-device verification.