TU WIEN Informatics

KYC onboarding in financial institutions: A best practice criteria catalogue for selection of video identification frameworks

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Business Informatics

by

Markus Wasserbauer, BSc
Registration Number 1327010

to the Faculty of Informatics

at the TU Wien

Advisor: Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Thomas Grechenig

Vienna, 31st March, 2022

Markus Wasserbauer	Thomas Grechenig

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Erklärung zur Verfassung der Arbeit

Markus Wasserbauer, BSc

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 31. März 2022

Markus Wasserbauer

Acknowledgements

Foremost, I want to thank Professor Grechenig for giving me the opportunity to write this thesis. I also want to thank his team of experts for their advice and encouragement. A big thank you goes to Phillip Niemeier as well, who supported me throughout the whole thesis by answering my questions.
Additionally, I would like to thank my parents, friends, student colleagues and my girlfriend who have always been supportive and motivated me throughout my studies.

Kurzfassung

Als eine Konsequenz von Covid-19 und den damit einhergehenden Lockdowns, ist die Nachfrage nach digitalen Bankprodukten und -services extrem gestiegen. Weiters wurde der digitale Wandel im Allgemeinen durch die Ereignisse in den vergangenen zwei Jahren erheblich beschleunigt. Für viele Banken, mit einer oftmals langen Historie, ist es schwierig sich den neuen Bedingungen ebenfalls so schnell anzupassen. Eingesessene Banken benötigen oftmals Entscheidungswerkzeuge, welche ihnen dabei helfen neue Technologien erfolgreich und zielgerichtet einzusetzen. Mithilfe dieser Arbeit werden Alternativen zur physischen Identifizierung aufgezeigt, die jeder neue Kunde, der ein Produkt einer Bank nutzen will, durchlaufen muss. Im Speziellen wird auf die Videoidentifizierung eingegangen, welche bereits seit dem 1. Juli 2017 rechtlich möglich ist. Um den passenden Anbieter, bzw. die richtige Software für die Videoidentifizierung zu finden, bietet der in dieser Arbeit bereitgestellte Kriterienkatalog die notwendige Entscheidungsgrundlage für Banken. Darüber hinaus wird dargestellt, welche Anbieter ihren Anforderungen entsprechen. Der Kriterienkatalog stützt sich auf die nationalen österreichischen Gesetze und somit auf die allgemein geltenden Richtlinien der Europäischen Union zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und ebenfalls auf die Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Die Kriterien sind allgemein gehalten, um somit einen Best-Practice Ansatz verfolgen und von Experten aus der Bankenbranche validiert werden zu können. Des Weiteren kann ein allgemein definierter Best-Practice Kriterien Katalog auch auf andere Jurisdiktionen angewendet werden. Bei der Validierung stellt sich heraus, dass der Kriterienkatalog eine gute Basis darstellt und alle legalen Voraussetzungen erfüllt, um daraus eine Entscheidung zu treffen, welche Anbieter für eine Bank geeignet sind. Die Experten erhalten eine holistische Übersicht über die geltenden Richtlinien und können dadurch schneller eine Entscheidung, in Bezug auf den Einsatz von Software für Videoidentifizierung, treffen. Des Weiteren kann der Kriterienkatalog dazu genutzt werden, um zu überprüfen, ob die bereits eingesetzte Software zur Videoidentifizierung, den aktuellen Anforderungen entspricht.

Abstract

As a consequence of Covid-19 and the accompanied lockdowns, the demand for digital banking products and services has increased dramatically. Furthermore, the digital transformation in general has been significantly accelerated by the events of the past two years. For many banks, often with a long history, it is difficult to adapt to the new conditions so quickly. Established banks often need decision-making tools that help them use new technologies successfully and appropriately. In this thesis, alternatives to physical identification, which every new customer who wants to use a bank's product has to go through, are presented. In particular, video identification, which became legally effective as of 1 July 2017, is discussed. In order to find the right provider or software for video identification, the criteria catalogue provided in this thesis offers the necessary basis for banks to decide which provider meets their requirements. The criteria catalogue is based on Austrian national law and thus on the generally applicable directives of the European Union on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and also on the regulation on electronic identification and trust services for electronic transactions in the internal market. The criteria are kept general in order to be able to follow a best practice approach and to be validated by experts from the banking industry. Furthermore a general defined best practice criteria catalogue can also be applied to other jurisdictions. The validation through expert interviews supports the hypothesis that the criteria catalogue provides a good basis and meets all legal requirements for making a decision on which provider is suitable for a bank. The experts receive a holistic overview of the applicable guidelines and can thus make a decision regarding the use of video identification software quicker. Furthermore, the criteria catalogue can be used to check whether the video identification software already in use meets the current requirements.

Contents

CHAPTER 1

Introduction

Digitalization has shaped the banking sector in the last years or even decade. The next trends for revolutionizing financial services are rather unclear. It may not be a trend, but it is omnipresent: efficiency. To increase performance, profit and other key indicators for banks year by year it is important to not only focus on customer acquisition or product development, but also to ensure higher efficiency in operations. Customers' expectations drive the need for banks to change and adapt their processes and IT infrastructure. However, banks tend to have low process automation and integration of IT [1]. Like all other big companies, banks are getting monitored by their investors, shareholders and additionally by the state. Satisfying all parties is the most crucial thing for continuous growth. The big players in the Austrian banking sector have a long history, which often leads to very conservative and inefficient process structures within these banks. Direct banks, also known as online banks offer only a small product catalogue tailored mostly for retail costumers. These specific and manageable products help younger banks to have very simplified internal process structures in regard of onboarding, offboarding and supervising customers.

Technologies to tackle this issue reach from artificial intelligence in identification processes to reporting software or to the right workflow tools to structure workload more efficiently. The thesis is focusing on the identification and verification process of people via video identification tools. It will provide a best practice criteria catalogue, which provides the reader with all necessary information about choosing the right video identification tool for a specific purpose. Furthermore, it shows the differences between those banks that are innovators, those that are early adopters, or those that, in the worst case, may be considered laggards.

In 1994, Bill Gates said: "Banking is necessary, banks are not." [2]. This statement has more relevance than ever. The big players have to prove that this statement of Gates is not true and therefore have to show their customers new ways of banking.

1.1 Problem description

The regulatory jungle for the KYC [1] principle and the onboarding process increases from year to year. To be compliant to given law is one of the most important goals for banks to avoid penalties from OeNB [2] and ECB [3] [3]. In order to stay compliant, banks have to adapt to the latest regulations quickly. This inflates the onboarding process from year to year [4]. In addition, the problem is that this makes the onboarding process more complex, time consuming and costly [5].

Most European banks use copies of government issued ID cards to verify new customers. They collect them mostly face-to-face. Replacing this kind of non-digital process steps with digital equivalents such as video identification tools can make onboarding easier and more efficient [6]. The problem is that there exist a lot of solutions and therefore it is not easy for banks to find the most appropriate tool for their use case. Moreover, no criteria catalogue for video identification tools exists, which can provide an overview about the most important criteria.

1.2 Motivation

The motivation behind this thesis is to increase the awareness for tools in regards of automation in regulatory processes, decrease human interactions and simplify existing processes. MiFID II [4] is effective since the 1st of January 2018, the 4th AML [5] directive has been introduced in 2017, the 5th and 6th AML directive have both been introduced in 2020 [7, 8]. The regulation flow increases from year to year and will not stop. The need to find an efficient way to implement regulations as quickly and structured as possible is increasing day by day.

1.3 Expected result

The main goal of the thesis is to develop a best practice criteria catalogue for video identification tools. With the help of expert interviews the criteria catalogue will be validated. The criteria catalogue can directly be applied on video identification tools. The result will be a table, which reflects the tools and which criteria the individual tools fulfil and which not. The banks can thus weigh up which tool would be most relevant for them on the basis of their preferred criteria.

[1] Know Your Customer
[2] Austrian National Bank
[3] European Central Bank
[4] Markets in Financial Instruments Directive
[5] Anti Money Laundry

Further aim of the work

The further aim, besides the expected result of this thesis, is to get familiar with the European laws in regard to AML and KYC and to get an understanding what criteria video identification tools have to fulfil in order to be compliant to given law. Another aim is to understand what "best practice" really means and which methodology can be used to identify it. Last but not least, expert interviews are in focus. Not only will the created best practice criteria catalogue be presented but the interviews should also give an insight to future technologies that can be used to identify a natural or legal person.

Research Questions

With the help of the research question an evaluation of the concepted best practice criteria catalogue can be conducted. The research question is defined in a way that the results can be applied on Austrian banks. However, this does not mean that the criteria catalogue can only be applied in Austria. On the contrary, the criteria catalogue can be applied in every European Union member state due to the standardised EU regulation regarding AML and KYC. The focus lies on Austria because the interviewees are experts in the Austrian banking sector. The research question is defined as the following:

> „*Which criteria can be used to guide the decision for or against a video identification software in KYC onboarding for Austrian banks?*“

1.4 Methodological approach

Literature research of regulations regarding KYC and AML

With the help of SLR [6] [9] suitable literature about regulations affecting KYC and AML will be looked up. Regulations which directly affect KYC and AML will be looked up in the European Parliament register [10, 11]. Furthermore to get a better overview why regulations are becoming more and more important in the banking sector, the most relevant regulatory directives and the history of laws which are needed to continue banking will be outlined.

State of the art research of technologies supporting KYC

The state of the art research [12] is focusing on technology which enables the user to automate certain activities or tools which support the daily business in operations for onboarding. The tools reach from automatic signature comparison [13, 14] to video identification [15, 16]. In addition, DLT [7] technology like blockchain [17, 4, 5] can be

[6] Systematic Literature Review
[7] Distributed Ledger Technology

used to increase the automation grade in onboarding processes[18]. All these technologies and more will be gathered to define the best practice criteria catalogue.

Analysis on how the online account opening in Austrian banks work - state of the art KYC onboarding

The state of the art KYC onboarding research is focusing on the seven biggest Austrian banks, as per their balance sheet of 2019 [19]. With the help of this analysis the reader gets an impression on how the onboarding process for certain banks and products is working and what identification technologies they are using. To be able to compare the onboarding processes among all participating banks,the online account opening is used as standard product to trigger the onboarding process. The approach on how the onboarding process is designed will be documented and reported in a summary. The summary also contains the following information:

- Which attributes are requested from the customer?
- When in the onboarding process are the relevant attributes requested?
- How long does it take to conclude the onboarding process?
- How does the identification and verification of the customer take place?

The methodology to conduct the analysis of the Austrian banks is done through an observation [20]. The process steps, that have to be fulfilled to order an online account, will be observed to gain an understanding about what is done in practice.
Throughout the analysis of the onboarding processes of the Austrian banks, several identification and verification methods will be introduced and briefly described:

- Verification in a bank branch
- EPS [8]
- Video identification
- Upload of legal documents like passport, driver license or government issued identification card

Introduction into the research of best practice

The core aspect of this thesis is the development of a best practice criteria catalogue for video identification tools. However, in order to define a catalogue it is important to understand what best practice research is all about. Therefore, a literature research is conducted, which focuses on best practice methodology according to S. Bretschneider [21] and E. Bardach [22].

[8] Electronic Payment Standard

Criteria for video identification tools

With the fundamental knowledge about best practice research, a literature research regarding criteria for video identification tools takes place. The research is focusing on [23]:

- Which countries are supported?
- Does the provider meet European and national KYC standards?
- What databases are used for KYC checks (PEP, sanction lists)?
- Are there add-on solutions which can be integrated in existing software?
- Analyse technologies and risks related to AML and KYC violations.

Applying criteria catalogue on video identification tool

The new found criteria for video identification tools will be applied on a video identification tool, which is used in Austria. The result will be a table, which reflects the tool and which criteria it fulfils and which not. Thus banks can weigh up if the tool is relevant for them on the basis of their preferred criteria. The catalogue will be applied on the video identification tool IDnow [15]. IDnow has been chosen to countercheck the criteria catalogue, as it is used by three of the analysed Austrian banks and therefore is the most used video identification tool in this context.

Validation of the best practice criteria catalogue through expert interviews

The approach of the interviews is a semi-structured one and is split into several parts [24]:

1. Determining purpose and scope
2. Identifying participants
3. Developing the interview guide
4. Conducting interviews
5. Memo and reflection
6. Analysing gathered data
7. Present findings

To analyse the data of the semi-structured interview a thematic analysis takes place [20]:

1. Familiarising with the data
2. Generating initial codes
3. Searching for themes
4. Reviewing themes
5. Defining and naming themes
6. Producing the report

1.5 Structure of the thesis

The thesis is structured as follows: Chapter 2 gives an overview of the legal framework and which laws and regulations have to be considered to stay compliant whilst onboarding customers. In Chapter 3, state of the art technology is mentioned, which supports operation departments in regards of conducting onboarding processes in a KYC conform way. In focus is video identification, which is a sub-process of the onboarding process. Further the used identification and verification methods of the analysed Austrian banks are described. Afterwards the seven biggest banks in Austria (Chapter 4) and their onboarding processes are analysed. In Chapter 5, first of all the theoretical background will be laid for "best practice" and how it can be achieved. Thereupon the practical part for "best practice" research and the analysis of the defined criteria for video identification tools is mentioned. Within Chapter 6 the defined criteria catalogue will be applied on one selected video identification tool. In Chapter 7, the semi-structured interview guide is designed. In addition the results of the expert interviews are analysed. The discussion of the results, a summary and outlook on future work complete the research on this topic.

CHAPTER 2

Regulatory processes

To get a feeling how certain regulatory processes are realized in the European and Austrian law, it is important to provide a short insight into regulations, that are tackled in this master thesis. In the overall regulatory processes in the banking environment, regulations like KYC [9], AML [10], FATCA [11] and CRS [12] are omnipresent. For this thesis, the most important regulations are coming from the AML directive [11] and the KYC regulation [10]. Before diving deeper into the regulatory jungle, it is crucial to understand how the process of defining and executing laws, regulations and directives of the European Parliament is constructed. The process for defining new laws for financial services is supported by the Lamfalussy architecture [25]. This is a four level regulatory approach to define new regulations and directives. It allows a more flexible decision making process as defined in Figure 2.1:

Abbreviation	**Meaning**
EBC	European Banking Committee
EIOPC	European Insurance and Occupational Pensions Committee
ESC	European Securities Committee
FCC	Financial Conglomerates Committee
CEBS	Committee of European Banking Supervisors
CEIOPS	Committe of European Insurance and Occupational Pensions Supervisors
CESR	Committee of European Securities Regulators

Table 2.1: Abbreviation table for Figure 2.1

[9] Know Your Customer
[10] Anti Money Laundry
[11] Foreign Account Tax Compliance Act
[12] Common Reporting Standard

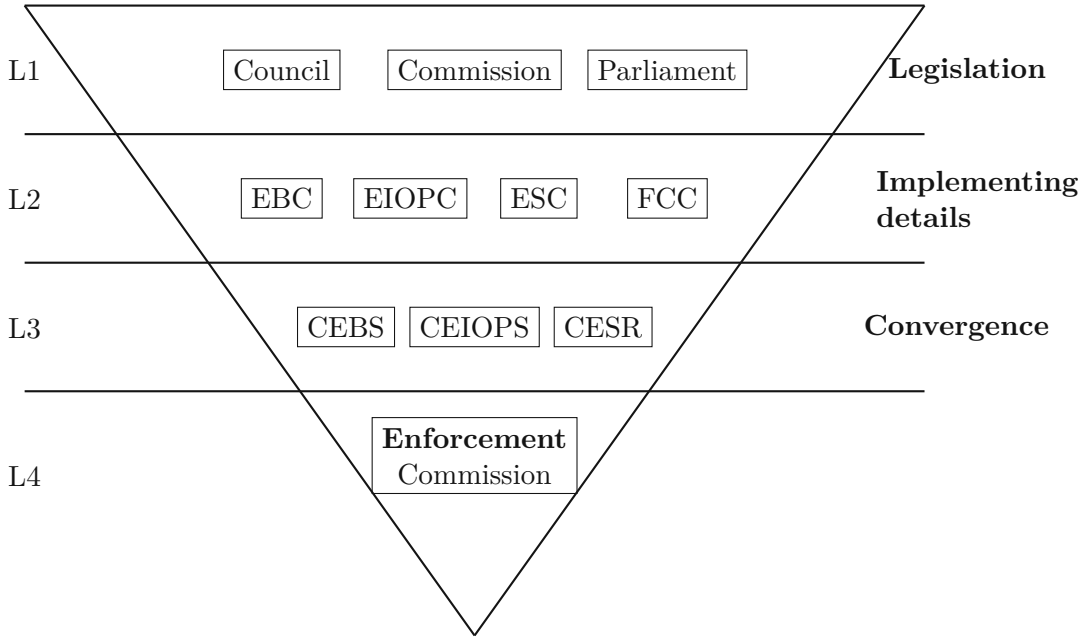

Figure 2.1: Lamfalussy structure (adapted from Committee of European Banking Supervisors [26])

1. **Level**
   The European Parliament and Council adapt the basic laws proposed by the Commission and define a framework for it.

2. **Level**
   The Commission has the discretion to adapt and update all technical relevant measures. Therefore the Parliament and Council can focus on the key political decisions.

3. **Level**
   The three independent supervisory authorities EBA [13], ESMA [14] and EIOPA [15] are responsible for advising the Commission on the adaption of level 1 and 2 in regard to issuing guidelines on the implementation of the rules. The three committees give technical advice regarding the development of implementing measures and promote the consistent implementation of community legislation.

4. **Level**
   The Commission has to ensure the correct enforcement of the new defined EU rules by the national governments.

[13] European Banking Authority
[14] European Securities and Markets Authority
[15] European Insurance and Occupational Pensions Authority

2.1 Systematic literature research for regulatory processes

There is a huge amount of legal acts available on the internet. A SLR [16] approach is helping to identify and aggregate suitable literature about regulations affecting KYC and AML. The key elements of SLR are [9]:

1. **Specify and formulate the research question**
   The thesis is tackling the following research question: Which criteria can be used to guide the decision for or against a video identification software in KYC onboarding for Austrian banks? This SLR is focusing on the legal framework of the research question which deals with the regulation and directive about AML and KYC.

2. **Develop a review protocol**
   The first method that will be used to undertake SLR is a manual search of regulations and directives in Google Scholar [27]. Due to the fact that the found papers refer and cite regulations and directives of the European Parliament register, the second method is to directly look up literature in the European Parliament register published since 2006. The European Parliament register was selected additionally as the European Parliament provides the basic laws for the whole European Union banking sector. Another selection criteria is that only regulations and directives are selected. Furthermore papers which directly analyse specific AML and KYC regulations are considered, even if there are not released from the European Parliament itself.

3. **Choose appropriate search keywords**
   Major terms: KYC, know your customer, aml, anti money laundry
   Related terms: onboarding, customer, review, money laundering, terrorist financing, identification, directive, regulation

4. **Conduct search and collect studies**
   The first part of the selection is to focus on the regulations and directives of the European Parliament. Because of the detailed selection criteria and the defined keywords only a handful of regulation and directive papers of the European Parliament are relevant, as illustrated in step "Select primary (relevant) studies". In total, 317 documents have been found on the European Commission homepage in connection with "AML directive" and 60 documents with "KYC regulation". However, almost all of them are referring to the legal acts described in Step 5.

5. **Select primary (relevant) studies**
   The four most relevant papers are:

   - Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing from 2008 [28]

[16] Systematic Literature Research

- Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing from 2018 [11]
- Directive on combating money laundering by criminal law from 2018 [8]
- Regulation on electronic identification and trust services for electronic transactions in the internal market [10]

The directive for AML has been included three times. In detail, the latest three directives, one from 2008 [28] and two from 2018 [11, 8]. The 6th version of the anti money laundry directive is the latest one and has been introduced from the European Parliament in 2018, but came into effect in December 2020.

6. Analyse primary studies

For the primary analysis the four documents mentioned above have to be read carefully and a data extraction takes place. Necessary data which need to be extracted are the source of the document, main topic area, the authors, summary and quality evaluation. After reading through the primary studies the AML directive from 2008 [28] can be discarded. The six versions of AML directives are building on each other. This means the latest AML directive (6th) [8] is building on the 5th, the 5th on the 4th and so on. Thus, the 6th AML directive reflects all information from past directives. Hence, it can be stated, that it is another addition to the previous AML directives.

6th AML Directive

Source of the document: European Commission
Main topic area: Prevention of the use of the financial system for the purpose of money laundering or terrorist financing
The authors: European Commission
Summary: The 6th AML directive increases the transparency about who really owns companies. Furthermore, the accessibility of financial intelligence units for centralised bank account registers has improved. In addition, the cooperation between anti-money-laundering supervisors and the European Central Bank has made improvements to be faster and more efficient.
Quality evaluation: The criteria for the quality evaluation are based on two quality assessment questions [9]:
QA1: Is the literature search likely to have covered all relevant studies?
Answer: Yes, the 6th AML directive is the latest one and equates to an extension of the 5th and 4th AML directive.
QA2: Are the review's inclusion and exclusion criteria described?
Answer: Yes, the regulation contains the necessary search keywords, a timestamp and the article is described as a directive.

KYC Regulation

Source of the document: European Commission
Main topic area: Electronic identification and trust services for electronic transactions in the internal market

The authors: European Commission
Summary: Know your customer is relevant to prevent financial crime and money laundering. It is the mandatory process to identify and verify the identity of the client who is willing to do business with a financial institution.
Quality evaluation: The criteria for the quality evaluation are based on two quality assessment questions:
QA1: Is the literature search likely to have covered all relevant studies?
Answer: Yes. In fact, there is only one regulation concerning electronic identification for the European Union.
QA2: Are the review's inclusion and exclusion criteria described?
Answer: Yes, the regulation contains the necessary search keywords, a timestamp and the article is described as regulation.

7. Report results

ID	Author	Date	Topic type	Topic area
1	European Parliament[8]	2018	AML	Directive
2	European Parliament[10]	2014	KYC	Regulation

Table 2.2: Systematic review studies for regulations

Table 2.2 summarizes the systematic literature review for regulatory processes. Both the directive for AML and the regulation for KYC build the regulatory fundament for defining the KYC onboarding process which will be presented in Chapter 3.

2.2 Know Your Customer - KYC

As Know Your Customer principle banks and other financial institutions understand the verification of the personal and business data of customers for the prevention of money laundering and terrorist financing on the basis of the Money Laundering Act 2008 [28]. In more detail, KYC is the mandatory process for identifying and verifying the identity of the customer when they get onboarded. After the initial onboarding the customer has to be reviewed periodically over time. High risk customers have to be reviewed every year, medium risk customers every three years and low risk customers every five years. Financial institutions are responsible to be compliant to the latest KYC regulation [10] and AML directive [11]. If they disobey any KYC or AML laws they have to expect to be fined by the legislator. In the European Union the legislator is ECB [17].

The KYC process can differ from company to company. It is not defined in the AML directive or KYC regulation how the process for onboarding per se has to look like. But essential checks have to be done and include:

[17] European Central Bank

- Identity verification
- Determination of the beneficial owner
- Documentation of the audit trail
- Periodical review of the customer
- Risk review based on official risk lists (PEP [18], sanctions)

The KYC process differs from financial institution to financial institution. Usually, an institution starts to gather data and information by using electronic identity verification. The identity is verified against existing databases which contain for example information about political exposed persons, sanctions or citizenship.
For KYC processes in general, it is also important to document all steps, which have been undertaken to identify a natural or legal person. Therefore, documents, which are needed for the identification, must be stored and be available for a certain period.

2.3 Anti Money Laundry - AML

Money laundering in the context of the financial sector is the act to camouflage money, which originates from an illegal activity, so that it looks like it originated from a legal source. In more detail, it means people with a criminal background conceal the origin of the money they illegally made and try to return it into the economy through e.g. a legitimate cash-based business. Money laundering can be split into three main steps as seen in Figure 2.2.

1. **Placement**
   In the first stage, the criminals, also called launderer, insert dirty money into a legitimate financial institution. This is the riskiest step in the whole process, because banks are checking large amounts of cash and have to report high-value transactions.
2. **Layering**
   In the second stage, money is sent through various financial transactions. This is the most complex step. With the help of these transactions the launderer changes the form of the money and also makes it more difficult to trace it.
3. **Integration**
   In the last stage, money re-enters the mainstream economy in legitimate looking form, due to the fact that it appears to come from a legal transaction. The launderer can then do whatever they want with the money, and from here on, after a legal transaction, the money can not be traced back.

[18] Political exposed person

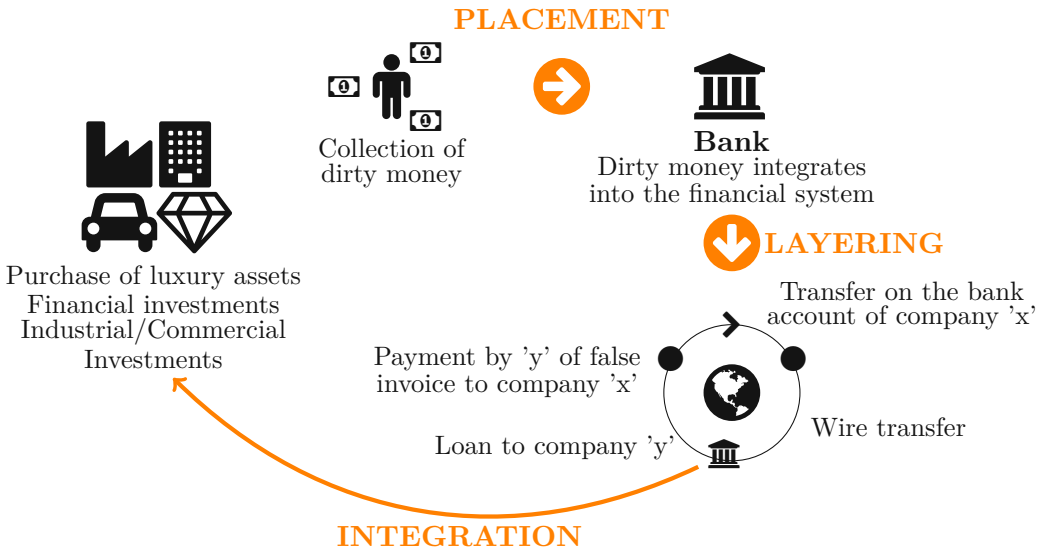

Figure 2.2: Money laundering main steps (adapted from [29])

The problem with money laundering, of course, is that if it is not prevented, criminal activities would pay off. This, in turn, encourages criminals to continue their illegal businesses or to even extend them further. To prevent this kind of behaviour, banks and other financial institutions have to comply with the latest AML laws, which support the process of revealing money laundering.

The first anti money laundering directive has been introduced in 1991. The second one in 2001, the third in 2006, the fourth in 2017, the fifth in 2020 [30] and the latest version of the AML directive at the end of 2020 [31]. The fourth to sixth directive have been introduced within a range of 4 years. This pattern underlines that technology is emerging at tremendous speed and laws have to be adjusted and extended in a much shorter period of time. The anti money laundering directive in general is building on five different controls to prevent money laundering [32, 11]:

1. **Criminalization**
   The first control is criminalization. It helps governments to sentence individuals involved in money laundering independent of their country of residence. That makes transnationally organized crime easier to be uncovered.

2. **Know your customer**
   Financial institutions have to do a background check before onboarding new customers. The focus lies on the verification and identification of the customer, the identification of the beneficial ownership of the company, politically exposed persons and the overall risk of the customers. Existing clients have to be reviewed on a regular basis.

3. **Record management and software filtering**
   Financial institutions must also monitor their customers transactions. In Europe, transactions in excess of 50.000 € have to be reported to the countries national bank. There are additional transaction patterns, which also lead to a monthly report to the countries national bank.

4. **Holding period**
   The holding period is a method, which binds the customer to keep the deposit on an account for a certain amount of time. Accordingly, it is not possible for the customer to withdraw a large amount of money in a short period of time which, would exacerbates money laundering.

5. **New technology**
   As a result of progress in technology, new possibilities will be discovered to identify malicious transactions, like with the help of machine learning and artificial intelligence. Algorithms are getting smarter after a certain learning period. Thus it becomes easier for machine learning algorithms to identify malicious behaviour, the longer they are used.

2.4 Difference between KYC and AML

Table 2.3 shows the most significant and important differences between KYC and AML in general. KYC is a necessary step to identify and verify customers, which helps to detect suspicious behaviour of customers and make it more difficult for criminals to enter the legal business. AML, on the other hand, is defining the legal framework to avoid money laundering. As a result, it is possible to state that KYC is a descendant of AML.

	KYC	**AML**
Process	Verification of customers by gathering personal information and verify it	Legal controls over the suspicious activities and transactions
Purpose	To prevent criminals from entering into the business platforms	To avoid money laundering and terrorist financing across the globe
Elements	Identity validation, risk identification and management	Risk assessment, detection, prevention and reporting of suspicious transactions
Features	Should be state of the art (digital), efficient and thoroughly done	Should be holistic, coherent and well thought-out

Table 2.3: Difference between KYC and AML (adapted from [33])

The two legal frameworks, necessary to onboard new customers, have been laid out in more detail in the previous chapter. The next chapter describes the latest technology in regard to KYC and further technological developments which may simplify the onboarding process for customers and financial institutions.

CHAPTER 3

State of the art KYC onboarding

This chapter provides an overview of the latest trends in technologies and tools which can help identify natural and legal persons in regard to KYC. Newly developed technologies may help to simplify the daily business of operation departments in financial institutions. The found state of the art technologies and tools from this chapter will be used to define a best practice catalogue, which is defined in Chapter 5.1.

The methodology used for the state of the art research in this chapter is based on the literature review goals of R. Baumeister and M. Leary [12]. They do not describe the steps how literature reviews should be conducted, on the contrary, they describe the main goals, which the literature reviewers try to accomplish. The five goals, from most to least ambitious, are:

1. Theory development
2. Theory evolution
3. State of knowledge
4. Problem identification
5. Historical development of theory and research

The literature review surveys the state of knowledge on KYC onboarding technologies. This type of goal is used to provide an overview of a specific area, but it does not intend to provide new ideas or insights. It gathers valuable information, which is used to get a general understanding of technologies already in use.

Furthermore this chapter provides a brief overview of all identification methods, which are available and used by the analysed Austrian banks described in Chapter 4. But

before these identification methods are described, Section 3.1 provides a brief definition of the terms identification and verification, to get a better understanding of the upcoming sections. Section 3.2 describes several methods, which support the process to identify and verify a natural person. As the verification of the customers signature is necessary to ensure that the contract between the bank and the customer is duly signed and compliant to given law, Section 3.3 provides details of technologies supporting the signature verification. The signature verification goes hand in hand with Section 3.4, which describes the possible methods for verifying an electronic signature in more detail. Section 3.5 gives a detailed overview of the identification methods used by Austrian banks. An identification can be accompanied by call agents or can be done by the customer without any interaction with employees of the bank.

3.1 Definition of identification and verification

This section provides a brief overview of the different terminologies of identification and verification. Both terms are used in this thesis quite often and should not be mixed up, as both terms have a completely different meaning.

3.1.1 Identification

In short, one can say that identification is answering the question "Who are you?". Identification can include many things like whome we claim to be as a person, whome a computer system claims to be over a network or simply what authority we claim to have. The identification process does not claim anything else and it does not contain any sort of verification of the identity. The claim of an identity can be fulfilled by full names, usernames, images, account numbers, fingerprints, etc. The problem is that not all of the mentioned identifiers are unique or can be duplicated or spoofed easily. Furthermore, physical identifiers such as height, colour, hair, weight, etc. can be changed. Therefore, the claim of an identity is not a reliable information on its own [34, p.24].

3.1.2 Verification

On the other hand, verification is answering the question "Are you who you say you are?". When someone is asked to show their driver's license, birth certificate or other similar forms of identification, this is for the purpose of identity verification. If the claimed identity matches with the proof of identity document, then the verification is successful. An identity verification can be circumvented by using tampered identification documents [34, p.25]. That is why there has to be an identification process in place, which acknowledges these issues and requests the right and complete information of people.

3.1.3 Authentication

For the purpose of completion, the term of authentication shall also be clarified. The step to verify people and to check if the claimed identity is correct, is called authentication. It should not be mistaken with the term authorization. Authentication only establishes a check if the claimed identity is true, but does not imply what the identity is allowed to do. This is the task of authorization. Common factors for authentication are usually passwords, PINs or biometric data, etc. [34, p.26].

3.2 Identification with video tools

The identification and verification of a person is the core aspect of KYC onboarding. One must distinguish between the identification of a natural person and the verification of signed documents, which are needed to do business with one another. With the help of video identification tools, a person usually is identified by a call agent. More and more video identification providers also offer video identification through a so called eID [19].

3.2.1 Video Identification

A usual KYC onboarding starts with gathering various information about the potential customer. The identification process is part of the onboarding and requires a potential customer to authenticate itself and therefore several documents are needed from the customer. Table 3.1 shows different document types which are needed to onboard a potential customer. Note, that this summary of document types contains documents needed for institutions, corporations or private individuals. For retail business, only a photo ID is necessary. However, for legal entities the proof of identity is much more complex and therefore a lot more documents are needed to identify them.

The documents which are needed can be categorized in different document groups like verification of ownership, CRS/FATCA, identification, evidence of existence and proof of graphic signature. The identification process itself can again be split into the identification of authorized persons of a company and the identification of the company. In this section, the identification of authorized persons stands in the foreground.
Usually a prospect who wants to use services of a bank has to come into one of the banks branches and identify themselves. The identification process in person uses the same documents like the video identification. The biggest disadvantage for the customer is though, that they have to come to the branch in person only to show to the bank's employee that they are in fact the person on the passport. This is not only time consuming, but also unpleasant for the future customer due to the fact that every authorized person for a company would have to do that. Here, the difference to the retail business is that in the world of corporate banking a company which may want to request a loan has several authorized persons, which all would have to show up at the bank in person.

[19] Electronic Identity

Document Type	Document Category
Company register extract	Verification of ownership
Certification of good standing	Verification of ownership
Register of Shareholders	Verification of ownership
Beneficial owner information	Verification of ownership
Organisation chart	Identification
Passport copy	Identification
Driver license	Identification
Government issued ID card	Identification
KYC letter	Identification
Passport copy	Proof of graphic signature
CRS/FATCA self certification	CRS/FATCA
License (for funds, banks and other companies dealing with financial services))	Evidence of existence

Table 3.1: Summary of different document types needed for KYC onboarding

The basic technology behind video identification is already well researched. More and more providers of such systems focus on AI [20] to help making the authentication more secure. Companies such as IDnow [15] or Signicat [35] are specialized on products for video identification. With the identification tool IDnow, it is possible to authenticate a person via mobile phone and the tool is also able to verify the used identity card. The benefits for the customer are obvious:

- Location independent identification of the person
- Time flexibility
- No additional hardware necessary
- Real time processing
- Fast

There are a many vendors providing such services with their own tools. As it will be mentioned in Chapter 4, for the seven biggest Austrian banks, there exist three different video identification vendors. What all banks using video identification have in common, is that they use only one aspect of video identification, namely the identification of the user via a call agent. That means the user has to be pro active in the call, for example when showing their official photo ID like passport, driver license or ID card into the camera after the call agent is asking them to do so. Furthermore, it could be that the user has to wait in queue until a call agent from the service provider is available. As mentioned

[20] Artificial Intelligence

before, using call agents is only one aspect of doing video identification. Another form of video identification is an automated one. The automated version of video identification does not need to be supervised and conducted by a call agent. This brings the advantage for the user to do the video identification at anytime they want. Another big advantage is the minimising of costs. Without the need of having call agents, the automated video identification is significantly cheaper than the non-automated method. The domain of application for fully automated video identification solutions are for example:

- Completing a liability insurance online
- Verification of age
- Registration for health insurance
- Proof of life
- Approval of the identity towards third parties like banks, insurance companies or gambling

Some vendors who offer both video identification methods in the European Union are IDnow [15], webID [36] or youniqx [37]. A vendor who is specialized in automated video identification is for example Nect [38]. The video identification, no matter if automated or not, can only be used for natural persons.

3.2.2 Electronic Identity

The electronic identity is a digital solution to identify natural persons, like the video identification. To the contrary of video identification, eID can be a fully automated identity verification process. IDnow offers both a video identification and an eID solution. Other providers like Nect [38] focus exclusively on eID solutions. With the help of the eID solution from Nect the user only has to take a selfie from themselves and upload an official photo ID. The AI [21] is focusing on five verification procedures:

1. **Real time check**
   Has the user taken the photo in this very moment?
2. **Liveliness check**
   Does the selfie contain a real person or is it just another photo or a person with a mask?
3. **Face match**
   Is the face of the selfie the same as the face on the official photo ID?

[21] Artificial Intelligence

4. **Document check**
   Is the provided document for verification an official photo ID, has it been tampered and are the security features for the ID available?

5. **Manipulation check**
   Has the information on the photo ID been changed or is the user using deep fakes?

There are a lot of use cases for eID like for example verifying your identity for an insurance, airline and hotel check in or verification of your age. Governments have already established own eID solutions to make visits to government offices obsolete. In Austria a pilot project called "ID Austria" [39] is already live. Although the intention to digitize governmental services is a good one, it is long overdue and the pilot project itself is not yet methodologically sound. The reason for that is a person, which wants to use the governmental solution of eID still has to do the registration in person by an local authority. No full digital solution is offered. "ID Austria" can be used for digital governmental services, electronic signature, electronic post office and in the near future the Austrian government will release the digital ID. This digital ID can then be used as a visual identity card, like the driving license. These are all use cases where a simple verification of the identity takes place. But probably the biggest disadvantage for now is that eID verification is not supported within the AML directive yet. That means eID can not be used for any verification where the AML directive is executed. Therefore, the eID can not be used for an online onboarding of a banking product. A review of the eIDAS regulation has been initiated by the European Commission in 2020 to collect feedback on how the services and development can further be extended and how an EU digital identity can be realized [40].

3.2.3 Distributed Ledger Technology

Probably one of the most known use cases for DLT is the blockchain technology. This technology is mostly influenced by Bitcoin, which was the first cryptocurrency that was not owned by a central authority. DLT was originally used to create money and transfer it via the Internet. However the blockchain technology can not only be used to create cryptocurrencies. With the help of the blockchain technology, also decentralized systems can be governed and run by using smart contracts. One of the most prominent examples in this area is Ethereum. Combining these technologies can simplify the KYC onboarding process [17]. In order to preserve confidentiality, personal and customer related data must be secured. Confidentiality describes the function of protecting data from unauthorized persons. One way to achieve confidentiality is the encryption of KYC data, before adding it to the blockchain. An example how encryption of data can be realized, is through symmetric encryption algorithms [41]. The encryption process is triggered by the symmetric key creation before data is added to the blockchain. The key is only shared with the customer which has to be onboarded. When the customer wants to get in contact with another financial institution, through the KYC blockchain, it only has to share the generated secret key. With the shared secret key the financial

institution can unlock the KYC data from the blockchain. Symmetric encryption is not the only encryption method, but it has already been used to optimize a KYC blockchain system[41].

If a customer wants to do business with several banks, they have to go through the KYC onboarding process many times, as illustrated in Figure 3.1. The customer has to pass the approval process of every bank, which makes it more expensive for the customer to do business with several banks, but also for banks, the effort increases tremendously.

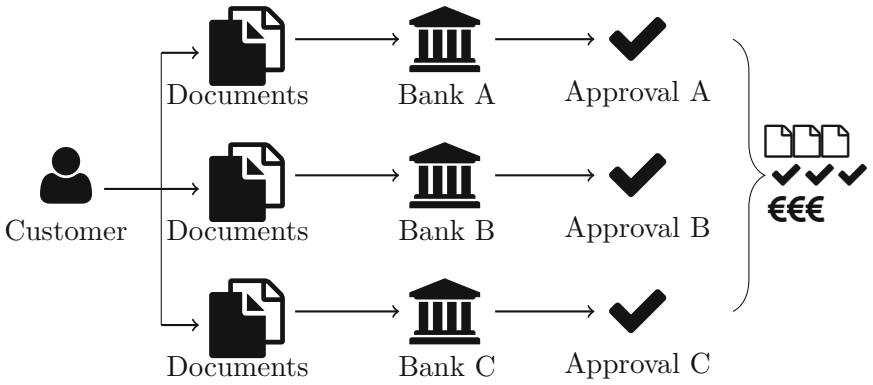

Figure 3.1: Current KYC process for one customer who wants to do business with several banks (adapted from [17])

With the help of DLT a comprehensive banking ledger can be introduced which is chronological and decentralized, as seen in Figure 3.2. This ledger can be used by the participating banks to execute the KYC process and if a customer would get verified a second time, the bank can just verify the results of the KYC onboarding which has already been done once. The KYC process would only need to be executed once for every customer. This saves time and money for all participating banks in the ledger. The results can easily be shared between banks and the DLT would act as single point of truth regarding the KYC verification.

KYC onboarding tools which already focus on blockchain are for example KYC-Chain [42] or KYCstart [43]. KYC-Chain is a web service, which can handle the complete KYC process for corporations, institutions or private individuals. With the help of DLT the identification and verification can be done with a high level of transparency. Furthermore, the identification process is done in an automated way with algorithmic validity checks [42]. KYCstart is Deloittes proof of concept to use blockchain technology for KYC as a service. The service should help companies to execute the KYC process for several financial institutions at once. The output is a digital identity which can be shared among permissioned financial institutions and platforms. With the help of DLT, customers have control with whom they share their data. This enables them to keep track of the authorizations they already gave [43]. As already mentioned in Subsection 3.2.2 the European legislation is lagging behind. For that reason there exists no legal foundation,

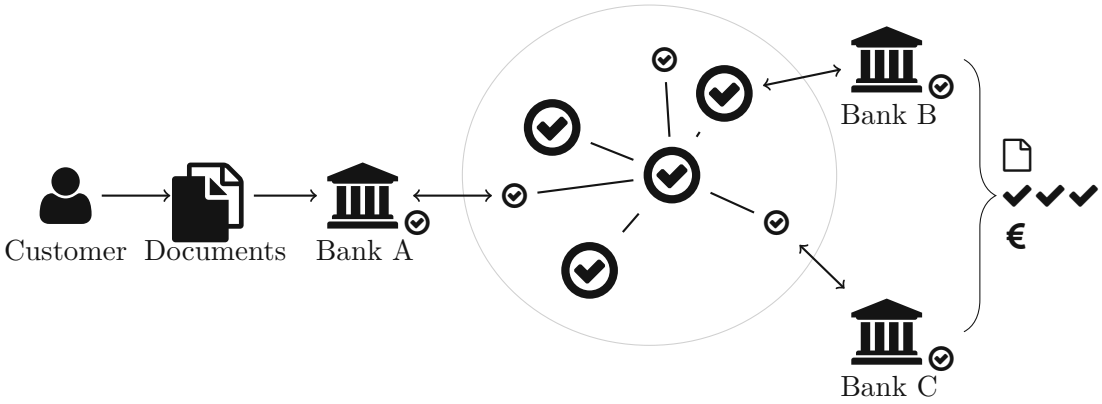

Figure 3.2: KYC process using DLT to minimize a customers interaction with several banks (adapted from [17])

on how these technologies can be used, yet. Therefore adaptions in the latest AML and KYC legislations are necessary.

3.2.4 OpenID Connect

OpenID Connect is an identity layer which is build on top of the OAuth 2.0 protocol. With the help of OpenID Connect, the identity of the end-user based on their performed authentication can be verified. The advantage of such an identity layer is that it can be applied by all types of web-based (native) and mobile clients. Hence, OpenID Connect is a further development of the OAuth 2.0 protocol [44].
With the help of the OpenID extension eKYC & IDA [22], a standardised communication of the identity information can be established. It claims the information on how the verification was done. The key features are [45]:

- Standardised interface to communicate how a verification from a user has been performed, based on the REST [23] paradigm
- The Interface can differentiate between verified and unverified claims in the same assertion
- Through the communication standard it can simplify the integration of remote identification processes
- Vendor solutions can interoperate with other standardised identity verification components

The OpenID Connect protocol is defined as follows:

[22] Electronic Know Your Customer and Identity Assurance
[23] Representational State Transfer

1. The relying party (RP) or client sends a request to the OpenID Provider (OP)
2. OP authenticates the End-User and obtains authorization
3. OP responds with an ID token and usually an access token
4. RP can send a request with the access token to the userinfo endpoint
5. The userinfo endpoint returns claims about the End-User

Figure 3.3 is an illustration of the OpenID Connect protocol. The client sends the authentication request to the authorization endpoint using HTTPS [24]. In the next step the authorization server logs in the End-User or verifies whether the End-User is logged in. The authorization server obtains an authorization decision for the requested claims. After the authorization is determined, the authorization server returns a response. After the server response the client makes an access token request using the authorization code to obtain tokens from the token endpoint. In the last step the userinfo endpoint, which is an OAuth 2.0 protected resource, returns claims about the authenticated End-User.

To validate the access token from the authorization endpoint, the client first of all needs to hash the octets of the ASCII [25] representation of the access token. Secondly the left-most half of hash is encoded with the base64url encoding scheme. In the third and last step of the access token validation the value of the hash must match the hash value of the authentication response.

OpenID Connect is used by a variety of providers. Only to name a few tech giants like Microsoft, Google or Oracle. But also in the financial industry OpenID Connect has big potential. Softbank or PayPal are also certified OpenID providers [46]. The Open ID extension eKYC & IDA is still in a development phase and is constantly refined by its own working group. The working group is also involved in the review of the eIDAS regulation. Governmental eID solutions in Europe, which already use OpenID Connect, are BankID or France Connect [47].

3.3 Signature verification

A KYC onboarding process can only be completed successfully if the necessary documents are duly signed. To ensure not only a verification of the authorized persons, but also a verification of the documents, which have been signed took place, signature verification is a must. It could be claimed, that this technology is the pendant to video identification. Specific tools, which are using this technology are Signotec [13] or Namirial [14]. Signotec offers an own API [26] which, includes functions like:

[24] Hyper Text Transfer Protocol Secure
[25] American Standard Code for Information Interchange
[26] Application Programming Interface

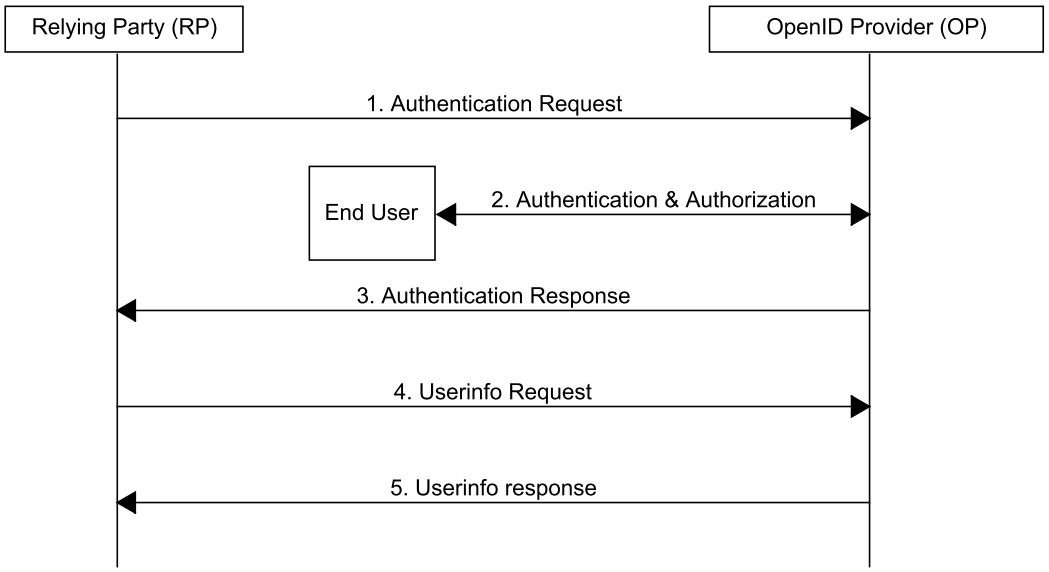

Figure 3.3: OpenID Connect protocol (based on [44])

- Capturing signatures
- Capturing images and biometric data
- Interface for hardware which is used to capture signature in a digital form (e.g. mobile devices, signature pads, tablets)
- PDF display, navigation, editing
- PDF signature

With the help of Signotec, documents can be verified without the need for employees of a bank to do a manual check of the signatures. The bank can develop its own signature database. With this database, newly signed documents, and thus the signatures of the customers can be compared with the already existing ones in the signature database. Signotec can save certain biometric data like pressure strength, pressure curve, writing direction and speed just to give a few examples. To save biometric data, it is crucial to know that specific hardware in support of this kind of tracking, is necessary. With a normal smart phone, no biometric data can be saved. However, Signotec also offers own signature pad solutions which can be used to capture biometric data.

Figure 3.4 shows how a signature verification can be done completely digital and without any physical documents. Such a process can also be automated. For this, other

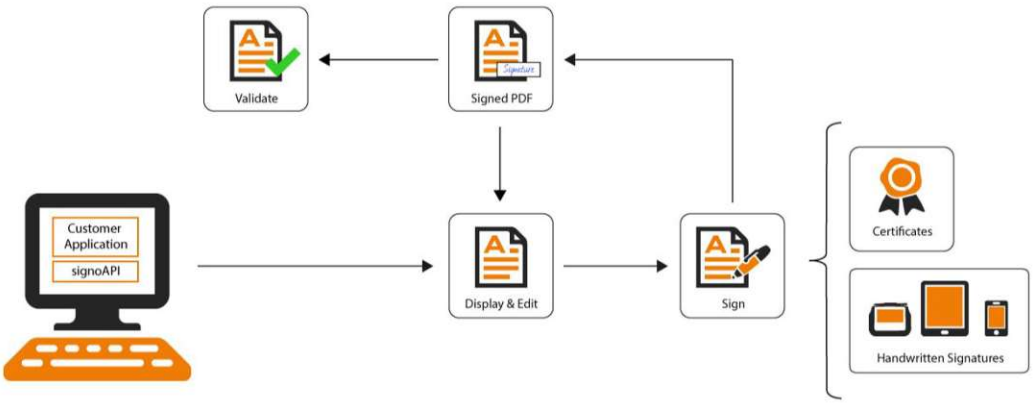

Figure 3.4: Signotec signature verification workflow (Signotec, e-signature solutions GmbH [13])

components like a document management system would be necessary. A digitized and automated signature verification process may save financial institutions time in regard to signature checks. Furthermore, physical documents do not have to be archived anymore. Consequently, physical archives would get redundant. This saves space and money.
The different types of electronic signatures BES [27], AES [28] and QES [29] are described in more detail in Section 3.4.

3.4 Verification methods with the help of electronic signature

A legal binding contract between two parties can only be achieved if the contract has been duly signed from the involved parties. An electronic signature is not just a scanned handwritten signature someone may assume. An electronic signature must fulfil certain aspects to be equivalent to a handwritten signature and also needs to be compliant to the eIDAS[30] regulation [10]:

- **Authenticity**
  Describes that the document originates from the given person and that the person can be uniquely identified.

- **Integrity**
  Recognizes any manipulation of the signature or the signed document immediately.

[27] Basic Electronic Signature
[28] Advanced Electronic Signature
[29] Qualified Electronic signature
[30] Electronic Identification and Trust Services

Nowadays, it is common to sign documents via an electronic signature, mobile phone signature or citizen card. These three mentioned electronic signature types are supported by the Federal Ministry of the Republic of Austria [48]. There are three different types or quality levels of electronic signatures which have to be distinguished. Every type of signature has certain requirements. The basic electronic signature has the weakest requirements in regards of authentication and integration and the qualified electronic signature has the strongest requirements and is therefore the only type of electronic signature, which is a digital equivalent to the handwritten signature. The Subsections 3.4.1, 3.4.2 and 3.4.3 introduce all three types of electronic signature, which are defined by the European Union and can be found in the eIDAS regulation [10] which is also referred as KYC regulation in this thesis.

3.4.1 Basic electronic signature

As already mentioned in Section 3.4 the basic electronic signature is the weakest signature type for signing a contract with regard to legal significance. An example for a basic signature can be a scanned handwritten signature pasted on a document or some tools providing signature features, by the help of which a user can sign a document with a predefined handwritten font, which is entered by keyboard. It depends on the country and therefore on national level if this kind of electronic signature is legally binding. This type of signature does not provide any evidence that the signatory is really the person they pretend to be. Therefore, authenticity is not fulfilled. In addition, integrity can not be assured because the signature can be exchanged easily and there is no protocol or anything comparable which logs activities regarding the basic electronic signature.

3.4.2 Advanced electronic signature

In contrast to the basic electronic signature, the advanced electronic signature and the document signed with it are protected through cryptographic features. The following measures have to be fulfilled:

- The identity of the signatory has to be verified.
- Nobody else can sign in the name of the person which signed the document initially.
- All changes in a document that happen after the signing are tracked.

Both authenticity and integrity are given in the case of the advanced electronic signature. Therefore, it already can be used for more sensitive contracts like a credit agreement or life assurance.

3.4.3 Qualified electronic signature

Lastly, the qualified electronic signature is the most secure digital signature one can apply in the European Union. It is in general an advanced electronic signature which,

uses a QSCD [31] to create the electronic signature and is therefore based on a qualified certificate. The measures for a qualified electronic signature are:

- A dedicated hardware or QSCD only the verified person can use. As hardware someone can use a mobile phone, like in Austria for the "Handy-Signatur", a card reader or a QSCD which is stored at a QTSP [32].
- For the signing process of the document, a QTSP has to be used.
- A certified based digital/electronical ID will be attached to the document, which is issued by the respective QTSP.

In some countries of the European Union already an advanced electronic signature can be used to sign legally binding documents. On the other hand, many countries insist that a qualified electronic signature needs to be used for such purposes.

3.5 Identification methods used by Austrian banks

One can distinguish between physical identification, where the customer has to be identified in person and electronical identification. The biggest advantage of electronical identification is for sure the flexibility of the customer. In times of the corona pandemic online banking gained more and more popularity. This has to do with the lockdowns and shutdowns of businesses in order to control the pandemic. Banks were able to digitize a lot of their products already before the pandemic, therefore it was easier for customers to do business with banks and their online products than with producers of physical products [49]. However, in order to do business with the bank a customer needs to be identified first.

3.5.1 Video identification

For the sake of completeness video identification is once more mentioned in Section 3.5, as it is also used by Austrian financial institutions. Detailed information regarding this topic can be found in Subsection 3.2.1.

3.5.2 Identification with official photo IDs

When talking about photo IDs in the seven investigated Austrian banks, it is possible to differentiate between three types of IDs:

- The classical passport, which every citizen can request.

[31] Qualified Secure Signature Creation Device
[32] Qualified Trust Service Provider

- The drivers licence, someone gets after finishing their drivers license course. It is admitted as official proof of identification in Austria, but not in other countries of the European Union.
- A government issued identification card, which also can be used as travel document within the European Union.

Nowadays, all of these mentioned document types are machine-readable. This is not only necessary for video identification tools but also for other digitized identification methods. One use case is the plain upload of such documents for the purpose of verification, as mentioned in the analysis of Erste Bank Group AG in Chapter 4, if someone is opening an online account. The Austrian passport and identification card have a separate machine-readable area, where the most important attributes regarding the person are stored. Both photo IDs are ten years valid after they have been issued [50]. The newly issued Austrian standard driver license as of 2013 expires after 15 years [51].
Even though all three mentioned photo IDs have an expiration date, the identification via a photo ID upload can be tricky. The government is using watermarks, tactile structures, reversible figure and changeable optical stripes to make the IDs tamper-proof. Banks, which provide identification services like the upload of a document, have to ensure that all mentioned tamper-proof features are available and that the uploaded document is no forgery.

3.5.3 Electronic Payment Standard - EPS

EPS is an online payment system, which has been developed in cooperation with Austrian banks. An EPS transaction is only available for customers of Austrian banks, which offer this type of transaction. This means that not every in Austria registered bank supports this service. However, the bigger banks like Erste, Raiffeisen, Bank Austria, Oberbank do so. In addition, it is also an electronic identification service. The identity service can verify a natural person via the online banking portal of the customers bank. Significant differences to other online payment systems are [52]:

- No data transaction to third party providers is needed
- No registration needed
- Server location in Austria

No registration and transaction to third party providers is necessary because EPS can interact with the participating banks online banking systems directly. The requested and verifiably data are [52]:

- First name

- Last name
- Birthdate
- Address
- Academic title
- IBAN [33]

The biggest disadvantage for this type of identity verification is, that a person which wants to use electronic identification with EPS technology, already has to have a bank account at one of the participating banks. Because the requested data has to be verified at least once somewhere.
An alternative to EPS, from the same publisher, is the identification method eID Bank-Ident. This method verifies the same attributes as EPS. Instead of a bank transaction the data is verified through the bank of the user, who is using the eID Bank-Ident [52]. One use case is to share the KYC status of the natural person, which has already been identified by its bank, to service providers. The service providers do not have to ask the customer about their personal data anymore and the customer does not have to provide their personal information to third parties. The communication between the service provider, customer and bank is done through a standardised XML [34] interface.

3.5.4 Physical identification in the bank branch

The last and least important identification method for an online account opening is the physical identification in a bank branch. This method is only mentioned, since one out of the seven analysed banks, namely Oberbank, does not offer any digital or digitized identity verification. This method is for an online account opening outdated. For other banking products, it may still be a state of the art verification method. However, a customer whose intention is to use an online product, probably does not want to visit a banking branch. Especially in times of the Covid-19 pandemic, a lot of customers increased their internet and mobile banking activities [53]. With this method, the employee of the bank is verifying the customers identification by checking an official photo ID as described in Subsection 3.5.2 and the customer confirms it by signing a confirmation.

Many technologies have been introduced in this chapter. These technologies have no national boundaries. Furthermore the different identification methods used by the seven biggest Austrian banks and what electronic signature types the European Union supports are mentioned. The next chapter gives an overview of how Austrian banks are aware of these technologies and how they conduct the onboarding of new customers.

[33] International Bank Account Number
[34] Extensible Markup Language

CHAPTER 4

KYC implementation in Austrian banks

To get an impression on how the onboarding process for online products works, the seven biggest Austrian banks will be analysed. The seven biggest banks are selected on basis of their balance of assets as of 2019 [19]. The output of this chapter summarizes the state of the art onboarding process in the mentioned banks for a online banking product. Furthermore, it will give the reader insights on how the investigated banks have implemented the guidelines for KYC and AML from ECB.

4.1 Conducting the analysis of the seven Austrian banks

An observational study involves several steps, but there is no single right way to conduct it [20]. First of all the setting for the observation needs to be defined (4.1.1). In the second step it has to be clarified, what exactly has to be documented (4.1.2). The third and last step gives an insight about the focus of the study (4.1.3).

4.1.1 Selecting settings for the observation

To ensure a comparability between all seven banks, the same product is used to analyse the onboarding process. The online account is probably one of the most used products in any bank due to the fact that every person needs an account either to receive a salary, unemployment benefits or just to transfer money to service providers [54]. Furthermore, all mentioned banks offer this type of product. The focus of the onboarding process lies on how the identification and verification of the individual, who wants to open an online account, is designed and implemented. Thus the technical analysis of the process stays in the foreground, and therefore an analysis of the product itself in regard to cost and condition is not made.

4.1.2 Documentation of the observation

For the analysis of the online account opening, a standardized approach will be defined beforehand. This ensures that for every bank the same aspects of the onboarding process are analysed so that a comparison between all participants is possible. The approach for analysing the banks is the following:

1. Which information of the customer is needed to complete the online account opening?

2. How is the process designed? In more detail the analysis will answer questions like when are user data requested, when are personal data needed, are CRS/FATCA information gathered and when, is there a summary of the entered data and contract details before completing the online account opening?

3. How is the identification and verification of the potential customer working?

4.1.3 Focus of the observational study

The seven biggest Austrian banks according to their balance sheet sum [19] are:

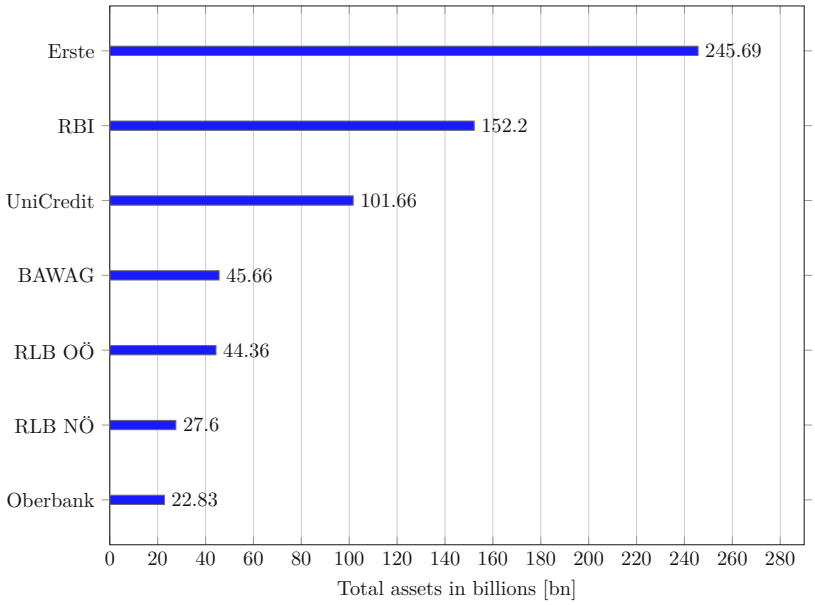

Figure 4.1: Seven biggest Austrian banks in 2019

Abbreviation	Legal (full) name of the bank
Erste	Erste Group Bank AG
RBI	Raiffeisen Bank International AG
UniCredit	UniCredit Bank Austria AG
BAWAG	BAWAG P.S.K.
RLB OÖ	Raiffeisenlandesbank Oberösterreich AG
RLB NÖ	Raiffeisenlandesbank Niederösterreich-Wien AG
Oberbank	Oberbank AG

Table 4.1: Abbreviation table for Austrian banks in Figure 4.1

Erste Bank Group AG

The biggest Austrian bank in regard to total assets is Erste Bank Group AG. To create an online account there, some information from the customer is needed:

- Amount of account receipts
- Official photo ID like passport, drivers licence, ID card
- Personal data like name, address, birthdate
- A phone number which is valid in Austria, Germany or Italy

According to the website of Erste Bank Group AG, the online account opening takes about 10 minutes. First of all, the user is asked if they are already a customer of Erste Bank Group AG. If yes, the onboarding process would be already over, because the customer just has to log in and select the new product. All the other information regarding the person is already known by the bank. However, since the analysis is about a new customer onboarding and the identification and verification of a person, the testcase implies that the person is not a customer of the bank yet. After the "already a customer?" question the user is forwarded to the product side of the online account. Subsequently the user has to fill in the amount of cash they will receive per month and from which source it is derived, like salary, pension or social security benefit. Furthermore, the customer has to approve that this account is for their own use and that they are not a PEP [35]. Afterwards, the customer has to provide information where their tax domicile is.
On the second page of the onboarding process, the user is asked to fill in their personal data. The mandatory fields for the personal data are first name, last name, birthdate, country of birth, profession, nationality, zip code, domicile, street, email address, phone number and which type of identification is used to verify the user (passport, drivers licence or ID card). Depending on the selected identification type, other fields have to be filled in. However, the ID card and validity date are always mandatory.

[35] Political Exposed Person

Lastly the user is presented a summary of all entered personal data and the product details. On this page, the bank asks the user how the contract documents should be distributed (per mail or in electronical form). The user can change their personal data in the summary if anything has been typed in wrongly. After the confirmation to receive the contract details per e-mail, a SMS [36] is sent to the phone number the user has stated. The SMS contains a pin code which is used to "sign" the contract, as well as the terms and conditions of the bank.

Erste Bank Group AG is not using video identification to verify customers during their online account opening process in the first place. Instead the verification is realized with a simple upload of a passport, driver license or ID card. After finishing the data input for the online account opening, in the last step the legitimation process is triggered. Without a legitimation the online account opening can not be finished. For the legitimation Erste Bank offers EPS or video identification.

Raiffeisen Bank International AG

In contrast to all other banks analysed in this thesis, RBI is the only bank, which limits its business in Austria to corporate customers and other financial institutions. The retail business is done only in the 13 CEE countries where RBI is active.

The information which is needed to open an online account is not comparable to other banks in this thesis, due to the fact that the account opening can only be done for business customers. Therefore, also the amount of data needed for the online account opening is different.

Document Type	Document Category
Company register extract	Verification of ownership
Certification of good standing	Verification of ownership
Register of Shareholders	Verification of ownership
Beneficial owner information	Verification of ownership
Organisation chart	Identification
Passport copy	Identification
KYC letter	Identification
Passport copy	Proof of graphic signature
CRS/FATCA self certification	CRS/FATCA
License (for fund, banks and other companies dealing with financial services))	Evidence of existence

Table 4.2: Summary of different document types needed for KYC onboarding

The process is designed in a way, that the user needs to be in contact with a relationship manager before they can start the online account opening. The user can trigger the

[36] Short Message Service

onboarding process only after a relationship manager has sent them an invitation link. After receiving the invitation link the user can edit the prefilled contract sheet. The prefilled information comes from the KYC onboarding, which has to take place before the online account opening. The KYC onboarding can also be done completely online. After the customer information has been added, users may set up their account preferences. This includes the authorized account holders and legal representatives for the company. Signing the contract is performed by an electronic signature verification.

RBI is using the video identification tool IDnow [15] to verify the identification of the person, which is doing the online account opening for the company. For the video identification an identification proof like passport, driver license or ID card is required. Moreover, the user needs a device with a camera and internet access.

UniCredit Bank Austria AG

Bank Austria belongs to UniCredit, one of Italy's biggest banking groups. At Bank Austria, the data needed from the customer are:

- Official photo ID (passport, driver license, ID card)
- E-Mail address
- Telephone number
- Personal data like name, address, birthdate

The online account opening process takes about 10-15 minutes and starts with an information side, where the user has to approve certain statements:

- They are at least 18 years old and open the account for themselves
- Their main residence is in Austria
- They will not transfer more than 50.000 Euro on their new created account
- They have only one citizenship
- They are no PEP and neither in close contact with a PEP

All personal relevant data like name, birthdate, nationality and address have to be entered in the first process step. Furthermore, the user has to choose the desired services. These comprise payments, cash investments or payments outside the EU [37] and EEA [38]. In the second step, the user is asked to agree to the terms of Bank Austria's external partner

[37] European Union
[38] European Economic Area

youniqx Identity AG, which executes the video identification. For the video identification, the user needs a good internet connection and a webcam. In the last process step, after the legitimation has been successful, the user can sign the contract via a password send to their mobile number.

The identification and verification for the online account opening is done via video identification. Bank Austria is not conducting the legitimation on their own, but instead outsources this process step to a company, which is specialized in video identification.

BAWAG P.S.K.

The online account opening process at BAWAG provides the user almost the same information like Erste or Bank Austria. To finish the account opening, several steps have to be fulfilled:

- Filling in the online account contract
- Identity verification and signature

The estimated time to finish the online account opening is stated as seven minutes. Like with Erste, the user is asked at BAWAG if they are already a customer of the bank or if they are a new customer. Furthermore, the user is asked to give their agreement on the following topics:

- Receiving a constant income
- Having no negative association for the protection of creditors entry and also no PEP hit
- The main domicile is in Austria
- Minimum age of 18
- That this account is used under the consumer protection act

After confirmation of above mentioned statements, the user has to fill in their birthdate, birth of place, nationality, address, profession, net income and highest completed education. In addition the user is asked about their relationship status and if they have an additional citizenship. In addition, the employer and the industry have to be filled in. Afterwards, the user is forwarded to the site where they can find a summary of the prefilled contract. Afterwards, the user can choose between video identification or EPS[39] identification. If the user chooses the video identification they can sign the contract via SMS TAN or mobile signature otherwise only SMS TAN is possible. The advantage of

[39] Electronic Payment Standard

EPS identification is that it can be done at any time, whereas video identification is linked to the operating hours of the service provider.

BAWAG is giving the user the choice how they want to identify themselves. In the case of Erste, RBI or Bank Austria, there has always been only one option for identification and verification. For both identification techniques, BAWAG cooperates with external partners like WebID (video identification) and mPAY24 (EPS identification).

Raiffeisenlandesbank Oberösterreich AG

RLB OÖ is one of eight "Landesbanken" of Raiffeisen in Austria. Before the online account opening the user is not informed about which data are needed for the onboarding.

The onboarding process starts by entering the name and salutation of the user. Furthermore, a telephone number and an e-mail address have to be entered. In the second step the birthdate, birthplace and country of birth have to be entered. As an additional information, the user has to enter their nationality as well as the requested account type. In addition, the country of residence and address, have to be stated as well as the profession and the civil status. After prefilling the personal data, RLB OÖ wants the user to select a bank branch. RLB OÖ is also asking if the user wants to shop additional insurance products, which are compatible with the online account. Additionally, the bank asks the user if they want to use a credit card with this account as well. In the last process step, the user has to approve that they are opening the account for themselves and have no tax activity in the USA. The prefilled contract will be sent to the users e-mail address.

For identifying the person and signing the documents the user can choose between several verification methods.

- EPS/Mail
  With an EPS transaction the user will be identified but still has to send the contract details with all necessary documents like account agreement, deposit guarantee, consent to electronic delivery and self disclosure physically signed to the bank branch. If the user is not using EPS for the verification of the identity they have to send a valid photo ID like passport, driver license or ID card to the bank branch as well. Sending of all necessary documents can be done online or in physical form with a letter.

- Bank branch
  The user can print the contract details and sign them at home. Afterwards they have to visit the bank branch to verify their identification.

- Video identification
  At the external partner IDnow [15], the user can do the video identification with the help of their smart phone or computer with webcam.

Raiffeisenlandesbank Niederösterreich-Wien AG

As already mentioned for RLB OÖ, RLB NÖ is also one of the eight "Landesbanken" of Raiffeisen. Both institutions are independent financial institutions. However, in regard to the online onboarding RLB OÖ as well as RLB NÖ are using the same online platform. The only difference in the whole onboarding process is that usually someone living in Vienna or Lower Austria would select RLB NÖ as bank and someone living in Upper Austria would select RLB OÖ as bank. This is because RLB OÖ as the broader bank branch network in Upper Austria and RLB NÖ on the other hand has the broader bank branch network in Vienna and Lower Austria.
From a technical point of view, the Raiffeisen online platform can distinguish between different financial institutions in the Raiffeisen sector due to the different bank codes.

For the sake of completeness, the different identification methods the user can make use of are an identification through EPS/Mail, visiting a banking branch in person or do video identification with the external provider IDnow [15].

Oberbank AG

Oberbank is the smallest bank of the "big seven" according to Figure 4.1. The onboarding process is split into four steps - product, customer data, bank branch/appointment and summary. In the first process step, the user has to select which product they want to use specifically and if they are already customers of Oberbank. In addition, the user has to enter if they want to use the online banking services, if they want a credit card as well and lastly, if in addition to the online account, also a saving account should be established. In the second step, the user has to enter their personal data like first name, last name, address of their residence, birthdate and their contact details like telephone number and email address. Afterwards, the user has to choose a bank branch. Employees of the chosen bank branch will get in contact with the user to finalize the onboarding.

Oberbank AG is the only bank out of the seven analysed ones, where the user is not able to finish the online onboarding on their own. A physical interaction with the bank branch is necessary to complete the onboarding process.

4.2 Summary of the onboarding processes

To summarize the approach of the analysis it can be stated, that the analysis is only focusing on one specific product - the online account. Furthermore, it must be mentioned that the onboarding processes, which have been analysed, have all been done online. Of course, everyone can go into a bank branch of their choice and buy a new banking product, but the focus lies on online onboarding. The supported identification methods mentioned in Table 4.3 are the ones offered to the user in the online onboarding process.

Bank	Product	Supported identification method	Third party provider
Erste	Online account	Upload official photo ID, EPS, Video identification	none
RBI	Online account	Video identification	IDnow
UniCredit	Online account	Video identification	youniqx Identity AG
BAWAG	Online account	EPS, Video identification	WebID, mPAY24
RLB OÖ	Online account	EPS, Video identification, bank branch	IDnow
RLB NÖ	Online account	EPS, Video identification, bank branch	IDnow
Oberbank	Online account	bank branch	none

Table 4.3: Different onboarding methods for the seven biggest Austrian banks

Erste is not offering video identification for this specific purpose in the first place. The user has to upload the official photo ID to get identified and to finish the online account opening. Only afterwards the legitimation via EPS or video identification takes place. RBI has a different approach and offers its non-retail customers video identification in house. The ID agent is working in house but RBI is using the video identification software from the German company IDnow. UniCredit on the other hand, also offers video identification, but the identification is done from their external partner youniqx. BAWAG is offering two different identification methods. The identification can be verified with EPS or video identification. In both cases, BAWAG works with external partners. For EPS, they use mPAY24 and for the video identification WebID. RLB OÖ and RLB NÖ give the user the choice of three different identification methods - EPS, video identification or a physical visit at a bank branch of choice. If the user wants to visit the bank branch they have to take their prefilled contract details from the online onboarding with them. Both banks use for video identification the services of IDnow. Lastly, Oberbank is not providing any online identification at all. The user can do the online onboarding, but is asked to come to a bank branch of their choice to complete the online onboarding process.

There are several different identification methods Austrian banks use for verifying a potential customers identity. The next chapter gives a theoretical overview of best practice in general and further of the defined best practice criteria catalogue.

CHAPTER 5

Criteria catalogue for video identification tools

Building up on the fundamental knowledge gained in Chapter 2 about KYC/AML, this chapter is focusing on the terminology of best practice and the creation of a best practice criteria catalogue for video identification solutions. With the help of the criteria catalogue, the reader gets an overview of which criteria are essential and are seen as best practice in the field of video identification. Some criteria may be more obvious than others, like for example criteria which have to be fulfilled to stay compliant to national law. On the other hand, an example for a criteria which is not that obvious, can be the provision of APIs and how easy they can be integrated in already existing software landscapes of financial institutions. The identified best practice criteria have been evaluated with a qualitative approach according to E. Bardach [55, 56]. At the end of the chapter, a summary of all mentioned criteria is presented.

5.1 Best practice

The approach of improving a company's performance by identifying, communicating and facilitating practices that look like they work successful somewhere else is called "best practice" [22]. It is not an official definition, but it is not easy to evaluate one true definition either. Several authors are defining "best practice" differently as Table 5.1 shows. In this context besides "best practice" also terms like "good practice" and "smart practice" can be found in literature. These terms relate to each other with regard to best practice research, but may be used in different matters. In the research of "best practice" we differentiate between the target and the source site. On the one hand, the target side is the business which wants to improve its performance. On the other hand, the source side is providing the inspiration for the target side. The best practice research can in general be divided into four steps [22]:

1. **Analysing target side**
   In the first step of the general best practice research, the target side has to find out what the concrete problems are and in what aspects it falls behind others. Therefore, the target side needs to have a clear mission and vision. The mission statement describes how the company is going to achieve the vision in a long-term perspective. The vision statement describes the long-term goal of the company and what it wants to achieve in the future. The target side should ask itself "what exactly is going wrong?" and "why?".

2. **Identifying best or smart practices**
   In the identification phase, the target side looks for examples of working practices that seem to be superior compared to the ones they use themselves. One can identify these working practices as best practice or smart practice.

3. **Explanation**
   The identification is one thing. Why the identified practice is working as it does, is another one. In the explanation phase, the target side tries to understand the identified practice and what exact role it plays in the source side.

4. **Extrapolation**
   The last phase in the best practice research deals with converting the experience from the source side to the target side.

A. Vesely differentiates between the quantitative microeconomic BPR [40] and case study-based qualitative BPR [22]. In Subsection 5.1.1 and 5.1.2 the two different approaches are discussed in more detail.

5.1.1 Quantitative Microeconomic BPR

The quantitative approach has been characterized by S. Bretschneider. According to his definition, best practice describes a way of action which is better than any alternative action and still follows the same goal. There are two conditions, which must be fulfilled to identify "best practice" [21]:

1. **The condition of completeness**
   One must include all possible and comparable approaches. However, in reality it is nearly impossible to consider all possible approaches at once, and therefore the set of cases for comparison are usually limited to geographical or temporary aspects. A representative sample of approaches is not sufficient enough due the fact that there is no guarantee that the "best" approach will be contained.

2. **The condition of comparability**
   All examples in a given set must be comparable in regard of actions, outcomes

[40] Best Practice Research

Definition Best Practice Research	Source
In a general sense, the term best practice refers to the most efficient way of doing something. The fastest method that uses the least resources (including labour and parts) to create the highest quality output is the “best practice.” Almost every thinkable industry has adopted best practices in some aspect of its processes, but those that have made use of it successfully and publicly have typically done so in the fields of technology development, quality control, project management, teaching (on the college and secondary circuits), manufacturing, healthcare and sales.	"Best practices" - Encyclopedia of Management (2009) [57]
The term “best practice” implies that it is best when compared to any alternative course of action and that it is a practice designed to achieve some deliberative end.	Bretschneider (2005) [21]
The phrase “best practices” or, in the singular, “best practice” is business jargon arising from the management tool known as “benchmarking.” The assumption underlying this term is that production and management processes are uniform enough so that a “best practice” can be identified and then adopted more or less “as is” by another entity.	"Best practices" Encyclopedia of Small Business (2007) [58]
The most precise definition of best practice research is the selective observation of a set of exemplars across different contexts in order to derive more generalizable principles and theories.	Overman and Boyd (1994) [59]

Table 5.1: Different definitions of best practice research (adapted from [22])

and contexts. A comparability can be shown through a relationship between the cause and effect of an action. S. Bretschneider uses the empirical approach of production theory to link the input and output of an action. With the help of statistical techniques complex relationships can be identified and furthermore help to increase the comparability of cases.

5.1.2 Case study-based qualitative BPR

The qualitative approach has been characterized by E. Bardach. According to him, the term "best practice" is misleading because most of the time we can not be sure that we have implemented the best approach of all possible approaches which have been identified to solve a certain problem. This is exactly the mentioned issue with the condition of completeness of S. Bretschneider. As it is almost impossible to take all options into consideration, E. Bardach tried to find another term - "smart practice", which suggests to have a look on an existing smart or interesting idea in a given practice. Exactly this smart idea should be studied by the researcher, and in a final approach, it should be

evaluated how and in which context it is applicable on the target side. This cost effective practice is called "smart practice".
In his context, a "smart practice" can be anything, which creates value and at the same time is cheap to accomplish. It has to be essential and supportive. In more detail, this means that an essential aspect of a "smart practice" produces value in regard to that executed practice. The supportive aspect in "smart practice" focuses on the effectiveness of an executed practice. Every "smart practice" itself uses the mechanism principle, which E. Bardach explains as a phenomenon at the medium level of abstraction. To transfer a so-called mechanism or "smart practice" from the source side to the target side one has always to consider the surroundings. A surrounding can be anything in an institutional, political, economic or inter-personal context. Summarizing "smart practice" is a more flexible and general approach to implement a case, which has been identified in the source side and afterwards has been implemented on the target side. The implementation itself should not be seen as enforcement of foreign practices but to adapt the identified practice to the circumstances of the target side [55, 56].

5.1.3 Comparison between the quantitative microeconomic and study-based qualitative BPR

The biggest difference between the two discussed BPR methods is that the quantitative methodology is based on statistical data analysis and the qualitative methodology is a form of case study. The main advantage of the quantitative approach is its accuracy and replicability. On the other hand the main advantage of the qualitative approach is in fact the qualitative aspects and extrapolation. Table 5.2 summarizes the biggest differences between the two discussed approaches:

BPR method	Key emphasis	Methodology	Theory	Key authors
"Best practice"	Exemplar identification	Mostly quantitative	Production function	S. Bretschneider [21]
"Smart practice" ("good practice")	Extrapolation of target side	Mostly qualitative	Mechanism	E. Bardach [55, 56]

Table 5.2: Comparison of the two mentioned BPR methodologies (adapted from [22])

As the advantages for both BPR methodologies have been stated also their limitations need to be written down.

Limitations of S. Bretschneiders quantitative approach:

1. Focus lies on identifying a best practice example rather than trying to extract the practice from the source side and applying it in a different context on the target side.

2. It is not always possible to assess output in units of production, as the theory behind the production function assumes (e.g. assess qualitative parameters which can not be quantified).

3. Probably not all examples gathered through quantitative analysis are comparable.

Limitations of E. Bardachs qualitative approach:

1. There is no description nor an instruction how to look for and select "smart practice" examples.
2. There is no exact way of conducting "smart practice" analysis.

The approach used in this thesis to define "best practice" is the concept of E. Bardach. There are multiple reasons why this approach fits better than the quantitative one of S. Bretschneider. The first reason is that it is almost impossible to execute a quantitative approach, due to the fact one can never be 100% sure that all possible solutions are considered. In regard to video identification tools, the same problem occurs. Analysing all possible tools is not possible. In times of emerging technologies one can never be certain, that on the next day not already a new, but also a better tool for identification exists. Secondly, the limitation regarding the "smart practice" analysis has been abrogated because E. Ongaro developed a protocol how to do the analysis [60]. Therefore, this thesis is focusing on a qualitative approach as it has been described by E. Bardach [55, 56]. Focusing on a qualitative approach also implies to search for "smart practice" and not "best practice".

5.2 Extrapolation protocol for smart practice

As the method from E. Bardach does not tell the reader how to look and select exemplars for "smart practice" [22], E. Ongaro has developed a protocol on how to extrapolate "best practices". It is an extension of E. Bardachs "smart practice analysis" and is defined as follows [60]:

1. Identify the function to be performed
2. Define what exactly the practice is about
3. Describe the practice by answering the following questions:
    - How does the system operate?
    - How does the practice try to take advantage of the way the system operates?
4. Identify all the effects of the practice
    - Main effects of the practice (results)
    - Variations of the practice
    - Possible side effects

5. Define the key "process context factors" under what conditions the practice works

   - The causal mechanisms that have made it possible for the practice to work in that specific context must be identified

Figure 5.1 is an illustrative example of practices from a selection process for a video identification tool which fulfils customer specific criteria. The functions are sub-processes that need to be executed to achieve the overall process goal. According to the extrapolation protocol, the first step is about the identification of functions which need to be performed in order for the process to take place. The overall process is to choose a video identification tool. The functions to choose the right video identification tool are influenced from so called software selection factors. These factors are split into technical and non-technical factors and both need to be considered to choose the right tool. Technical factors focus on the practical aspect and capability of the tool to deliver the desired results. Whereas non-technical factors focus on the non-practical aspect of the tool. Both factors need to be considered equally. Common technical factors are functionality, efficiency or reliability. Non-technical factors focus more on cost, price or the return of investment [61].
The first function (F1) is about creating the criteria catalogue. The criteria catalogue includes all kinds of criteria, which specific video identification tools may fulfil or not. The catalogue includes mandatory criteria, which have to be fulfilled by video identification tools, for example to be KYC compliant. Without the mandatory criteria being fulfilled, a video identification tool can not enter any market. A certain basis on criteria is required. The qualitative research on video identification tool criteria function (F1.1) derives from the creating criteria catalogue function (F1). One uncertainty of the qualitative approach is that it can occur that an essential criteria may have been missed out, since the qualitative approach does not guarantee that all possible criteria of the investigated video identification tools have been identified. The identified criteria get categorized. This step should help the user to define their needs and therefore the criteria for a video identification tool (F2). In the last process step, the user contrasts the needed criteria for their business with the video identification tools and its fulfilled criteria (F3). The tool with the highest consensus regarding the criteria is the user's best choice.

5.3 Summary of the extrapolation

Table 5.3 shows the extrapolated practices from the selection of video identification tools process, which is illustrated in Figure 5.1. The columns represent the five main steps of the extrapolation protocol. The rows represent the functions, which have been defined in Section 5.2. Summarized, every cell in the table contributes to explain and answer one of Ongaros main steps in regard to every function. First of all, each practice must be linked to the function it performs (column 1). The practice is, generally speaking, a mechanism, which makes the function work. In the second step the content of the practice is described (column 2). How the practice is working must be described (column 3), by answering the two questions stated in Section 5.2. The effect or in other words the

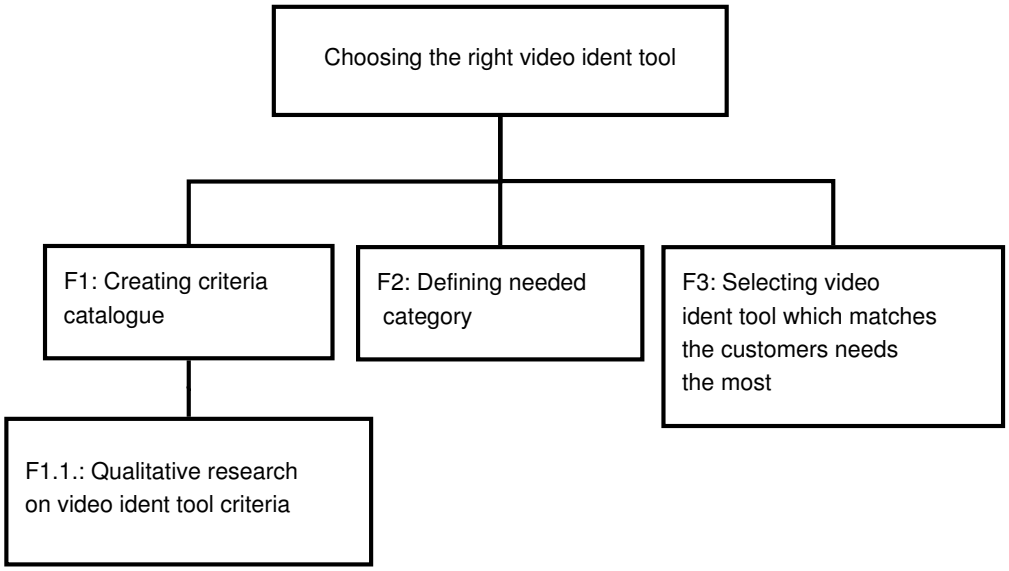

Figure 5.1: Functions on choosing the right video identification tool

result of the practice (column 4) is the way how the outcome of executing the practice allows performing the function. The context factors (column 5) provide a domain, where the practice is applicable.

The methodology for selecting criteria from different video identification providers is based on the framework for evaluation and selection of software packages according to Anil S. Jadhav and Rajendra M. Sonar [62]. This methodology is a guideline and can be adapted to the needs of an organization:

1. Requirement definition
   The first step in the framework is about the identification of functional and non functional requirements of the software.
2. Preliminary investigation of availability of software packages
   In the second step the availability of the software packages, including functionalities and features will be examined.
3. Short listing packages
   All packages, which do not provide the necessary functionalities and features are eliminated. Criteria examples for eliminating packages can rely on hardware, operating system, vendor or price.
4. Establishing criteria for evaluation
   Criteria are identified to evaluate the software packages. The identified criteria are arranged in a hierarchical tree structure. Every branch of the tree results in measurable and well defined criteria.

5. Evaluating software packages
   In the fifth step weights are assigned to each criteria. For all criteria in the hierarchy tree a rating is assigned and an aggregated score for each software package is calculated.

6. Selecting software packages
   In the last step the software packages are ranked in order of their score. The score gives an overview, which software package is better. But the decision for selecting a software packages is always human dependable. There can be a tradeoff between certain attributes like price or performance, which may affect the selection of the software package.

5.4 Video identification criteria

The upcoming subsections describe each criteria which may help to select a video identification tool in detail. The criteria come from qualitative research according to E. Bardach as described in Section 5.3 (F1.1). The selection criteria for the providers and the video identification providers themselves, can be found in Subsection 5.4.1.

5.4.1 Video identification providers

The qualitative research to define the criteria for the best practice catalogue starts with looking up providers with a between-study literature analysis [63, p.5]. With the help of existing providers, the criteria for video identification tools can be extracted. The research is focusing on video identification providers which do business in Europe. The mentioned providers according to Table 5.4 are screened and analysed in respect of their features. Afterwards the features of all providers and additionally the criteria mentioned on the providers homepages are compared to each other. On basis of the features provided by the analysed tools, the criteria are derived with the approach of E. Ongaro [60]. The list of mentioned providers is not complete as a quantitative research is not realisable within this thesis. This issue has already been described in more detail in Subsection 5.1.3. The search is also limited to video identification providers who are compliant to European legislation in regards of electronic identification and anti money laundering. Criteria for selecting the mentioned providers are:

- Established companies with at least three years of experience
- Providers which are compliant to European regulations and directives
- The minimum services which have to be provided are identity verification, document verification, electronic signature and video identification

It is difficult to provide quantitative data in regards of the customer base or how many identifications the selected providers conduct on a regular basis. On their homepages

Function	Practice	Description	Effects	Key Process Context Factors
F1.1	Creating a criteria catalogue by going through well-established providers of video ident tools	1. Looking up ident tools for screening purposes 2. By extracting criteria of the ident tools, which seem to be superior or mandatory	1. Qualitative research is initiated 2. Talking to banks or video ident providers directly may further help to identify criteria 3. Not all mandatory criteria can be identified	Nature of qualitative research
F2	Defining categories for the criteria of video ident tools	1.Every criteria needs to be linked to one category 2. By defining categories the user becomes a better overview of criteria, which share the same topic	1. Categorization of video ident criteria 2. Categories may help to get a better overview of defined criteria 3. Some criteria probably can be linked to more than one category	Categorization for all criteria must be possible
F3	Selecting video ident tool with highest consensus between the users needs and the fulfilled criteria	1. Compare criteria with needs of the user 2. By selecting only the tools which really are in the users perspective useful	1. Smartest selection regarding video ident tool from user perspective 2. User may be able to select multiple tools with identical criteria 3. User choosing not the smartest option because of not being aware of other criteria	The user has to know their preferred criteria

Table 5.3: Extrapolation of best practices according to E. Ongaro [60]

providers show off which institutions are using their services but pricing information is limited and identification turnover a secret. White papers of the providers themselves are first of all looked up on the web, with the mentioned criteria. But the three defined criteria are not enough to limit the search to a meaningful number for a qualitative analysis. Therefore two additional criteria for the qualitative research are introduced. One

criteria is used for the amount of case studies published by a provider. The second one represents the amount of so called testimonials. In other words, references of customers who are using the providers identification solutions.

Provider	Country	Founded	Case Studies	References
IDnow [15]	Germany	2014	9	21
Mark ID [64]	Lithuania	2018	5	7
Shufti Pro [65]	Sweden	2017	6	17
SwiftDil [66]	United Kingdom	2016	6	2
Global RADAR [67]	United States	2007	2	n.a.
acuant [68]	United States	1999	5	4
Electronic Identification [69]	Spain	2013	22	n.a.
Signicat [35]	Norway	2007	3	14

Table 5.4: Summary of video identification providers

The below chosen criteria result not only from research, but also from observations in Chapter 4, as well as from the subsequently conducted interviews with experts.

5.4.2 Conditions for video-based identification in Austria

The first criterion tackles the conditions, which must be fulfilled for video-based identification. In Austria, the FMA [41] is responsible that the conditions are fulfilled by the entities which apply video identification. The following conditions are in accordance with the KYC regulations [70]:

- The entity doing the video identification must take screenshots of the potential customer itself and from the official photo ID.
- During the identification process, the potential customer must tilt the official photo ID in front of the camera to allow the onboarding employee of the entity to check the holographic security features.
- The onboarding employee must check the serial number of the presented official photo ID and furthermore, has to make sure that it has not been tampered.
- The video identification has to be executed in a dedicated room, which is equipped with an access control system.
- The identification process should be terminated if a verification of the potential customer or the official photo ID is not possible. Furthermore, the process should be terminated if other uncertainties occur.

[41] Financial Market Supervision in Austria

The conditions how the video-based identification has to be executed differ from country to country. The legal acts about KYC and AML provide a framework under which the KYC onboarding and subsequently the video identification have to be performed. However, national governments may define additional conditions, which have to be fulfilled.

5.4.3 Country support

Since the regulation about electronic identification became effective on the 1st of July in 2016 [10], more and more video identification tools came on the market. A video identification tool can naturally only be used in those countries, where it is in accordance with the national guidelines as well as the ones set by European Union. As already mentioned in Subsection 5.4.2, Austria has certain guidelines, which have to be fulfilled before executing the video identification process. Such criteria can occur in other member states of the European Union as well. Nevertheless, an analysis of other national guidelines besides Austria has not been conducted due to the limitations of this thesis.

5.4.4 Document support

The difficulty of video identification tools is that they need to support many different document types at once since every country has its own measures to make identification documents tamper-proof. There is a strong link between country and document support but also to the language support criteria. Two evidence of identity documents which are standardised in the whole European Union are the government issued card [42] and the passport. Therefore, these two identification documents are easy to use for video identification purposes in the whole European Union. However, video identity solution providers also tend to integrate country specific identification documents. For example in Austria, the driver license is also a valid and official photo ID and can be used for identification purposes. The more documents a video identification tool provides the bigger is the potential customer base.

5.4.5 Language support

As video identification is a sensitive process, tools should support every language where the provider is active. Misunderstandings due to not supporting a language for customers in a certain country can cost time and money. It should also be seen as a service from the provider to the customer to offer multiple language options. The user experience is much better if the customer is familiar with the supported language. The language support criterion focuses on the language of the video ident tool presented in the tool, more specific in the GUI [43].

[42] German translation: "Personalausweis"
[43] Graphical User Interface

5.4.6 Call agent support

Furthermore, not only the identification software has to support different countries, document types and languages but also the call agents have to be able to work with multiple document types from different countries and be able to guide the user through the identification process in different languages. As long as automatic electronic identity, as mentioned in Subsection 3.2.2, is not supported within the AML directive the video identification has to be conducted by call agents.

5.4.7 KYC compliant

Every provider of video identification tools who wants to do business in the European Union has to be compliant to the given laws and the KYC regulation builds the legal basis. To be able to identify and verify customers, service providers must be recognised as trusted service partners. A trusted service partner is able to issue a qualified electronic signature and this signature again is in some countries equivalent to the handwritten signature. Electronic IDs and signatures are the key to adopt new services, which lead to economic and social development [10]. To sum up one can say the KYC regulation is aiming for an adequate level of security of electronic identification and trusted services.

- Electronic identification
  - Mutual recognition
  - Eligibility for notification of electronic identification schemes
  - Assurance levels of electronic identification schemes
  - Notification
  - Security breach
  - Liability
  - Cooperation and interoperability
- Trust services
  - General provisions
  - Supervision
  - Qualified trust services
  - Electronic signatures
  - Electronic seals
  - Electronic time stamps
  - Electronic registered delivery services
  - Website authentication
- Legal effects of electronic documents

5.4.8 API support

Video identification tools may also have solutions for already existing customer-specific applications. With the help of APIs, customers can integrate the functions of video identification tools in their own applications. This carries the advantage that customer applications can interact independently with ID verification platforms. Moreover, customers, with the help of APIs of such ident tools, can create an individual identification process.

5.4.9 Sandbox support

A sandbox support is important for everyone who uses a video identification API of a provider. With the help of a sandbox the customer can test the capabilities of the API first. Furthermore, the sandbox functions as a test and development environment. This is an important feature for developers who integrate certain features of video identification tools into to their own customer application. One disadvantage of ident tools, which support many countries or regions, is that the test samples in the sandbox may not be representative enough.

5.4.10 GDPR conform

The identification of natural persons is delicate in regards of the storage of user specific data. Every video ident tool has to be aware of data residency laws in all countries it is doing business. A data residency law regulates how personal information is stored and processed in a certain region or state. In the European Union, GDPR [44] is regulating how to deal with personal data. According to the GDPR regulation of the European Union [71], personal data is defined as any information relating to an identified or identifiable natural person.

5.4.11 Database usage for KYC checks

KYC checks are necessary for people in political positions and for businesses to be identified. Video identification providers have to request this data from official governmental institutions. For Austrian businesses, it is the Austrian Company Register. This register provides all the necessary data regarding the identification of businesses.
What applies to businesses also applies to PEPs [45]. A PEP has to be identified in the onboarding process. But the standard attributes for video identification do not imply whether someone is a PEP or not. Unfortunately, no standardised EU wide database for PEPs exist. As a result, every country has it's own database providing the information if a natural person works in a public function or has big influence in politics. Relatives of that kind of natural person also count as PEPs in Austria.

[44] General Data Protection Regulation
[45] Political Exposed Person

5.4.12 Data storage

Another criterion which should not be neglected is the question about where the processed data of conducted video identifications is stored. Financial institutions can use a build in version of a video identification tool, what may imply that the data is stored inside the organisation. But if a financial institution is using video identification as a service it is necessary to know where the processed data is stored. Data storage has again something to do with the GDPR regulation, as well with how customers of a bank perceive the trustworthiness of the institution when it saves personal data in other countries.

5.4.13 Cost effectiveness

Depending on how many video identifications take place in a financial institutions, vendors of video identification tools have different remuneration models. They may charge per video identification, time spent for a identification, flat rate, etc. Furthermore, should a second or third level support be needed, then the price would increase as well. If a financial institution is using video identification as a service from a third-party supplier also the priority of the request may lead to a price increase. Therefore, a financial institution needs to calculate precisely if it makes sense to forward requests for identification to third-parties or to invest in an in-house solution.

5.4.14 Platform dependency

Certain video identification vendors provide platform independent identification solutions. On the one hand, that means a user can identify themselves on a computer, laptop or smart phone (device independent). On the other hand, the identification can take place independently of the operating system of the device.

5.5 Categorization of the criteria

To get a better overview of the defined criteria from Section 5.4, additional categories will be defined. The categories reflect the respective underlying characteristics of the criteria. More precisely, every category deals with a certain aspect of the criteria.
The category "general" is focusing on criteria that have a universal understanding. Criteria linked to this category deal with more abstract features that video identification tools can provide. The category "legal" comprises criteria which are linked to any law, regulation or directive topics. Lastly, the category "technical" is used to group criteria which are linked to all technological aspects. The categories for each criteria can be found in Table 5.5.

5.6 Summary criteria catalogue

Table 5.5 gives an overview of all the video identification criteria provided in this thesis. The additional information (columns) necessity and category are added in the table to

categorize every criteria. The table differentiates between criteria which are mandatory because they have to be fulfilled and criteria which are optional. Without the mandatory criteria a specific video identification tool would not be able to operate in Austria or other EU member states. The categories are divided into three different areas legal, general and technical. All legal criteria are mandatory, to be compliant to given law. The general and technical criteria are mostly optional.

Criteria	**Necessity**	**Category**
Conditions for video based identification in Austria	mandatory	general
Country support	mandatory	legal
Document support	mandatory	legal
Language support	mandatory	legal
Call agent support	optional	general
KYC compliant	mandatory	legal
API support	optional	technical
Sandbox support	optional	technical
GDPR conform	mandatory	legal
Database usage for KYC checks	mandatory	legal
Data storage	optional	legal, technical
Cost effectiveness	optional	general
Platform dependency	optional	general

Table 5.5: Summary of criteria for video identification tools

Having presented the defined best practice criteria catalogue, it can be applied on a video identification tool. The next chapter functions as a countercheck for the best practice criteria catalogue.

CHAPTER 6

Applying criteria catalogue

In this chapter the defined best practice criteria catalogue will be applied on one chosen video identification tool. The chapter serves as a countercheck and supports the validation, to show that the best practice criteria catalogue can be applied in practice. The tool, which is used to apply the criteria catalogue on, is IDnow [15]. IDnow has been chosen, because out of the seven analysed banks, six are using video identification tools and IDnow is the most used tool among them.

- **Conditions for video based identification in Austria**
  IDnow is conducting video identification through its own call center or is giving financial institutions the opportunity to do the video identification themselves. Call agents are trained in the way to conduct video identification and therefore must be aware of the conditions and parameters stated by the FMA. This criterion can not directly be fulfilled by the video identification tool itself, but by the call agent. It can only be assumed that the FMA is auditing call centers and if they fulfil the specific conditions to conduct a video identification or not.

- **Country support**
  IDnow is supported in 195 countries and supports all countries of the European Union. According to the homepage of IDnow, they are constantly adding new countries. This criteria is for sure fulfilled in the European Union and furthermore in Austria.

- **Document support**
  IDnow supports passports, identity cards, residence permits and driving licences according to the ICAO [46] standard. The document types are linked to the 195 countries.

[46] International Civil Aviation Organization

- **Language support**
  The video identification software of IDnow supports the languages English, German, French, Spanish and Portuguese. They offer more languages in their SaaS [47] model (30 languages in total). If further language support is needed, IDnow will also introduce new languages on customers request.

- **Call agent support**
  IDnow provides a call center service or the software can also be used as a service, for in-house solutions. In the second case IDnow coaches employees of financial institutions on how to use the tool.

- **KYC compliant**
  The identification software is certified by TüV IT and EY and is compliant to the latest European directives and regulations with regard to KYC and AML. Additionally it is used by several European banks, which have to validate that the tool is compliant to respective laws. Otherwise these financial institutions would make themselves culpable.

- **API support**
  IDnow is offering its own API to integrate video identification functions into already existing onboarding processes of financial institutions. The interfaces of IDnow can be used through web services or native apps.

- **Sandbox support**
  Even though an API support is available, there is no sandbox support. IDnow offers an API and SDK documentation. Additionally they provide a real time operational status of the systems.

- **GDPR conform**
  The overall communication through IDnow is encrypted and the data centres are located in the European Union. The customer data is stored at servers located in Germany. Gathering, storing and processing user data is one thing, but the GDPR regulation further protects the fundamental rights and freedom of natural persons. Especially the users right to the protection of personal data is covered. Therefore IDnow must fulfil a users right to erasure their specific data or inform users about which personal data are stored, if requested. The software must be compliant to the GDPR regulation, otherwise it can not be used in the European Union.

- **Database usage for KYC checks**
  IDnow uses global sanction- and PEP lists to screen customers. Additionally a negative media check can be conducted.

- **Data storage**
  As already mentioned in criterion GDPR conform, all servers and data centres are located in the European Union. IDnow is a German company.

[47] Software as a Service

- **Cost effectiveness**
  IDnow does not publish any pricing details about their identification solutions. Therefore this criterion can not be analysed in more detail. In this industry it is more or less usual to offer a fixed price per video identification or a flat rate for a defined amount of identifications per month.

- **Platform dependency**
  The tool is available as SaaS, web service, iOS or Android app. This means there are almost no limits in regards of devices, where the video identification can not take place. The customer can use a computer with a webcam, smart phone or tablet. In addition an internet connection must be established. Lastly a mobile phone is needed to receive a SMS [48]. Only with the ID code stated in the SMS, the video identification can be triggered.

Criteria	**Fulfilled**
Conditions for video based identification in Austria	yes
Country support	yes
Document support	yes
Language support	yes
Call agent support	yes
KYC compliant	yes
API support	yes
Sandbox support	no
GDPR conform	yes
Database usage for KYC checks	yes
Data storage	yes
Cost effectiveness	n.a.
Platform dependency	yes

Table 6.1: Applying the best practice catalogue on IDnow

As shown in Table 6.1, IDnow fulfils all mandatory criteria. In addition almost all optional criteria are fulfilled as well. Only a sandbox is not support. The criterion cost effectiveness can not be evaluated, because IDnow is not publishing any price information. IDnow can therefore be used in financial institutions, which are doing business in the European Union. IDnow has a big assortment of identification methods. Furthermore it has a good country-, document- and language coverage. The provided information for the best practice criteria catalogue comes from published white papers by IDnow and from their own homepage [15], as scientific elaborations regarding IDnow have not been satisfactory.

[48] Short Message Service

After applying the defined best practice criteria catalogue, the semi-structured interviews can be presented. The interviews are used for validating the criteria catalogue. The next chapter gives an overview about the interview guide, the participants, the conduct and the thematic analysis of the interviews.

CHAPTER 7

Expert Interviews

To perform the analysis and validation of the defined criteria catalogue from Chapter 5, semi-structured interviews according to M.Saunders, P.Lewis and A.Thornhill [72] are conducted. This chapter gives an overview of why this type of interview is used for the expert interviews and what the challenges are.

7.1 Semi-structured interview

Semi-structured interviews usually have a list of themes and questions, which will be covered during the interview. In general, the interviewer can adapt the interview guide during the interview. In addition, the order of questions can differ from interview to interview, depending on the flow of the conversation. Thus, the interview guide in a semi-structured interview does not need to be followed in a rigid manner. The interviewer may as well add questions during the interview to go into more detail in certain areas. The data for semi-structured interviews usually will be audio-recorded due to the agile execution of the interview [72, p.320].
Because the expert interviews will be conducted on a one-to-one basis, such interviews are usually held as a "face to face" meeting between the interviewer and interviewee. As a result of the corona pandemic, such interviews may be held as virtual meetings more often. Interviews can be conducted in a synchronous way, for example video-chat programs, or in an asynchronous way, for example by e-mail [72, p.321].
In general, interviews are used to gather information. Semi-structured interviews can be used in relation to an exploratory study, where the interviewer tries to understand what is happening and to seek new insights. In addition, interviews can be used in explanatory studies, where the interviewer is trying to understand the relation between variables. The upcoming four subsections give an in-depth analysis about why a non-standardised (qualitative) interview is used in this research.

7.1.1 The purpose of the research

For the interviewer it is necessary to understand why the participant of the interview has taken certain decisions. Furthermore, the interviewer wants to know the reason behind this decision. Therefore, a qualitative interview is necessary. A semi-structured interview provides the interviewer with the opportunity to investigate or probe given answers. Furthermore, it provides an interpretivist epistemology, which is used to understand the meaning of the provided answers of the interviewee [72, p.323]. With the help of a semi-structured interview interviewees may also describe ideas, which lead to discussions that would not have been considered by the interviewer. This adds significance and depth to the obtained data.

7.1.2 The significance of establishing personal contact

Managers are more likely to agree to interviews, rather than completing questionnaires or other written forms. If the interview topic is relevant for their current work this increases the managers attention even more [72, p.324]. A semi-structured interview gives them the opportunity to reflect events and topics without writing anything down. The interviewees can also receive feedback on how the data and which information will be used. Potential interviewees may also decline interview requests, which are conducted via questionnaires and other written forms because it can feel inappropriate to provide sensitive and confidential content to someone they have never met before. Furthermore, they may also not be aware of how the gathered data is used.

7.1.3 The nature of the data collection questions

Collecting data via an interview is the most advantageous approach in certain cases:

- a large number of questions has to be answered
- the questions are complex or open-ended
- the order and logic of questioning may vary

A semi-structured interview is preferable if the second and third item are fulfilled [72, p.324]. As the second and third item apply in this thesis, the semi-structured interview method has been chosen for the data collection. As an alternative, also in-depth interviews are possible.

7.1.4 Length of time required and completeness of the process

An advantage of semi-structured interviews over questionnaires is that interviewees tend to invest more of their time to do an interview rather than filling out a questionnaire [72, p.325]. The aim of the interview is to obtain as much data as possible and to use this data to answer the asked questions. An interviewee may also decline to answer a

question, therefore it is important for the interviewer to ask why an answer can not be provided. On the other hand, in a questionnaire the answer why something has not been answered will be lost.

7.2 Semi-structured interview guide

Section 7.1 of the expert interviews chapter has given an overview of why a semi-structured interview is used to obtain data regarding the best practice criteria catalogue. This section deals with what questions will be asked, how the interview will be structured and how the interview will be executed. The semi-structured interview guide can be found in the appendix of this thesis A.
The approach how and what type of questions are asked in a semi-structured interview is of great importance. The right questions help to get the information needed and also help to lead the interview. There are three types of questions to differentiate [72, p.337]:

- **Open questions**
  With the help of open questions, an interviewee can provide a detailed and lengthy answer, which can be used to obtain facts or reveal attitudes.
- **Probing questions**
  These type of questions are usually worded like open questions but have a specific focus or direction. They are used by the interviewer to get a better understanding of the interviewees answer. Probing questions are used to reflect answers or in case an open question does not lead to an answer it is a way of rephrasing the original question.
- **Specific and closed questions**
  The use of specific and closed questions is similar to the ones of a structured interview. Generally, they can be used to confirm a fact or opinion.

7.3 Conducting the interviews

As already mentioned in the introduction of Chapter 7, the interviews are conducted in a semi-structured way [72]. The interviews take place face-to-face and will be transcribed afterwards. The analysis of the interviews takes place as a thematic analysis [73].

7.3.1 Aim of the interviews

The interviews aim to clarify if the provided criteria catalogue is able to provide bank employees with guidance to make a decision for or against a specific video identification tool. With the insights of the interviews flaws and enhancements can be revealed. Additionally the interviews validate if all mentioned criteria for video identification tools make sense and if mandatory criteria are missing. The interviews provide insights on how important onboarding is according to experts.

7.3.2 Interview partner overview

The interview participants are employees from financial institutions, more specifically from two Austrian banks. As the interviews are declared as expert interviews, the requirements the interviewees have to fulfil include the following:

1. A minimum working experience in a financial institution of 10 years
2. Working in a customer onboarding related department
3. Possession of know how in legal topics such as AML and KYC
4. Working in a management position (at least department head)

Alias	Position	Experience [years]	Department
Alpha	Department Head	> 20	Customer Data Management
Beta	Department Head	> 12	Customer Data Services
Gamma	Department Head	> 20	Mid Office Corporate Customers

Table 7.1: Overview of interview participants

The first interview partner "Alpha" is department head of Customer Data Management. The interviewee has more than 20 years of experience in the financial sector and has a lot of know how in the IT architecture environment of the bank. "Alpha's" know-how regarding AML and KYC comes from practical experience over the course of several years dealing with onboarding relevant topics. "Beta" is department head of Customer Data Services, has worked in several Austrian banks for more than 12 years and is a certified AML/Compliance officer. Lastly, the third interview partner "Gamma" is department head of the Corporate Customers Mid-Office, with a working experience of at least 20 years. Furthermore, interviewee "Gamma" was involved in implementing a video identification tool and gained the necessary legal know-how through working in the onboarding department for several years.

7.3.3 Recording interview data

Creating a complete record of an interview as soon as possible after it has been conducted helps to prevent bias and is more useful for analysis purposes [72, p.339]. For the interviewer, it is important what the interviewee is saying and also how they say it. Recording an interview helps the interviewer to focus more on what the interviewee is saying, and also what impressions they make. The recording can also be re-listened and it is accurate and unbiased. Lastly, it allows direct quotes and can permanently be used.

However, recording interviews also bears some disadvantages as it can affect the atmosphere of the interview. The interviewee may be inhibited by answering certain questions. A technical defect during the interview cannot be ruled out either. The necessity to write a transcript of the interview can also be considered a disadvantage.

To sum up, the interviews in this thesis will be audio recorded due to the mentioned advantages in the first paragraph of this section. In addition, it is important to mention that direct quotes of the interviews help to maintain a good reading flow.

7.4 Transcription of the interviews

Transcribing goes hand in hand with qualitative data collection. There are several different transcription methods, which can be used to convert speech to text:

- **Verbatim transcription**
  Every single word is written down, including pauses, expressions of the interviewees and gap fillers. This type of transcription is useful if the researcher is also interested in how an interviewee is saying something and not only what they say.
- **Intelligent verbatim transcription**
  In this method, every spoken word is again written down, but without the gap fillers. Furthermore, grammar mistakes and broken sentences can be corrected. With the help of intelligent verbatim transcription, the transcript is more readable. However, data about how the interviewee is saying something may be lost.
- **Edited transcription**
  Lastly, the edited transcription is a summary of the intelligent verbatim transcription. The summary only contains relevant paragraphs. Sentences, which are irrelevant with regard to meaning and output of the interview, are omitted.

For the purpose of this thesis, the intelligent verbatim transcription fits best. This method of converting speech to text is a central component to the reliability, validity and veracity of qualitative data collection [74]. With the help of a transcript, researcher get a better understanding of their data. On the other hand, intelligent verbatim transcription is costly with regard to time as well as physical and human resources. In addition, it is also prone to a range of human errors.

7.5 Thematic analysis of the interviews

For analysing the interview data, the thematic analysis approach from V. Braun and V. Clarke [73] is used. The thematic analysis is an analytical method used for analysing qualitative data. To be more precise, it is used for identifying, analysing and reporting patterns or so called themes in a data set. This method works both for reflecting reality,

as well as for clearing up reality. Before going into more detail regarding the thematic analysis, V. Braun and V. Clarke are highlighting three characteristics, which one has to be aware of before executing the analysis:

- Inductive vs theoretical (deductive) thematic analysis
- Semantic vs latent themes
- Essentialist/realist vs constructionist epistemology

Thematic analysis can be conducted within several different paradigms. For this thesis, a theoretical thematic analysis will be chosen. This type of analysis has the advantage that it is not focusing on the data overall but on a more detailed aspect of some of the data. This leads to the fact that coding through the data is done over a specific research question.
For identifying themes in the thematic analysis, a semantic approach is used. This approach has the advantage that the themes are identified explicitly within the data captured and nothing else. Other things the participant said that go beyond the scope of interview and which have not been captured in written form will not be analysed.
Lastly, the thematic analysis is conducted within essentialist/realist epistemology. It guides the researcher what they can say about their data. With the help of an essentialist/realist approach one can theorise motivations, experiences and meanings in a straight-forward way.
The thematic analysis is split into six steps (see Table 7.2). According to V. Braun and V. Clark these qualitative guideline steps are no fixed rules, but can be adapted in a flexible way to fit the research question and data. Furthermore, they mention that the analysis is not a linear process, but more a recursive one, in which it is possible to go back and forth.

7.5.1 Familiarising yourself with the data

Transcribing the conducted interviews is the first step and an excellent way to get to know the data. [73, p.16]. The initial ideas after reading through the transcripts once are:

Generalizing the positions and responsibilities of the interviewees

- Position: department head
- Responsibility: sales support, customer onboarding, customer data management, run the bank, new to the bank customers, reviewing of customers, product opening, account opening, loans, deposits, cash management, compliance

Phase	Description of the process
1. Familiarising yourself with the data	Transcribing of data, reading and re-reading the data, noting down initial ideas
2. Generating initial codes	Coding interesting features of the data in a systematic fashion across the entire data set, collecting data relevant to each code
3. Searching for themes	Collecting codes into potential themes, gathering all data relevant to each potential theme
4. Reviewing themes	Checking in the themes work in relation to the coded extracts and the entire data set, generating a thematic map of the analysis
5. Defining and naming themes	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells; generating clear definitions and names for each theme
6. Producing the report	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis

Table 7.2: Phases of thematic analysis (adapted from [73])

Importance of onboarding

- One of the most important processes in the whole bank
- First touchpoint with the customer
- Customer experience especially important in the onboarding process
- Banks are obliged to identify natural persons in person. For example directors, authorized signatories, people who transfer money of business accounts
- Onboarding is like a bottleneck. Everyone has to go through this process
- Many iterations, depending on the risk level of the potential customer
- The longer the onboarding process takes, the longer the customer has to wait for their requested service or product

Importance of video identification

- In times of Covid-19 and home office importance increased significantly
- Physical identification often not achievable

- You do not have to fly to the customer and the other way around, it is practical
- Very useful for offshore customers, because a relationship manager is usually not traveling there
- Everything is documented. The used legitimation document, the picture of the customer, time, call agent

Video identification outsourcing/in-house

- Outsourcing was an idea but has been discarded, because customers are not private individuals but corporations
- Call center does not distinguish between a CEO, director or CFO of a corporation and a private individual
- In-house solution is faster for the potential customer
- Software of external provider is used
- Customer is not forwarded to a call center for the identification process but the call agents are employees of the bank
- If you outsource the process you have to deal with third-party suppliers and data storage
- In-house solution is providing a better customer experience, is faster and customer oriented
- Not outsourced because the video identification is a service of the bank
- Employees in the bank cover more languages
- Call center are impersonal
- Video identification has been outsourced in the retail business, because it is a lot of effort
- Binds a lot of resources (argument why it has been outsourced)
- The bank can outsource the process of video identification, but it will always be responsible if the natural person has been identified correctly or not

Bank products associated with video identification

- For every product relevant
- Account opening
- Video identification will be used for corporate customers and their authorized representatives or authorised signatories
- Video identification is independent from any product. The employees of a corporation which use certain services of the bank have to be personally identified (payroll accounting, people in authority for company payments, etc.)

Alternative to video identification

- As an employee of a bank you can meet the person which needs to be identified physically
- Use the services of qualified third parties like notary, lawyer or auditor
- Qualified third parties (of the European Economic Area) are not available in every country, e.g. Dubai
- With the new video identification regulation, it will be possible to use biometric data for identification purposes (face recognition, fingerprint)
- Passport copy and verification in person

Advantages of video identification and why it is used

- Saves money because you do not have to visit the customer only because of the identification
- Fast service which can be done anytime
- Service according to the customers wishes
- Identification can be shared with other financial institutions if the customer allows the bank to forward the identification data
- Audit proof system
- Customer does not have to show up in person (extremely important in the offshore area)
- Time and cost savings for the customer as well as for the bank
- Location independence

- Bridging time differences
- Works with smart phone, tablet or laptop. No further additional hardware is needed

How the right video identification tool for a bank has been selected

- 2-3 provider have been screened in detail
- Interviewee not directly involved in the search process of a video identification tool
- "Beauty contest" - several providers have been screened in detail

Criteria which played a role for the banks

- No start up, experience is needed
- Video identification tool which is also capable to handle biometric data
- Provider must be capable to train banking employees how to use their tool
- Tool must be supported in all countries the bank is doing business
- Country coverage
- Call center availability
- Costs per video identification
- Is the provider able to hold all their promises - PoC [49] successful?
- The tool has to support the integration into already existing internal processes of the bank
- Usability of the tool is important for the employees of the bank, as well as for the customers
- Stability of the system
- Easy access for the customer
- Compatibility of the tool
- Feature to start at the point of the process, where it has been cancelled
- Feature to reserve a time slot in the tool right away
- The tool has to be intelligent enough to understand if the picture is too bright, dark, blurry
- The tool should point out to the person which is getting identified, if the contrast is bad

[49] Proof of Concept

Provided criteria catalogue and its impact

- **"Condition for video based identification"**: is something that has to be fulfilled anyway; the tool which is used has to be flexible so it can be used in other jurisdictions besides in Austria; mandatory criteria as provided in the criteria catalogue; general statement all criteria where legal requirements have to be fulfilled must also be fulfilled by the video ident tool, otherwise it can not be used;

- **"Country support"**: the more countries are supported the better; you have to know which countries are supported and which are not; provider has to be flexible and be able to support countries, where the bank has not done business before;

- **"Document support"**: the more documents are supported the better; there is a limited number of documents available; the website PRADO [50] lists all of the EU approved legitimation documents; important; basis documents like passport should always be supported;

- **"Language support"**: is extremely important; the tool must support several languages but also symbols, e.g. Cyrillic, Nordic letters, etc.; app has to support the customers language; our employees support multiple languages, therefore the tool should support them as well; important because the user has to provide sensitive data;

- **"Call agent support"**: the call agent has to be able to speak multiple languages; the most important ones are English, German, Russian; problem with outsourcing is that call agents do not support as many languages as the employees of the bank; in-house call agents are customer-oriented; languages of core markets should be covered; call agent is always needed because in the banking sector a fully automated identification process is not compliant to given law;

- **"KYC compliant"**: better name for the criteria would be compliant with the law for electronic identification; of course mandatory, because if not fulfilled you can not use the video identification tool; legal requirement therefore must be fulfilled;

- **"API support"**: is important to automate processes, e.g. upload the documents automatically into the document management system; not mandatory, but has an impact on digitisation and automation; on the other hand mandatory for banks which need to integrate the identification process into internal process structures; API support has a strategic value because it affects the customer experience;

- **"Sandbox support"**: additional test environment of the complete system in-house; for testing and training purposes; not necessary but nice to have;

[50] Public Register of Authentic identity and travel Documents Online

- **"GDPR conform"**: is a basic requirement and has to be fulfilled; must have; GDPR violations are heavily punished; no brainer mandatory because of legal requirement;
- **"Database usage for KYC checks"**: no criteria for the bank, because it has its own sanction lists, fraud databases, etc.; the video ident tool checks if there has been a fraud attempt under the person's name which gets identified; should not be mandatory for video ident tools because this is a topic every compliance department in a bank has in its focus as well; sanction lists, PEP lists, whitelists or OFAC [51] lists; bank has to do all of these compliance checks anyway; bank relies more on internal provided information; every additional information is welcome; maybe the provided lists and checks of the video ident tool do not cover everything, but a bank has usually its own lists as well - the more lists the better the coverage is; banks need their own lists and checks because a natural person can also be identified in other ways but video identification;
- **"Data storage"**: no criteria; the video identification provider is not allowed to store any data; the bank is storing the data itself; should not be optional because you can not use a tool which stores data outside of the EU regarding GDPR; provider has to be transparent where the data is processed and stored;
- **"Cost effectiveness"**: the additional costs for the service are not being charged on to the customer; it is a service the bank is providing; fixed contract; is an important criteria; paying per video identification; bank is doing the video identification for other units as well - payment via SLA [52]; depending on how many video identifications take place; cheaper than flying to the customer or going to a notary;
- **"Platform dependency"**: video identification app only available for smart phone; no browser support on the computer anymore, because company firewalls often blocked the traffic and it was not broadly used on the computer; but everyone has a smart phone; regarding customer experience an important topic; should support smart phones and laptops; app should be as user-friendly as possible; very important because it supports the customer experience

Criteria which are missing in the catalogue

- If the video identification is outsourced a criteria is missing for call agents how they behave. Should be friendly, polite and respectful with the customer
- The process has to be tamper-proof
- Call agent office of third parties should have the highest security features in regards of conducting the video identification

[51] Office of Foreign Assets Control
[52] Service Level Agreement

- Be aware that the video ident tool is able to handle all kind of symbols, like Cyrillic, Nordic letters, etc.
- Provider has to be really flexible to add additional jurisdictions if needed from the bank
- Process has to be as automated as possible
- VIP service (telephone hotline)
- Convenience features are missing, e.g. booking system within the app, resume if interrupted, point out to users if the camera or microphone has a bad quality

Issues with the criteria catalogue

- Not every provider will cover all criteria
- The bank does not know how the third party call agents are trained
- Legal requirements are changing rather fast. If someone is relying on the criteria catalogue and is selecting a provider who can not adapt so fast to new requirements, you have to switch to another provider fast, which is not that easy
- Legal requirements are carved in stone. Provider can stand out if they integrate useful features, which lead to better customer experience

7.5.2 Generating initial codes

After familiarising with the data the production of codes from the data can be started. Codes identify a feature of the data, which seems to be interesting for the analyst. The codes should be in a basic and meaningful form so that it describes the phenomenon [73, p.18]. Table 7.3 summarizes the initial codes.

7.5.3 Searching for themes

After the data has been coded, the search for themes can start. A theme is an overarching topic which, can be linked to several codes [73, p.19]. A visual representation, like a mind map can help to sort different codes into themes.

Initial thematic map referred to Appendix A.1

7.5.4 Reviewing themes

In this phase, the generated themes from the third phase are reviewed and refined. Reviewing takes place on the code level and refining will take place on theme level in relation to the whole data set [73, p.20].

Developed thematic map referred to Appendix A.2

Data extract from	Code for
Generalizing positions and responsibilities	mid level management; end to end responsibility; sales; onboarding
Importance of onboarding	one of the most important processes; customer experience in focus; obligation by law to identify natural persons
Importance of video identification	increased dramatically during Covid-19 and home office; alternative to physical identification; cost-saving; process is documented
Video identification outsourcing/in-house	in-house solution faster for customer; external software used; outsourcing for retail customers but not corporations; better customer experience in-house; call agents of third parties not as trained and less language coverage; in-house solution demands a lot of resources; outsourced because it is too much effort
Bank products associated with video identification	not bound to a product; can be used for authorized representatives, authorised signatories, directors; in the retail business for account opening
Alternative to video identification	meet in person; use qualified third parties like notary, lawyer, auditor; biometric data (after the eIDAS regulation has been updated); difficult for customers outside the EEA
Advantages of video identification	saves money for the bank; time and location independent; audit proof; fast; works with smart phone; eID can be shared with other banks
Selection of video identification tool	POC [53] of 2-3 providers; not directly involved in selection process; possibility to train employees of the bank to use the tool
Used criteria for selection	experienced provider; country coverage; integrable in existing onboarding process; call center availability; usability/customer experience;
Provided criteria catalogue of thesis	all legal requirements have to be fulfilled otherwise tool can not be used; the more countries, documents and languages are supported the better; call agents critical for customer experience; banks use their own sanction lists and databases to screen natural persons; video identification mostly used on smart phone
Missing criteria in the catalogue	criteria for call agents sitting at third party provider; flexibility of the provider to add document types, countries, languages; high degree of automation; convenience features
Issues with the criteria catalogue	not all criteria will be covered by all providers; the bank does not know how well the call agents of the provider are trained; legal requirements are changing quickly, and therefore, the catalogue needs to be updated as well; legal requirements are given, therefore, providers can only distinguish from one another through user features

Table 7.3: Data extract, with codes applied (2. phase of thematic analysis)

7.5.5 Defining and naming themes

In the second to last step of the thematic analysis, the themes are refined once again. The simpler the themes are the easier it is to write the analysis [73, p.22]. In this process step, it can also be reconsidered if the themes should have sub-themes or not.

Final thematic map referred to Figure 7.1

7.5.6 Producing the report

Lastly, the analysis of the thematic map is made. The analysis is split into three parts. Each part represents one theme and the involved data extracts.

Onboarding

All three experts mentioned that the onboarding process is the first touchpoint with the customer and therefore, it is one of the most important processes in the bank. According to Gamma the onboarding process gives the customer already insights on how the employees of the bank are working and how reliable they are:

> „*This is the entry into the company. This is when he sees us for the first time, gets to know us for the first time and has the first feeling of how things are actually going, how things are not going.*“
> (Quote of interview with Gamma)

Furthermore, Alpha mentions that the onboarding process is so important, because everyone, who wants to do business with the bank, has to go through it. If the process is complicated and frustrating in the first place, the customer starts with a bad experience, which may affect future businesses with the bank:

> „*So, it is actually like a bottleneck where everyone has to go through and if this process is tedious, that is of course a potential moment of frustration for the customer.*“
> (Quote of interview with Alpha)

The onboarding process itself obligates banks to identify natural persons and therefore banks and other financial institutions must obey the law to be compliant:

> „*Because of course also from a regulatory point of view and on the basis of the FM GWG, we are obliged to identify persons personally.*“
> (Quote of interview with Beta)

For Gamma, the onboarding process is extremely customer experienced driven and therefore, they try to make the onboarding process as convenient for the potential customer as possible:

> „*There is always a person behind the company and that person's customer experience is just like yours or mine. So, when I sign up somewhere, usability is important. How am I guided through the process? How do I fulfil the first contact with the bank? [...] The onboarding process is extremely important.*“
> (Quote of interview with Gamma)

Video Identification

What makes video identification so attractive for banks and also customers is the independency from time and location. Furthermore, almost every common smart phone or laptop is capable of performing the video identification. Only a webcam, microphone and internet access are needed:

> „*One advantage is that it is location independent, i.e. I do not have to physically fetch the person or drive there to be able to carry it out. It can also be used to bridge time differences. So, if someone is in a different time zone, I can still do it [...] I can do it on a normal tablet, laptop or smart phone. Because these devices all have a camera and a microphone.*“
> (Quote of interview with Alpha)

All three experts see video identification as an alternative to classical personal identification where both parties meet physically. There are several ways to identify a natural person physically:

> „*You can meet the person yourself, see the person and look at the passport. You can use a qualified third party. That would be notaries, lawyers and auditors.*“
> (Quote of interview with Gamma)

In some areas video identification is the only alternative way to identify a potential customer, except of going there and meet physically. The problem is that not every country in the world has qualified third parties approved by the European Union:

> „*A lawyer in Dubai is not a qualified third party. In Austria for example, only lawyers, notaries and auditors from EEA are actually qualified third parties. [...] In some destinations, video identification is almost our only option instead of actually going there and looking at the passport and the person.*“
> (Quote of interview with Gamma)

For Alpha and Gamma the video identification is product-independent. The video identification is necessary for employees of corporations who interact with company accounts or do money transfers in the name of the corporation:

> „*Product use is independent of identification. We have classic banking services, such as company accounts. These accounts are used to process all company payments, including payroll. And the people who normally have access to these accounts are, for example employees in payroll accounting or in purchasing, who simply have to make transfers. And these people are identified so that they can use these services.*“
> (Quote of interview with Alpha)

On the other hand, Beta mentioned that the video identification is linked to the account opening, which is a standard product in retail banking. The owner of the bank account has to be identified:

> „*Definitely once for the account opening, other products I do not have in mind right now. [...] and there you also can have authorised signatories. You have to identify them out of KYC and out of money laundering.*“
> (Quote of interview with Beta)

By using video identification, the travel costs are basically zero. Especially for offshore customers this is a huge advantage. Beta and Gamma stated that the bank is saving a lot of travel costs and it is also more convenient for the customer:

> „*The client does not have to show up in person. That is very important in the offshore sector. The fact is that the client will certainly not book a flight to come here and be identified personally. That is also associated with costs. In other words, it is an easy way for the customer to get identified online.*“
> (Quote of interview with Beta)

Another advantage of video identification is that the tool logs all steps and the bank has a proof that the identification took place:

> „*It is a system. The identification is stored away, there is a file on it and there is an audio file on it. So, we can confirm that we have identified the customer. [...] With the video identification you have a proof, it is 100% audit proof and of course verifiable for the supervision.*“
> (Quote of interview with Gamma)

Outsourcing the video identification is not an option for Alpha and Gamma, because the customer experience would suffer. Furthermore, in this area usually CEOs, CFOs or directors have to be identified, not private individuals. In the corporate banking sector, bank employees support more languages and usually already know the person which needs to be identified:

> *„Our customers are neither private individuals nor retail customers, but large corporations. [...] We know these people in the sense that we really know that this is the CFO, CEO, director or whatever in this company. In most cases, we may have already spoken with them and we do not want to have them sitting there in a queue for 10 minutes, 20 minutes.“*
> (Quote of interview with Gamma)

In the retail area, according to Beta it is easier to outsource the video identification, because the requirements of call agents are not as high as in the corporate banking area and an in-house solution binds a lot of resources as well:

> *„But to be honest, I think I would have outsourced it. Simply because it is a lot of work. [...]it also ties up a lot of resources. The provider normally also has a call center and they handle it there.“*
> (Quote of interview with Beta)

All three experts agree that providing an in-house solution or using a video identification software in-house and handling all the operations within the bank implies a much better customer experience:

> *„No it is not outsourced for the reason of customer experience. [...] To offer the customer a service, so to speak. We have colleagues on site who speak several languages. We can also guide the customer through the process or arrange appointments with them personally.“*
> (Quote of interview with Beta)

Criteria catalogue

According to Alpha and Gamma, all necessary mandatory criteria for selecting a video identification tool are available. Beta challenged two criteria where the necessity should be switched. The first criteria "Database usage for KYC checks" can be optional, because usually banks have their own internal KYC checks and do not use the available databases from providers:

> *„I am now a little bit confused why it says mandatory. Because normally, the examples you gave are in the compliance department and there are existing lists that are checked against. There are sanction lists, there are PEP lists, there are whitelists, there are OFAC lists, etc. against which people are also matched.“*
> (Quote of interview with Beta)

Secondly, "Data storage" should be mandatory because it goes hand in hand with the GPDR regulation:

> „*So, when I look at a tool like that, from a criteria point of view, and I see that data is stored outside the EU, then I can't just say, yes, it fits, I do not care, but that is then a conflict with the GDPR directive. It would be a no-go de-facto. That is why it should be mandatory.*“
> (Quote of interview with Beta)

The catalogue misses a criteria which focuses on the degree of automation of the video identification tools, says Gamma:

> „*The process must have a degree of automation as high as possible, not a lot of typing. There are control loops, they have to be, they have to be manual. Everything else has to go through automatically.*“
> (Quote of interview with Gamma)

Beta and Gamma mentioned that the screening of natural persons (KYC checks) is usually done within the bank. The compliance department provides all necessary lists, databases and other information which is required. Therefore, the banks do not use external sources, databases or lists from video identification providers:

> „*As bank you are obliged to do much more than just a PEP check. You need advised media, you need PEP, you need wealth check, etc. This was not a criterion for us. We do the KYC checks ourselves.*“
> (Quote of interview with Gamma)

The legal environment regarding video identification is changing fast. Alpha mentioned that if someone is selecting a video identification tool with the help of the provided criteria catalogue, it may happen that the provider is not able to adapt to the new regulations and the bank has to look for another tool again. Provider changes are rather difficult, as they may have to be integrated in the complete process structure again:

> „*If you decide on a provider on the basis of the criteria catalogue and then relatively fast new requirements come along that are simply legally binding and the provider has a hard time complying with them, then in case of doubt, I might have to change the provider relatively quickly. And changing providers is always potentially difficult.*“
> (Quote of interview with Alpha)

Furthermore, the legal requirements have to be fulfilled anytime, otherwise the selected tool can not be used. However, since all legal requirements are mandatory, the different video identification providers and their tools mostly differentiate from one another in the features which come with the tools and how they influence the customer experience:

> *„So the catalogue of criteria per se, all the legal things, [...] there are just many aspects of what is allowed and what is not allowed [...] I always have to fulfil that. In addition, there are perhaps simply nice-to-have features that improve the customer experience. This also differentiates the providers a bit from each other.“*
> (Quote of interview with Alpha)

Although there are criteria for video identification providers, the criteria for third-party call agents are missing. Beta and Gamma have the need of a criterion in the catalogue for call agents, in case the video identification process is outsourced. Otherwise, they can not rely on the provider and risk that customer satisfaction is not met.

> *„Do I rely on a call centre where I do not know how the turnover of staff is [...] I don't know what the training looks like? I will only notice the issues if complaints pile up that something is not working as it should be.“*
> (Quote of interview with Beta)

7.5.7 Summary of the report

Alpha and Gamma approve the best practice criteria catalogue and for them it contains all mandatory criteria to provide guidance for or against a video identification tool. Beta challenged the necessity of two criteria, but overall approves the criteria mentioned in the catalogue. All three interview partners have ideas how to extend the best practice criteria catalogue with optional features. Table 8.1 shows the adapted best practice criteria catalogue with input provided by the interviewed experts.
Additional goals for introducing video identification tools according to the experts are on the one hand the financial aspects. Video identification pays off for corporate clients as the account managers save travel costs. In the retail area it saves money, because clients can get identified by third party providers and bank employees therefore are not involved in the bureaucracy tasks, which are time consuming. On the other hand the flexibility of the providers is important. They need to have the capacities and knowledge to implement additional requirements for financial institutions. Not every bank has the same product portfolio or country coverage and video identification providers should be able to adapt to their needs. Nice to have are so called convenience features. Convenience features such as a booking system in the app of the video identification tool or an interruption feature, which lets the user continue the video identification wherever it has been stopped or cancelled, help providers to stand out from competitors.

Within this chapter, the interviewees have been introduced, the interviews have been summarized and the results have been presented within a thematic map. The second to last Chapter 8 will provide a deeper analysis of the interviews and discuss the statements of the experts in more detail.

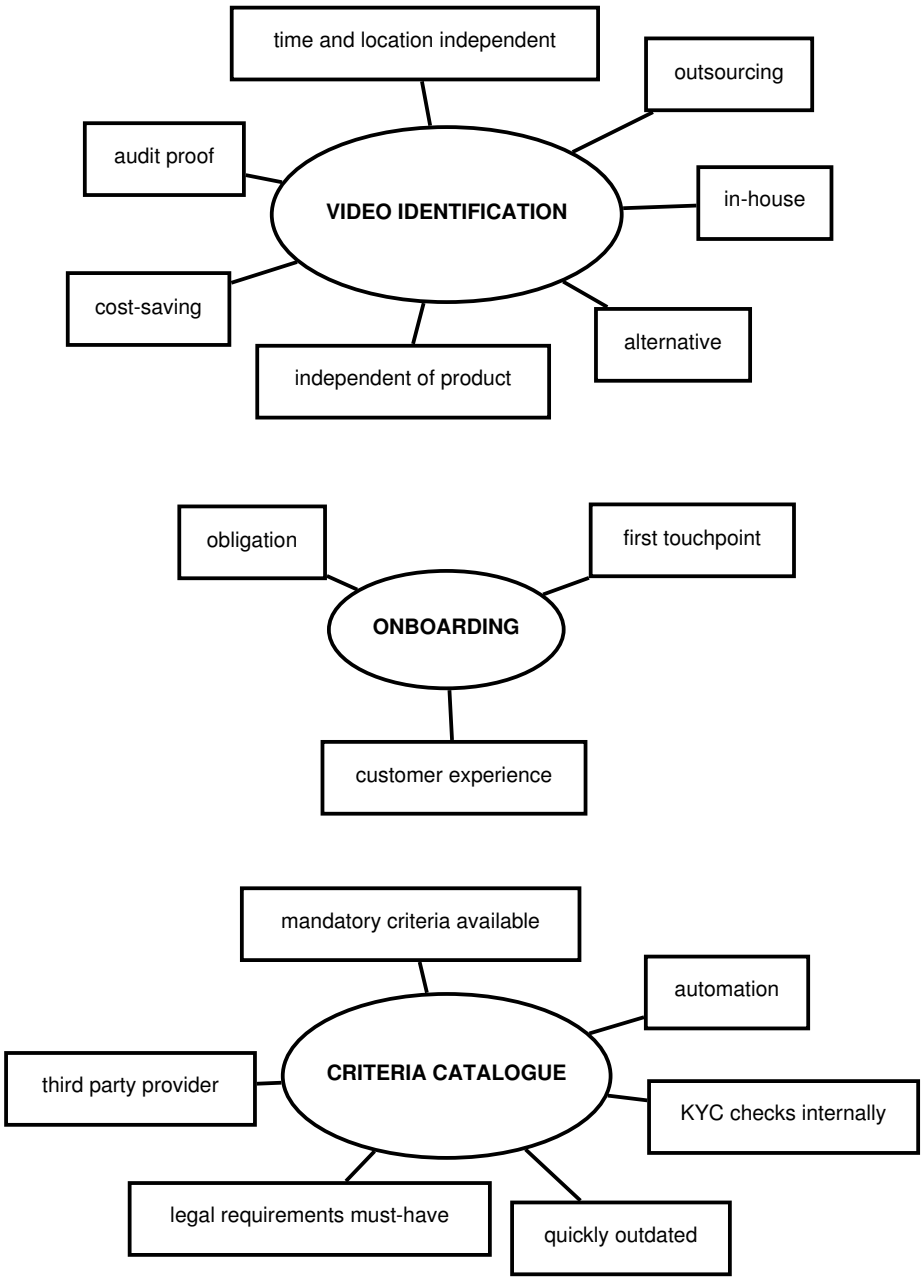

Figure 7.1: Final thematic map with three main themes

CHAPTER 8

Discussion of the results

In this chapter the result of the thesis are analysed in detail. In Section 8.1, a summary about the importance of onboarding and video identification is made. Subsequently, in Section 8.2 the experts opinion on the criteria catalogue are summarized. The third Section 8.3 provides a critical view on the concept of the video identification criteria catalogue.

8.1 Onboarding and video identification

The onboarding process is undisputedly one of the most important processes in any bank. All interviewed experts agree on that. The onboarding process is regulated in many ways and needs to be done by every new customer, whether it is a retail customer, corporation or financial institution. The technologies which support the onboarding process will be developed further and new technologies will arise and enter the market sooner or later. Therefore the regulation flow will certainly not decrease.

The expert interviews have shown that technologies concerning of video identification are the most used alternative to physical meetings. The providers of video identification tools do not stand still and already implemented features, which can be used, after the updated KYC/eIDAS regulation becomes effective. With the update, the processing of biometric data will come to the forth. This will have a huge impact on how video identification is done right now. It probably will make call agents obsolete, because fully automated video identification tools can then also be used in the financial sector. The call agents are a critical point in the decision process either to outsource the video identification or to integrate it into internal banking processes. If automated video identification takes over the onboarding process, this will also have a huge impact on customer experience. All experts mentioned because of customer experience they have integrated video identification in their systems and did not outsource it. At least for their corporate and financial institution customers.

Video identification will further go hand in hand with banking. The demand significantly increased since the outbreak of Covid-19. As a result of the outbreak, also the digital transformation increased rapidly. More and more customers appreciate the location and time independent service, as it makes banking easier and more comfortable. This implies that even after the corona pandemic customers will use video identification. Especially younger generations, which are digital natives and mostly use online banking on their mobile device, will request such digital services. However, not only customers profit from digital identification methods, but also the banks themselves do. With the help of video identification, relationship managers do not have to travel the world just to onboard a new customer. This saves a lot of travel costs, especially, when the bank is doing business around the globe. A fact which should not be neglected is the verifiability of the identification by the auditor.

8.2 Analysis of the criteria catalogue

The catalogue contains all necessary legal criteria in addition to some nice to have features. The legal requirements have to be fulfilled, it is a must. Thus video identification providers only distinguish themselves from one another in regard to user features or criteria which are marked as optional in the catalogue. As mentioned by one expert, it will be hard to find a provider who fulfils all criteria. However, the catalogue gives an overview of what essential criteria are. Every expert is of the opinion that the more countries, documents and languages are supported the better it is. Of higher importance, though, is that the video identification provider covers all the countries, documents and languages of the core markets, where the specific bank is doing business. In other words, this means the provider with the highest country, document and language coverage does not have to be the best choice for the bank, as it is not guaranteed that the bank's core markets are covered as well.

It was identified through the creation of the criteria catalogue and the expert interviews that call agents, regardless of whether it is a third-party provider or an employee of the bank itself, are critical for the customer experience. However, the criterion "Call agent support" does not elaborate on how the call agents are working and what additional characteristics they should have. They have to be able to work with different document types and speak multiple languages in the best case. But how they work and how they have been trained in regards of customer service and behaviour, or how solution-focused they are,was not mentioned in the criteria catalogue. Furthermore, the criteria catalogue does not cover how flexible video identification providers are with regard to adding new countries and documents in their software. This is important for banks because it can occur that a bank is starting to do business with a customer in a country they have never done business before. If a video identification tool is not yet providing the country and documents, then it must be capable of adding them in an agile way.

During the expert interviews it has been suggested that the "Database usage for KYC

checks" criterion does not have to be mandatory. The check itself is mandatory but the video identification tool does not have to provide this feature. Decisive for that argument is the fact that the checks of a natural person are closely supported by the compliance department. The banks have their own lists and databases for screening and matching individuals. These are very sensible data and banks usually do not use third party lists nor share their compliance databases with providers. On the other hand, it has been suggested by one of the experts to rank the criterion "Data storage" as mandatory, as it goes hand in hand with the GDPR regulation. GPDR is a legal requirement and therefore mandatory.

Since a fully automated video identification process is not yet supported by the EU regulations, as mentioned in Subsection 3.2.2, it has not been added as a criterion in the initial best practice catalogue. However, an automation criterion is still useful for the experts. The criterion would be useful in order to know what repetitive tasks the software can automate while still being in compliance to given law. Certain tasks can be automated without violating the law, for example if the video identification tool provides an API, the documents which have been gathered during the identification process can automatically be transferred to the DMS [54]. Such automation features simplify the work of the call agents and furthermore help them to be more efficient. A convenience feature criterion would further help the experts to decide for or against a video identification tool. As already mentioned at the beginning of this section, the mandatory requirements have to be fulfilled in any case. Otherwise, the tool would not be compliant to given law and could not be used. Convenience features such as a booking system in the app of the video identification tool or an interruption feature, which lets the user continue the video identification wherever it has been stopped or cancelled, help providers to stand out from competitors.

8.2.1 Enhanced best practice criteria catalogue

The comparison between the initial best practice criteria catalogue and the adapted one in Table 8.1 shows an increase in general and optional criteria. The adapted or newly inserted criteria are marked in red. Subsection 7.5.6 already explained why the necessity for "Database usage for KYC checks" and "Data storage" should be changed. For the record only one out of the three experts suggested a change of necessity for the two mentioned criteria. The new inserted criteria "Degree of automation", "Adaptability to new legal requirements", "Quality and security measures for third party call agencies", "Degree of tamper security" and "Availability of convenience features" have been identified in Subsection 7.5.1 from the thematic analysis.

[54] Document Management System

Initial catalogue			Adapted catalogue		
Criteria	**Necessity**	**Category**	**Criteria**	**Necessity**	**Category**
Conditions for video based identification in Austria	mandatory	general	Conditions for video based identification in Austria	mandatory	general
Country support	mandatory	legal	Country support	mandatory	legal
Document support	mandatory	legal	Document support	mandatory	legal
Language support	mandatory	legal	Language support	mandatory	legal
Call agent support	optional	general	Call agent support	optional	general
KYC compliant	mandatory	legal	KYC compliant	mandatory	legal
API support	optional	technical	API support	optional	technical
Sandbox support	optional	technical	Sandbox support	optional	technical
GDPR conform	mandatory	legal	GDPR conform	mandatory	legal
Database usage for KYC checks	mandatory	legal	Database usage for KYC checks	optional	legal
Data storage	optional	legal, technical	Data storage	mandatory	legal, technical
Cost effectiveness	optional	general	Cost effectiveness	optional	general
Platform dependency	optional	general	Platform dependency	optional	general
			Degree of automation	optional	technical
			Adaptability to new legal requirements	optional	general
			Quality and security measures of third party call agencies	optional	general
			Degree of tamper security	optional	general
			Availability of convenience features	optional	general

Table 8.1: Comparison of the initial best practice criteria catalogue with the gathered insights of the expert interviews

8.3 Limitations with regard to the concept

In order to keep the best practice criteria catalogue as general as possible, the criteria themselves are also on a general level. Every criterion could be analysed in more detail and one could write a scientific paper about each criterion on their own. However, this of course goes beyond the scope of the master thesis. Furthermore, the criteria catalogue should be kept general with regard to the expert interviews. To gather as much information as possible and therefore, to get an answer to every question, the criteria need to be defined in a general way. The experts can not have detailed know how about every single criterion. Another reason for the general approach of the best practice criteria catalogue has to do with the fact that the expert interviews and gathered data can only be summarized in a meaningful way, if the level of detail is kept to a minimum.

This best practice criteria catalogue does not claim to be complete. But the extracted codes of the expert interviews and the recurring patterns are represented in the catalogue. The thematic analysis has been conducted by one person. Different researchers may extract different codes and therefore other results. However, in each of the expert interviews recurring patterns occur and therefore a completely different result of another

researcher will not be expected.

Another point of criticism is within the qualitative data analysis of the expert interviews. The amount of conducted interviews is low. By conducting more expert interviews, probably more insights and more aspects of the criteria catalogue could be gathered. Thus, the criteria catalogue itself is limited. In the expert interviews the focus was on the criteria for video identification tools. If the focus would have been broader a more detailed analysis of the complete video identification process could have been conducted.

Lastly, only regulations and directives within the European Union are in focus of this thesis. Therefore, only criteria which have to be fulfilled according to the European standards are mentioned. That means the whole research of this thesis is limited to European legislation. Analysing further jurisdictions would exceed the scope of the thesis.

CHAPTER 9

Summary and future work

First of all, a theoretical basis with regards to the AML directive and KYC regulation is built. These guidelines build the legal framework for the whole video identification and KYC onboarding topic. Thus, also a general introduction into how regulations and directives are defined and established in the European Union is stated in Chapter 2. How legal requirements are organized within the EU is important to understand as there are new regulations coming nearly every year and this effects of course the mentioned video identification criteria catalogue.

With the help of the theoretical background, the state of the art chapter introduces methods how to identify natural and legal persons in the digital age, without meeting them in person. Such tools are necessary mainly because the demand has increased tremendously during Covid-19. In addition, customers nowadays expect these services. Blockchain technologies for identification purposes in financial institutions, as mentioned in 3.2.3, are on their way to the industry, and are already being tested extensively. It is only a matter of time before they will be implemented in a comprehensive way.

The analysis of the seven biggest banks supports the picture about the importance of video identification tools. Almost all of the analysed banks work with video identification tools in one way or another. Alternatives to video identification and personal meetings are the upload of legal documents or other verification methods such as EPS [55].

The best practice concept provides the reader with 13 criteria for video identification tools, which need to be fulfilled in order to be used in the European Union. The criteria catalogue itself is divided into the three categories: legal, general and technical. The legal criteria must be fulfilled, otherwise a video identification tool can not be used at all. The other categories are of supporting nature for the process. The criteria catalogue itself serves as a decision guidance. Through the elaboration of a best practice criteria

[55] Electronic Payment Standard

catalogue, the criteria are defined in a more general way. The interviewed experts approve the defined criteria catalogue. It contains all relevant criteria they need to make a decision. Nevertheless, the interviews give also an insight, how important customer experience during the onboarding process is and therefore how important it is for the bank that the selected tool supports and even increases the customer experience. The results of the expert interviews show that modern banking is not possible without using video and signature identification tools.

The defined best practice criteria catalogue serves as basis and can be further developed. One way to extend the catalogue can be the inclusion of other jurisdictions around the world, or the inclusion of other general or technical features. As the legal requirements are changing quite rapidly, the catalogue has to be adjusted over time to stay up to date. Moreover, criteria for processing biometric data can be added in the near future, after the updated KYC regulation has become active.

APPENDIX A

Appendix

Semi-structured interview guide

The interviews have been executed in a semi-structured way. This interview guide serves as an orientation tool during the interviews and has not the intention to answer the questions in the guide precisely, but do establish a good basis of discussion.

Interview preconditions

- Pitching the topic of my master thesis
- Discuss the publication of the interview (anonymized)
- Is an audio recording of the interview allowed?

Introduction

- What is your position in the company?
- How important is the onboarding topic and furthermore the video identification of customers in your financial institution?
- Is the video identification process outsourced (why/why not)?

Onboarding

- For which products is video identification used?
- Is there an alternative to video identification?
- What advantages has video identification and why is it used in your institution?

Criteria for video identification tools

- How did you choose the right video identification tool for your organisation?
- Which criteria played a role?
- Is the provided criteria catalogue helping you to find the video identification tool you would need for your organisation?
- What criteria are missing in the catalogue?
- Where do you see issues with the criteria catalogue?

Thematic analysis mind maps

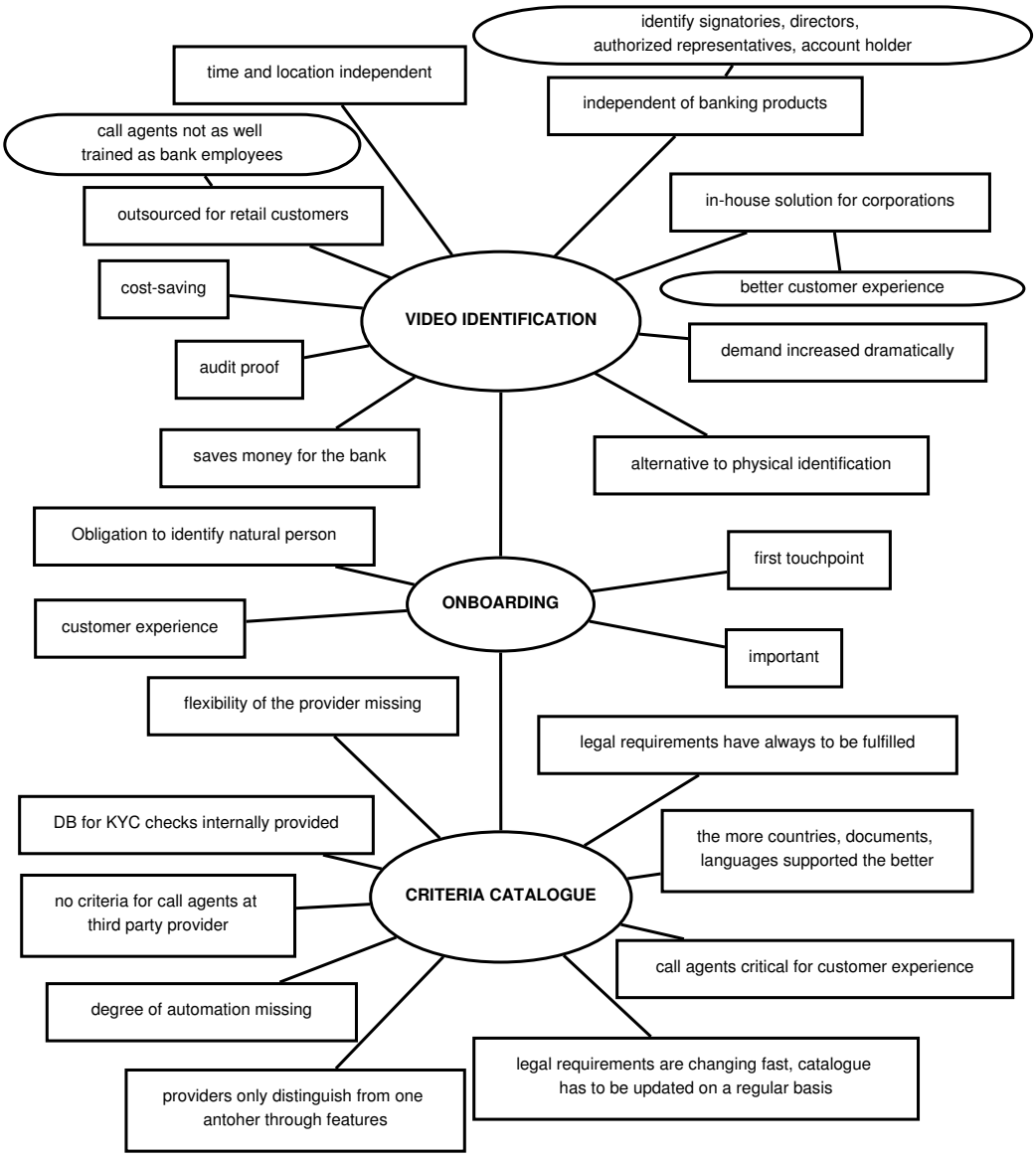

Figure A.1: Initial thematic map

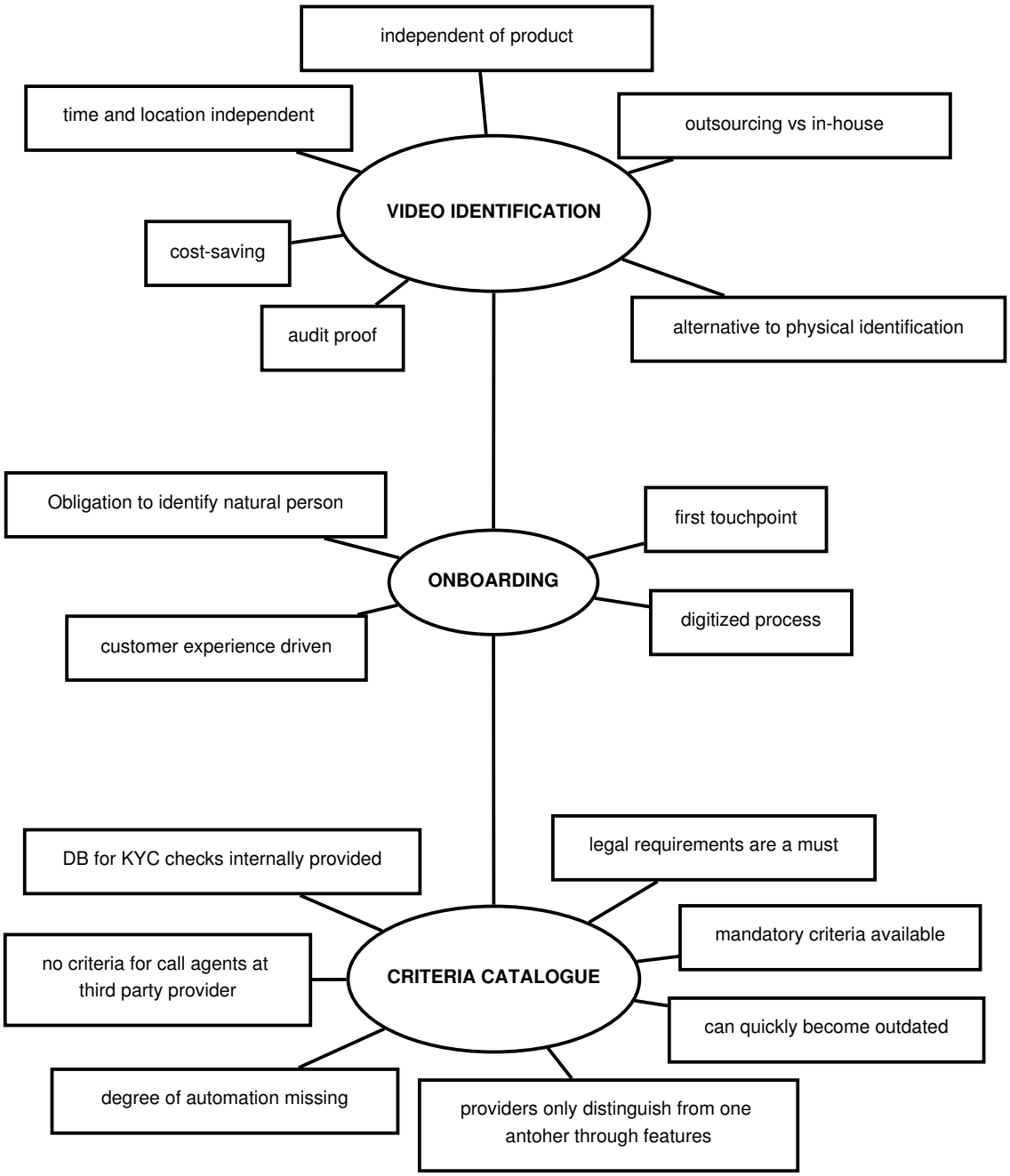

Figure A.2: Developed thematic map

Interview transcripts

The interviews have been conducted in German, because it is the native language of all interviewees and the interviewer. Therefore the transcripts are written in German as well. Additionally the information loss is minimized when speaking in everyone's native language. The passages used in the thesis have been translated into English.

Transcript Alpha

Interviewer: Markus Wasserbauer (M)
Interviewee: Alpha (A)
Date: 04.10.2021
Point of presence: The interview has taken place physically

M: Welche Position haben Sie im Unternehmen?
A: Ich bin bis vor kurzem gewesen der Head of Customer Data Management und übernehme jetzt die Position Operational Excellence, das heißt wir stellen für die Bank Platformservices zur Verfügung. Zum Beispiel für das Dokumentenmanagement, aber auch die ganze Kundenstammdatenverwaltung, dass läuft über meinen Tisch. Die Product Ownership, also im Prinzip die Userstories schreiben, was sollen die Systeme abdecken, welche Usecases sollen sie supporten und wie soll das dann für die User genau aussehen.

M: Wie wichtig ist das Thema Onboarding und darüber hinaus die Videoidentifikation von Kunden in Ihrem Finanzinstitut?
A: Onboarding ist ein sehr wichtiges Thema, weil dass an und für sich der erste Customer Touchpoint ist den der Kunden zu den Services der Bank hat. Also normalerweise, dass erste was er kennenlernt ist entweder die Homepage oder den Kundenbetreuer und da kann er sich einmal schlau machen. Da bekommt er ein Angebot bzw. sucht sich heraus, was für ihn ein interessantes oder relevantes Service ist. Und bevor er dann dieses konkrete Service nutzen kann, muss er durch diesen Onboarding Prozess durch. Also dass ist eigentlich wie ein Bottleneck wo alle durch müssen und wenn dieser Prozess mühsam ist, ist dass natürlich für den Kunden ein potenzieller Frustrationsmoment. Vor allem in der Vergangenheit war dieser Prozess oftmals geprägt von Iterationen, weil sich erst im späteren Zeitpunkt des Onboardingprozesses bestimmte Dinge herausstellen, zum Beispiel welche Risikoklassifikation bekommt er intern. Und wenn er eine höhere Risikoklassifikation hat, muss er mehr Dokumente beibringen, als einer der ein österreichisches protokolliertes Unternehmen ist, das quasi um die Ecke sitzt. Als wie wenn einer irgendwo auf Zypern, oder irgendwo in Korea sitzt. Das ist der eine Punkt. Also die Iterationen sind ein Thema, dann ist ein Thema das ganze Formular basierte. Viele Angaben von den Kunden werden immer noch mit klassischen Forms abgedeckt, das heißt der füllt dir ein Formular aus. Zum Beispiel seine Self Certification für die Steueransässigkeit und dann muss er dieses Unterschreiben, klassisch/firmenmäßige Fertigung und dann musst du intern sehen, hat das der richtige unterschrieben, kann man das akzeptieren und so weiter. Kann ich es nachvollziehen, dass es firmenmäßig gefertigt ist? Also der Onboardingprozess ist schon sehr wichtig, weil da jeder durch muss und je länger dieser

Onboarding Prozess dauert, desto mehr Zeit vergeht natürlich bis der Kunde tatsächlich die Services nutzen kann. Im worst case wenn ihm das zu blöd wird und parallel mit einem anderen Service Provider, der das gleiche anbietet wie wir, da leichter und schneller durchkommt, kann es sein dass er abspringt und das ist natürlich ein wirtschaftlicher Schaden für uns.

M: Du hast eher vom Onboarding generell geredet. Und im weiteren Bezug auf Videoidentifizierung, wie wichtig ist die für das Unternehmen selbst?
A: Also für die Nutzung unserer Services, gibt es die Notwendigkeit, dass du die Personen, die konkret die Services nutzen dürfen, also zum Beispiel Zeichnungsberechtige vom Konto, oder Personen die einen ELBA-Verfüger kriegen. Also die im Electronic Banking Überweisungen durchführen dürfen, oder überhaupt auch nur die Umsätze ansehen dürfen. Es ist notwendig, dass du diese Personen persönlich identifizierst. Das heißt du berechtigst nicht eine Firma, sondern du berechtigst immer eine Person. Und diese Berechtigung musst du an die Person knüpfen und deswegen musst du auch genau wissen, wer ist die Person und wie stelle ich sicher, dass ich jetzt diese Person als Gegenüber habe, über das elektronische Medium. Deswegen ist einmal der erste Schritt, ich lege einen Record für diese Person an, in unserem Stammdatensystem. Dann bekommt diese eine Nummer. Mit dieser Nummer verknüpfe ich dann bestimmte Rechte, zum Beispiel Zeichnungsberechtigter für ein Konto. Das Recht kann ich dann noch einschränken, da gibt es zum Beispiel diese A und B Unterschriften. Kann der nur mit jemanden anderen gemeinsam unterschreiben, auf der gleichen Ebene oder eine Ebene höher und so weiter. Solche Konzepte. Damit ich sicher bin dass der Record auch wirklich zu der Person gehört, muss ich diese Person zweifelsfrei identifizieren können. Dass kann ich machen, indem diese Person herkommt und sich mir vorstellt und ich sozusagen ein Legitimationsdokument überprüfe, oder dass geht auch über elektronische Wege. Sprich Videoidentifikation wo mir diese Person bestimmte Fragen beantworten muss, wo sie mir ein Legitimationsdokument zeigen muss. Das Ganze wird über diese Plattform abgewickelt. Dieser Prozess wird auch dokumentiert. Sprich das Video wird aufgehoben und so weiter und die Bilder von dem Dokument, dass er mir zeigt, werden auch aufgehoben, damit das einfach nachvollziehbar bleibt.

M: Wird der Videoidentifizierungsprozess ausgelagert (warum/warum nicht)?
A: Also derzeit ist es glaub ich für uns nicht möglich rechtlich dass wir das Auslagern dürfen. Weil wir als Bank sozusagen ja auch verpflichtet sind, diese ganzen BWG, AML und so weiter Bestimmungen einzuhalten. Ich bin aber kein juristischer Experte. Also ich kann mich im Zweifelsfall, wenn ich nicht sicher sein kann, dass eine Person auch wirklich die ist die sie vorzugeben scheint, nicht an jemanden anderen verlassen. Weil dieser ganze Identifikationsprozess birgt natürlich ein Betrugsrisiko. Also wenn jemand mit einem gefälschten Ausweis kommt, dann muss ich Möglichkeiten haben, dass ich diesen Betrug erkenne und dann auch sozusagen den Prozess abbreche, oder die Identifikation nicht akzeptiere. Es gab in der Vergangenheit oft die Anforderung, dass wenn wir Reisepässe aus irgendwelchen Drittstaaten bekommen, dass diese Reisepässe dann auch von Notaren vor Ort postuliert werden mussten. Sprich der Notar bestätigt ja er hat von der Person

dieses Dokument bekommen und er kann zweifelsfrei nachweisen, das ist die Person und das Dokument gehört auch zu dieser Person und nicht da kommt irgendjemand anderer, der sich nur als diese Person ausgibt. Und genau das gleiche, wenn jemand zu mir kommt, muss ich das als Bank genau so machen. Und wenn ich das über Video mache, dann habe ich das gleiche Thema. Wenn ich das auslagere, ich kann vielleicht die Abwicklung teilweise auslagern, oder die Archivierung der Dateien, aber das entbindet mich nicht von der Pflicht, dass ich diese Person zweifelsfrei erkennen und zuordnen können muss.

M: Sprich, es muss quasi in der Bank liegen, es kann nicht outgesourced werden?
A: Die Verantwortung muss bei uns in der Bank liegen. Warum,? Weil ja dieser Zuordnungsprozess, also ich identifiziere die Person und ich ordne der zuerst einmal einen Stammsatz und in weitere Folge Berechtigungen zu, könnte ja auch missbräuchlich genutzt werden, im Sinne von Steuerhinterziehung und Geldwäsche. Dafür gibt es rechtliche Vorgaben, die nicht ausgehüllt werden dürfen durch ein auslagern. Also ich sage jetzt übertrieben gesprochen, wenn ich das nach Indien auslagere und die machen diesen Prozess einfach schlampig, dann kommen die Geldwäscher alle durch, dann wäre ich mit dem nicht gedient, dem Gesetzt. Und deswegen glaube ich sind sollte Sachen potenziell eher schwierig zum Auslagern.

M: Für welche Produkte wird die Videoidentifikation eingesetzt?
A: An und für sich ist die Produktnutzung unabhängig von der Identifikation. Also wir haben klassische Bankingservices, wie Firmenkonten. Über diese Konten werden die ganze Firmenzahlungen inklusive die Payroll abgewickelt. Und die Leute die normalerweise die Verfügungsberechtigungen über diese Konten kriegen, sind halt beispielsweise Mitarbeiter in der Lohnbuchhaltung oder auch im Einkauf, die halt einfach Überweisungen tätigen müssen. Und diese Personen werden identifiziert, damit sie diese Services nutzen können. Es gibt andere Bankingservices wie Verbriefungen oder Garantiegeschäft. Das ist eher dokumentenbasiertes Geschäft. Da geht es eher für die rechtsgültige Unterschrift, um die firmenmäßige Fertigung der Geschäftsführer von den begünstigen Firmen. Da kann man wahrscheinlich auch ohne Videoidentifikation auskommen. Aber grundsätzlich wenn ich identifiziert bin, bin ich identifiziert. Was ich damit mache, bleibt mir überlassen, als Bank. Also die Produktnutzung ist eigentlich nicht so das ausschlaggebende meiner Meinung nach.

M: Gibt es eine Alternativen zur Videoidentifikation?
A: Naja, es gibt die klassische, persönliche Identifikation. Sprich die Person muss in die Räumlichkeiten der Bank kommen, das Dokument vorlegen, ich sehe mir das Dokument an. Sehe mir an ob das die gleiche Person ist, aufgrund des Fotos. Ich sehe mir an ob das Dokument noch gültig ist, mit dem Ablaufdatum und dann kann ich das genauso akzeptieren.

M: Was vielleicht auch in vielen Fällen nicht realistisch ist, wenn man mit irgend einem Offshore Kunden Geschäfte machen will.
A: Genau, bei unserem Kundenportfolio, also wir haben halt sehr viele internationale Kunden, die teilweise sehr weit weg sind. Wo nicht einmal die Kundenbetreuer jedes mal selber hinfliegen, so wie karibischen oder nordamerikanischen Standorten, weil das

einfach viel zu teuer wäre. Deswegen ist man da auch schon auf die Nutzung von solchen elektronischen Medien angewiesen. Aber im klassischen Filialbankgeschäft, ist dass schon noch so, dass jemand der zum Beispiel eine Überweisung oder Abhebung über 5000€ tätigt, der legt ein Dokument vor, der legt einen Ausweis vor.

M: Welche Vorteile hat die Videoidentifikation und warum wird sie in Ihrem Institut eingesetzt?
A: Ein Vorteil ist, die Standortunabhängigkeit, das heißt ich muss nicht physisch die Person herholen oder hinfahren, um es durchführen zu können. Ich kann damit auch Zeitdifferenzen überbrücken. Also wenn jemand in einer anderen Zeitzone ist, kann ich das trotzdem machen. Ich kann es eigentlich mit heute gängigen Endgeräten machen, sprich mit einem Handy. Ich brauche nicht unbedingt einen Kiosk, oder irgend eine Hardware hinstellen um es zu machen. Sondern ich kann das auf einem normalen Tablet, Laptop oder Smart Phone machen. Weil diese Geräte alle eine Kamera haben und ein Mikrofon haben. Diese Geräte sind mittlerweile so gut von der Auflösung, dass das funktioniert.

M: Wie haben Sie das richtige Videoidentifikationstool für Ihre Organisation ausgewählt?
A: Das ist schwierig, weil damals war ich nicht dabei in dem Prozess. Ich meine ich kann was dazu sagen was heute Kriterien wären, wenn man ein neues Tool aussuchen müsste. Also das eine ist die Stabilität, weil so wie ich am Anfang gesagt habe, dass ist ein Teil der Customer Experience. Wenn das vom Ablauf her und der Kunde muss, wenn er da einsteigt auf einen Einladungslink klicken und vielleicht muss er sich dann noch irgendwie authentifizieren. Entweder bekommt er von uns Username und Passwort, oder bekommt einen Token in dem Link. Wie auch immer. Wenn das mühsam ist, dann ist das schlecht. Dann ist ein wesentliches Thema die Kompatibilität. Ich kann nicht ein Service anbieten, dass nur auf iPhones funktioniert, weil ich kann nicht sicher sein, dass alle meinen Kunden diese Endgeräte haben. Es können auch andere Geräte verwendet werden. Also Kompatibilität ist ein Thema. Stabilität ist sicher ein Thema. Wenn der Prozess abbricht, dass er dann nicht von vorne anfangen muss, sondern dass ich vielleicht irgendwo aufsetzen kann. Weil vielleicht hat der erste Teil des Prozesses funktioniert, aber der zweite Teil, wo er dann den Ausweis hinhaltet ist auf einmal abgebrochen. Dann brauche ich vielleicht nur noch das mit dem Ausweis wiederholen und nicht alles. Dann wären natürlich sicher auch gute Features, dem Kunden zu ermöglichen, dass er sich für einen Slot registriert, so ein Buchungssystem. Dass unser momentanes Tool nicht unterstützt. Also wir müssen eigentlich die ganze Terminverwaltung hinten irgendwie selber machen. So etwas wie heute die Reservierungssysteme bei den Restaurants haben. Book a table. Ich sehe mir an welche Tische gibt es noch zu welcher Zeit, dann klicke ich darauf, drei Personen, zack ich bekomme das Mail und der Slot ist gebucht. So etwas wäre ein gutes Feature.

M: Welche Kriterien spielten eine Rolle?
A: Es gibt natürlich sicher noch jede Menge anderer Kriterien, wie zum Beispiel dass die Qualität der Aufzeichnung aussagekräftig ist. Es hilft mir nichts, wenn ich ein schwammiges verschwommenes Bild von einem Dokument irgendwo abgelegt habe, wo

ich dann nicht einmal mehr die Passnummer lesen kann, oder das Foto identifizieren kann. Also das muss die Software natürlich können. Wobei erfahrungsgemäß nicht die Software der limitierende Faktor ist, sondern eher die Hardware oder das Licht. Wenn die Person das irgendwo macht, zu weit weg, dann muss die Software sagen, hör zu suche dir einen Platz mit einem besseren Licht.

M: Weil es auch Software gibt die so etwas klarstellen kann, ein fehlerhaftes Bild, ein überbelichtetes Bild.
A: Ja sicher, das gibt es auch. Aber die Frage ist, wenn die Software den Benutzer hinweisen kann auf ich merke die Kontraste sind schlecht, versuche einen anderen Platz zu finden. Oder wenn die Netzwerkqualität schlecht ist, dann kannst du einfach sagen, bitte sieh zu, dass du besseren Empfang findest, dass der Prozess einfach flüssiger läuft und nicht einfach abbricht.

M: Ist auch für den Kunden angenehmer, der was ongeboarded wird.
A: Ja genau
M: Hilft Ihnen der bereitgestellte Kriterienkatalog bei der Suche nach dem Videoidentifikationstool, das Sie für Ihre Organisation benötigen würden? „Condition for video based identification in Austria“ sind quasi die Rahmenbedingungen, in Österreich vor allem. Die FMA gibt ja vor, wie darfst du die Videoidentifizierung durchführen in Österreich. In Österreich ist es ein bisschen strenger ausgelegt, als es die EU Richtlinie sagt. Du musst einen abgesperrten Raum haben, du musst abbrechen sobald irgendwie ein Fraud Versuch besteht. Du muss ein Bild machen von dem Pass, der Ausweiskopie und so weiter. Das wäre quasi einmal der erste Punkte.
A: Aber was ist die Frage noch einmal?
M: Ob die Kriterien was helfen? Also ich will mit dir einfach die Kriterien durchgehen, quasi sagen, ja natürlich brauch ich das. In der Spalte Necessity sieht du schon, dass ist eine Legal Precondition, ohne die geht es gar nicht. Und jetzt würde ich mit dir Step für Step die Kriterien durchmachen, siehst du das auch so, gehört das rein, warum nicht und so weiter?
A: Vielleicht ein Allgemeines Statement. Wenn es gesetzliche Anforderungen gibt, an welche Daten muss ich sammeln, wie muss ich diese aufbewahren das ist klar. Dass muss ich immer erfüllen. Darüber hinaus gibt es vielleicht einfach nice to have features, die die Customer Experience verbessern. Wodurch sich diese Anbieter auch ein bisschen differenzieren voneinander. Wo es dann halt bessere und schlechtere gibt. Also zum Beispiel das mit dem Adressbuch Feature oder dem Book a Slot Feature ist vielleicht nicht gesetzlich notwendig, weil es einfach angenehm ist für den Kunden und dass ist vielleicht für mich deswegen ein wichtiges Kriterium. Also ja gehen wir das durch. „Condition for Video based identification in Austria“ das verstehe ich nicht ganz, weil was heißt das?

M: Das ist genau das, was ich gerade gemeint habe. Du musst die Grundvoraussetzungen erfüllen, die Bank muss einen Raum bereitstellen, die Bank muss den Prozess so machen.
A: Ja, generelle gesetzliche Kriterien sicher.

M: Da könnte man sehen, alle legal Aspekte sind eigentlich mandatory. Du siehst zum Beispiel bei „Country Support“, wie viele Länder deckt das Tool ab.

A: Also da ist für uns, wir machen auch rund um den Globus Geschäft. Vielleicht in manchen Ländern nicht, ich kann aber nie wissen, ob nicht Morgen ein Kunde kommt, der in einem Land sitzt, wo ich bis jetzt nicht tätig war. Und natürlich wenn mir das Tool dann nicht ermöglicht dort zu arbeiten, weil die User von dort nicht einsteigen können, dann habe ich natürlich ein Problem. Dann muss ich vielleicht wieder den Kunden bieten, dass er zum Notar geht, oder herfliegt, oder ich muss hinfliegen, also ja das Kriterium macht Sinn.

M: Dann der „Document Support“ ist etwas ähnliches. Du kannst nicht nur mit dem Pass legitimiert werden. Du kannst zum Beispiel in Österreich den Führerschein herzeigen, du kannst in der EU auch den EU weiten standardisierten Personalausweis herzeigen. Je mehr Dokumente du im Tool hast die unterstützt werden desto besser, würde ich jetzt einmal behaupten.
A: Vielleicht gibt es in irgendwelchen Ländern Dokumente die dort sehr gebräuchlich sind, aber international nicht wirklich aussagekräftig sind. Dann ist die Frage, ob das nicht vielleicht eine Lücke wird. Aber das muss man sich im Detail ansehen. Natürlich die Basisdokumente, also ein Reisepass ist normalerweise weltweit gültig. Auch nicht immer. Es gibt Länder wo die Pässe nicht von jedem anderen Land akzeptiert werden. Dass muss man sich im Detail ansehen. Aber natürlich, das Dokument, welches gezeigt wird, im Zuge des Prozesses ist ein wesentlicher Punkt. „Language Support“

M: Da geht es vor allem nicht um die generelle Sprache, da geht es um die Sprache im Tool, in der GUI. Sprich wenn die Bank ein Geschäft macht mit einem türkischen Kunden und das Tool ist nur auf Englisch. Ist das wichtig, nicht wichtig? Weil es geht um sensible Daten, es geht um einen sensiblen Prozess, Customer Experience ist vielleicht ein Thema?
A: Es ist wichtig, weil wenn der User dort bestimmte Dinge erklären muss, dann muss er natürlich verstehen, was er da erklärt. „Call Agent Support“

M: „Call Agent Support“ ist genau das, was jetzt intern läuft. Sprich es muss quasi sichergestellt sein, dass diejenigen Mitarbeiterinnen und Mitarbeiter, die das durchführen auch die Sprache vom Kunden sprechen. Den Prozess verstehen, mit dem Tool arbeiten können und so weiter. Dass die quasi auch verstehen, bei dem und dem Dokument musst du auf diese Merkmale achten, beim Pass musst du auf diese Merkmale achten.
A: Ich verstehe nur nicht genau, was das Kriterium da für die Software oder den Lösungsanbieter aussagen soll? Also ob ich einen Agent einsetzten kann oder nicht? Einen Agent brauch ich immer. Dass ist ja kein maschineller Prozess, wo eine AI den identifiziert und die AI dann entscheidet, ist das jetzt der oder nicht.

M: Aber das ist jetzt im Kommen. Das vollautomatisiert eine Identifikation möglich ist. Zurzeit, wie du es richtig sagst, gibt es noch nicht, oder ist auch nicht im BWG erlaubt. Aber es gibt Anbieter, welche eine fully automated Videoidentifikation supporten. Aber diese sind im Bankenwesen angesehen. Sprich du kannst, wenn du eine Versicherung abschließt, vollautomatisiert identifiziert werden, durch einen deutschen Anbieter. Generell im Videoidentifikationsspektrum gibt es das noch nicht, weil es Gesetzlich noch nicht gestützt ist.

A: Also das ist ein wesentlicher Punkt. Wir können uns heutzutage noch nicht so auf diese Technologie so verlassen und wenn das rechtlich gar nicht geht, dann ist es so.

M: Das nächste ist eigentlich wieder ein legales Thema, was gegeben sein muss. Du musst natürlich als „KYC compliant“ auch noch den Richtlinie der eIDAS entsprechen. Die Richtline gibt ja vor was ist eine elektronische Identifizierung, was ist QES, qualified e-signature, was ist eine standard signature. Und das müssen die Provider natürlich auch abdecken.
A: Ja sehe ich auch so.
M: Also weil es einfach ein legal Requirement ist. Und du hast vorher gemeint, alle legal Requirements müssen abgedeckt sein.

M: „API Support“. Du hast vorher gemeint, es wäre schön, wenn es Features gibt, wo sich die Kunden abheben können. Ist das zum Beispiel ein Feature, wo du sagst, wenn der Provider eine API zur Verfügung stellt, was man auch verwenden kann, in seine interne Prozess einbinden kann, nice to have?
A: Nein, dass würde ich schon eher als strategisch relevant sehen, dass das mandatory ist für unsere Auswahl, weil wir halt auch die Daten von dem Prozess in unsere internen Systeme übernehmen können müssen. So wie ich am Anfang beschrieben habe, wenn ich eine Person beginne zu identifizieren, muss ich einmal einen Stammsatz anlegen. Wer ist sie, wie heißt sie, Geburtsdatum, Geschlecht, usw.? Und wenn ich das über programmatische Schnittstellen machen kann, bin ich einfach effizienter und potentiell auch schneller in der Abbildung der internen Systemen. Als wenn der Agent zum Beispiel das alles wieder händisch erfassen müsste. Oder ich bekomme das in einem Batch, in einem File einmal am Tag, dann habe ich den zwar identifiziert, er kann es aber trotzdem erst am nächsten Tag nutzen, weil einfach der Batch erst über Nacht läuft. Also solche Sachen sind mittlerweile strategisch wichtig, weil die natürlich die Customer Experience wieder beeinflussen und auch für uns intern natürlich Arbeitserleichterung bedeuten.

M: Dann mit API Support geht eigentlich Hand in Hand ein „Sandbox Support“. Sprich ob Tools auch ein Testenvironment zur Verfügung stellen, wo man das Tool vielleicht auch testen kann.
A: Ist sicher nett. Ich meine zur Not kann man immer zur Not solche Sachen testen. Dann ist halt die Frage, was mache ich mit den gewonnenen Daten? Ob ich die dann wieder wegschmeiße oder aufbewahre? Weil durch die Identifikation per se passiert noch nichts. Die relevanten Daten entstehen ja erst durch die Verknüpfung. Ich gebe dieser Person dann bestimmte Rollen und Rechte. Das kann ich ja stoppen, weil die Identifikation ist nur ganz vorne. Insofern sehe ich da nicht das Thema, dass man das nicht auch mit der Produktion machen könnte. Ist sicher nice to have, vor allem wenn man neue Features ausprobieren kann, bevor man diese Live schaltet in der echten Umgebung.

M: Oder in einem POC schon sieht was möglich ist und was nicht?
A: Ja! Also „GDPR conform“ ist wieder ein no brainer, weil es ist eine rechtliche Anforderung. „Database usage for KYC checks“. Was soll das bedeuten?

M: Zum Beispiel wir müssen bei der Identifizierung auch PEPs identifizieren können, also

political exposed persons. Und wie passiert das? Bringt die Software, das Tool das man verwendet, Sanktionslisten mit, PEP Listen mit, wo man einfach den Kunden nur mehr gegencheckt. Oder ist dass eher was, was man intern macht, weil man das besser macht, oder bessere Daten hat.
A: Ja ist ein Punkt. Jede zusätzliche Information ist da natürlich willkommen. Weil ich sage vielleicht ist diese eine Sanktionsliste nicht vollumfänglich. Dann habe ich aber noch zwei, drei andere Listen und ich gehe aber alle durch im Rahmen des Prozesses. Dann habe ich natürlich mehr Abdeckung, vor allem wenn ich das automatisiert machen kann. Insofern wenn es da solche Warnhinweise oder Dinge gibt, ist das sicher gut. Wenn ich nicht dieses Tool nutze, sondern der kommt persönlich, dann muss ich den ja genau so screenen können, ob er ein PEP ist oder ob er irgendwo sanktioniert ist. Und deswegen brauche ich sowieso eine zweite Lösung dafür. Nicht nur dieses Videoidentifikationstool, solange ich nicht ausschließlich Videoidentifikation machen. Ist sicher ein guter Punkt, sehe ich aber nicht als rein verpflichtend, eben weil ich ja auch parallel den nicht Videoidentifikationsprozess unterstützen muss.

M: Sprich, es wäre eigentlich nicht verpflichtend für das Tool deiner Meinung nach?
A: Für das Tool per se nicht. Dann muss ich es halt anders abdecken. Also ja die rechtliche Anforderung habe ich, aber die kann ich zur Not vielleicht auch wo anders abdecken.

M: So „Data storage“ ist das nächste. Sprich es hat auch wieder mit GDPR zu tun, DSGVO. Wie werden die Daten gespeichert. Werden die vom Provider direkt gespeichert, beim Provider? Dann ist die Frage wo steht der Provider, wo stehen seine Server?
A: Das ist sicher auch wieder ein rechtliches Thema, weil eben der Kunde, wenn er dieser Identifikation zustimmt, bestimmte Widerrufsrechte hat. Das sind halt sensible Daten und personenbezogene Daten und wenn die irgendwie geleakt werden, oder wenn das nicht sicher aufbewahrt ist. Dann hat nicht nur der Provider ein Thema, sondern jeder der dieses Service genutzt hat. Insofern sehe ich das schon als kritischer an. Aber was man da darf oder nicht darf. Wichtig ist es glaub ich, dass es da Transparenz gibt. Also dass der Provider halt nicht irgendwo nicht offenlegt, wo er die Daten verarbeitet oder speichert. Weil ich dann natürlich im Falle von einem Leak ein Problem bekomme.

M: Ok, dass nächste ist „Cost effectiveness”. Vielleicht noch kurz. Da geht es eher darum, wenn es zum Beispiel ausgelagert wäre, oder auch nicht, wenn die Videoidentifizierung intern gemacht wird, wie wird verrechnet? Wird man, wenn man einen Provider hat, pro Identifikation bezahlt, hat man eine Flat Rate? Also wie sehr sieht man auf die Kosten pro Identifizierung, oder dass durchführen der Identifizierung. Wenn man es nicht outsourced, sind viele Mitarbeiter an den Prozess gebunden, was auch wieder einen Aufwand innerhalb des Unternehmens ist.
A: Es kommt darauf an wie oft es verwendet wird. Also wenn man es momentan der Fall ist, wenn ich es nur für die initiale Identifikation brauche und dann vielleicht noch einmal bei einem Review alle paar Jahre, dann ist es vielleicht weniger relevant ob es 10€ oder 20€ kostet pro Fall. Wenn der Kunde das aber nutzen würde, bei der Transaktion die er freigibt, also bei jeder Anmeldung, oder bei jeder Zahlung die er tätigt, was ja

nicht der Fall ist, weil da nimmt er Momentan den ELBA-Verfüger den er hat. Wo er halt einen anderen Authentifizierungsmechanismus verwendet. Dann wäre das natürlich ein riesen Thema, wenn ich pro Fall weiß nicht wie viel Euro zahlen müsste. Wobei der Identifikationsprozess ist natürlich viel breiter, weil das ist mit Ausweis und hin und her und auch Menschengestützt. Sobald ich mich darauf verlasse, dass ist der und der unterschreibt jetzt nur noch mit seinem iPhone mit einem Push-TAN, habe ich viel geringere Anforderungen. Aber damit ich eben sicher bin, dass ist der, muss ich vorher mehr Aufwand in kauf nehmen. Und diesen Aufwand, muss man ins Verhältnis setzen. Wenn ich den Kundenbetreuer hinfliegen lasse müsste, oder der Kunde müsste zum Notar gehen und sich apostilieren lassen, dass das sein Ausweis ist, das kostet ja auch Geld. Insofern ist das natürlich schon potenziell immer billiger und eine Ersparnis. Diese Anbieter müssen ja auch eine Marge und Rendite erwirtschaften können. Deswegen, dass wird es nicht als public domain Lösung geben.

M: Weil es ein Geschäftsmodell ist.
A: Ja, aber natürlich 100€ pro Person für eine Identifikation wäre wahrscheinlich zu teuer. Insofern muss es einen Wettbewerb geben. Also die müssen sich auch konkurrenzieren dürfen am Markt und das wird den Preispunkt auch beeinflussen. Wenn es nur einen gibt, der das kann, dann ist es natürlich ein anderes Thema.

M: Typisch Monopol.
A: Ja

M: Der letzte Punkt wäre die „Platform dependency“. Sprich du hast es schon gesagt, wie wichtig ist es das man es am Handy machen kann, am Tablet, am Computer?
A: Sehr wichtig. Weil es eben wieder Customer Experience ist. Ich kann nicht dem Kunden sagen, gehe dir ein iPhone kaufen, dann kannst du es nutzen, weil mit deinem Android geht es nicht. Das wäre ein No-Go.

M: Welche Kriterien fehlen im Katalog?
A: So wie ich gesagt habe, Convenience Features. Buchungssystem zum Beispiel. Ein „resume when interrupted“ Feature. Also wenn der Prozess abbricht, warum auch immer, Bildqualität zu schlecht, Netzwerkverbindung zu schlecht. Und ich habe aber schon einen Teil des Prozesses erledigt, dann hätte ich gerne einen Wideraufsetzpunkt. Oder manchmal brechen diese Identifikationsversuche auch ab, weil vielleicht der Kunde hat einen dringenden Anruf und muss raus. Dass man dann möglichst einfach den Prozess zu Ende bringen kann. Oder einfach einen neuen Slot ausmachen kann, oder dass der Kunde das selber machen und veranlassen kann, weil nur er weiß, wenn er Zeit hat. Wenn ich den irgendwann anrufe und sage ich würde Sie gerne jetzt identifizieren in den nächsten 20 Minuten, dann passt das vielleicht für den nicht. Deswegen würde ich den Prozess eher umdrehen, dass er sagt wann er das gerne machen möchte. Was fällt mir noch ein? Natürlich so Features dass die Software den User darauf hinweist, wenn es Schwierigkeiten gibt. Netzwerkverbindung, Lichtqualität, Auflösung, Dokument nicht lesbar, keine Ahnung vielleicht hat er einen Reisepass verknittert normalerweise nicht. Aber das sind so Sachen was die Technologien mit sich bringen. Ich halte irgendwas

papierbasiertes in die Kamera und die Kamera muss halt den Winkel, die Lichtverhältnisse, Spiegelungen, usw. handeln und die Software muss mit dem umgehen können.

M: Wo sehen Sie Probleme mit dem Kriterienkatalog?
A: Du hast es gesagt, die Anforderungen und vor allem die Rechtsnormen, bewegen sich relativ schnell weiter. Das heißt wenn man sich jetzt aufgrund von so einem Kriterienkatalog auf einen Anbieter festlegt und dann kommen relativ neue Anforderungen, die einfach Gesetzlich bindend sind und der tut sich schwer das einzuhalten, dann muss ich im Zweifel relativ schnell vielleicht den Anbieter wechseln. Und Anbieterwechsel sind immer potenziell schwierig. Weil dann muss ich das in meine neuen Prozesse einbinden, ich muss die Leute schulen, ich habe vielleicht wieder Customer Experience derivation, das heißt es wird schlechter. Also der Kriterienkatalog per se, die Ganzen rechtlichen Sachen, das ist nicht nur technisch. Da gibt es halt viele Aspekte was darf man und was darf man nicht. Das ist alles sozusagen „carved in stone“. An dem kann ich nicht rütteln. Und darüber hinaus sind halt die technischen Features, die User Features und so Kostenthemen natürlich ein Differentiator.

Transcript Beta

Interviewer: Markus Wasserbauer (M)
Interviewee: Beta (B)
Date: 01.10.2021
Point of presence: The interview has taken place physically

M: Welche Position haben Sie im Unternehmen?
B: Ich bin Service Owner für Customer Onboarding, inclusive Review und auch Group KYC

M: Wollen Sie vielleicht spezifischer darauf eingehen, was diese Themenschwerpunkte beinhalten?
B: Themenschwerpunkt ist einmal eine End2End Verantwortung für den gesamten Prozess. Von wenn der Kunde reinkommt, bis zu dem Endpunkt wo er über seine Produkte verfügen kann. Wie gesagt Onboarding behandelt „new to the bank customers“, also Neukunden und review Bestandskunden, die anhand ihres Risikoprofils gereviewed werden müssen. Hochrisiko jährlich, medium risk alle drei Jahre und low risk alle fünf Jahre. Schwerpunkte auch bei dieser End2End Perspektive sind natürlich die Produkteröffnung, Kontoeröffnungen, Loans, Depots. Dann natürlich Gruppe verbundener Kunden und diverse Meldungen dazu. Kontenregistermeldungen, Cash Management, damit der Kunde auch über sein Konto verfügen kann. Mit den entsprechenden Zugängen. Was da auch gibt ELBA, ELGA, Mulit Cash. Das ist es eigentlich. Da habe ich die End2End Verantwortung für den gesamten Prozess. Auch wenn diese Teile jetzt nicht unbedingt in der Linienführung bei mir sind. Und Compliance ist da natürlich auch ein Part. Wenn es um regulatorische Themen geht, muss man auch zum Beispiel bei Hochrisiko Kunden ein OK von Compliance einholen.

M: Wie wichtig ist das Thema Onboarding und darüber hinaus die Videoidentifikation von Kunden in Ihrem Finanzinstitut?
B: Das ist sehr wichtig. Weil natürlich auch aus regulatorischer Sicht und aus dem FM GWG sind wir verpflichtend Personen persönlich zu identifizieren. Und da dient auch die Videoidentifikation als Mittel dazu und wird verwendet um Direktoren zu identifizieren in Offshore Bereichen, um Zeichnungsberechtigte zu identifizieren. Also die Erfordernis ergibt sich aus dem FM GWG.

M: Das betrifft jetzt eher das Onboarding und wie wichtig ist im spezifischen die Videoidentifizierung für das Unternehmen?
B: Um die regulatorischen Vorgaben erfüllen zu können muss man eine Videoidentifizierung machen.

M: Unter anderem. Gibt es vielleicht andere Weg dazu auch noch?
B: Es gäbe andere Wege in dem man einfach notariell beglaubigte Passkopien anfordern würde, oder wenn die Person persönlich vor Ort erscheint und so von einem Kundenbetreuer oder Mitarbeiter identifiziert wird.

M: Wird der Videoidentifizierungsprozess ausgelagert (warum/warum nicht)?
B: Nein wird nicht ausgelagert und zwar aus dem Grund wegen der Customer Experience. Also ich habe diese Entscheidung damals nicht getroffen, weil ich noch nicht hier war. Aber grundsätzlich wurde die Entscheidung getroffen es nicht auszulagern, sondern hier dem Kunden quasi ein Service zu bieten. Dass man sagt, man hat vor Ort Kollegen und Kolleginnen die mehrere Sprachen abdecken. Und dadurch auch den Kunden hier durchführen können. Mit ihm persönlich Termine vereinbaren. Die Videoidentifikation durchführen, anstatt dass man es einfach in ein Call Center gibt, wo jetzt dieser persönliche Service, oder generell der Service vielleicht etwas unpersönlich ist und nicht so wie bei uns.

M: Wenn du damals schon in der Position gewesen wärest, die Entscheidungsbefugnis gehabt hättest für auslagern oder nicht auslagern, würdest du es quasi auch so machen? Oder würdest du sagen, was ist der Vorteil wenn du es auslagerst, oder wenn du es quasi in house machst, aus deiner Sicht?
B: Ich war ja vorher schon in einer anderen Bank. Dort war es in dem Bereich wo ich war, noch nicht so wirklich durchgesetzt, sondern eher in der Retail Bank. Dort hat man es verwendet und dort war es auch eher ausgelagert und nicht so dass man es selber gemacht hat. Wie ich hier her gewechselt habe, war ich im ersten Moment ein bisschen überrascht. Ich kann es nachvollziehen, dass es natürlich für den Kunden ein besseres Service ist, wenn das sofort abgewickelt wird. Ich glaube aber dass ich es, um ehrlich zu sein, outgesourced hätte. Einfach weil es sehr viel Aufwand ist. Man muss halt immer Abwegen. Customer Experience ist natürlich sehr wichtig und das ist auch etwas auf das wir sehr stark schauen und was uns sehr wichtig ist. Aber es bindet auch sehr viele Ressourcen. Der Anbieter hat auch ein Call Center normalerweise und dort wickeln sie es ab. Vielleicht hätte ich mich auch für einen anderen Anbieter entschieden. Dass kann ich jetzt nicht sagen, was wäre wenn. Aber es gibt mehrere am Markt und auch in der

Bank wo ich davor war, gab es durchaus schon die eine oder andere Beschwerde über diesen Anbieter, dass es nicht so reibungslos funktioniert.

M: Für welche Produkte wird die Videoidentifikation eingesetzt?
B: Auf jeden Fall einmal für die Kontoeröffnung, sonst für andere Produkte wären mir jetzt nicht bekannt.

M: Wahrscheinlich grundsätzlich, wie du vorher schon gesagt hast, um Zeichnungsberechtige zu identifizieren, um Directors zu identifizieren. Personen die die Kontoführung für das Unternehmen übernehmen.
B: Genau, deswegen Kontoeröffnung und da hat man auch Zeichnungsberechtigte. Die muss man identifizieren und aus dem KYC heraus und aus der Geldwäsche.

M: Eigentümer müssen identifiziert werden, CEOs, CFOs die Geschäfte für das Unternehmen tätigen:
B: Weil du explizit auf die Produkte abgestellt hast, ist es die Kontoeröffnung. Bei einem Loan gibt es keine Zeichnungsberechtigten.

M: Gibt es eine Alternative zur Videoidentifikation?
B: Naja, jetzt kommt die neue Video-Ident Verordnung, oder die neue Verordnung raus. Und jetzt werden auch Biometrische Verfahren zugelassen. Das heißt das wäre eine Alternative, die man auf jeden Fall nutzen sollte. Und ansonsten die Alternativen, wenn man es jetzt nicht per Videoidentifizierung macht sind die, die ich vorher schon genannt habe, mit der Passkopie oder dem persönlichen Erscheinen. Aber es gibt natürlich unterschiedliche Anbieter, die unterschiedliche Produkte anbieten. VideoID, über IDnow. Dann gibt es andere Anbieter, die schon früher mit biometrischen Daten gearbeitet haben. Wie einfach mit einer Gesichtserkennung, oder einem Fingerprint, oder was auch immer. Aber man durfte es nicht verwenden, weil der Regulator es nicht erlaubt hat. Und wann das jetzt fällt, finde ich, sollte man schon auch nach anderen Lösungen schauen.

M: Quasi biometrische Sachen die im Kommen sind.
B: Ja genau

M: Welche Vorteile hat die Videoidentifikation und warum wird sie in Ihrem Institut eingesetzt?
B: Naja die Vorteile sind, dass der Kunden nicht persönlich erscheinen muss. Dass ist ganz wichtig im Offshore Bereich. Es ist so, dass der Kunde sicherlich nicht einen Flug buchen wird, damit er herkommt und sich persönlich Identifizieren lässt. Das ist ja auch mit Kosten verbunden. Das heißt, es ist eine einfache Möglichkeit, für den Kunden online einzusteigen. Seine Passkopie herzuzeigen, sich selber zu identifizieren. Also ich denke auch eine Zeitersparnis und Kostenersparnis. Wenn man die Unterlagen natürlich auch notariell beglaubigen müsste, fallen auch Kosten beim Notar an. Also ich denke das ist einfach ein Vorteil für den Kunden, sowohl eine Kosten- als auch eine Zeitersparnis.

M: Und warum wird sie in Ihrem Unternehmen eingesetzt?
B: Es ist ein Service an den Kunden und auch für uns eine Erleichterung, was die Videoidentifizierung betrifft oder die persönliche Identifizierung einer Person, weil man

das eben einfach Online abhandeln kann. Also wenn man jetzt eventuell mit jedem ein persönliches Meeting ausmachen müsste, oder auf Originaldokumente oder beglaubigte Kopien. Aber ich sehe es mehr als ein Service für den Kunden das auch anzubieten.

M: Würdest du sagen, dass mithilfe von Videoidentifizierung auch neue Märkte erschlossen werden können?
B: Es kommt auch immer drauf an, welche Länder diese Videoident Anbieter anbieten, wie die Abdeckung ist. Also von dem her ja sicherlich, in manchen Ländern, wo es vielleicht andere Möglichkeiten gar nicht gibt ist das natürlich ein Vorteil. Wenn man zum Beispiel in Usbekistan eine Videoidentifizierung machen kann.

M: Wie haben Sie das richtige Videoidentifikationstool für Ihre Organisation ausgewählt?
B: Das kann ich nicht sagen, weil ich nicht dabei war und bei der vorherigen Bank nicht dabei war, weil wo ich war, das nicht gegeben hat. Aber ich gehe stark davon aus, dass es eine Art Beauty Contest gegeben haben wird, mit mehreren Anbietern und sie sich dann für IDnow entschieden haben.

M: In beiden Fällen (Banken)?
B: Ich schätze in Beiden. Normalerweise sind Beauty Conteste üblich. Ich weiß es nicht, es gab bei meinem vorherigen Arbeitgeber eine Einheit, die sich mit solchen Themen sehr stark beschäftigt hat. Die auch schon lange bevor das mit den biometrischen Verfahren war, schon an solchen Lösungen gebastelt haben. Die waren da sehr innovativ. Da habe ich damals schon so eine Identifizierung mit Gesichtsmerkmalen gesehen als Prototypen. Aber normalerweise, so wie ich es kenne, ist es üblich dass man einen Beauty Contest macht, sich mehrere Anbieter ansieht und dann sich für einen entscheidet.

M: Welche Kriterien spielten eine Rolle?
B: Man müsste sich einmal ansehen, was der Provider überhaupt anbietet. Welche Länder Abdeckung er hat – Ländercoverage. Wie die Erreichbarkeiten sind. Gibt es eben solche Dinge, wie gibt es ein Call Center, gibt es Mitarbeiter, muss man das Insourcen, kann man das Outsourcen? Natürlich Kosten sind auch eine Frage. Wieviel kostet das? Und auch wie kann der Provider auch das halten, was er verspricht? Weil am Anfang ist es meistens immer so, dass die Unternehmen dann immer wir können das und das und das. Deswegen macht man dann einen Proof of Concept und kommt dann drauf ja es funktioniert oder es funktioniert nicht. Das sind so die Kriterien, die mir jetzt adhoc einfallen würden, wo man darauf schauen würden. Und natürlich noch die Anbindung an interne Systeme. Wie das ist? Muss man da extra was neues bauen, kann man das leicht integrieren oder nicht?

M:Hilft Ihnen der bereitgestellte Kriterienkatalog bei der Suche nach dem Videoidentifikationstool, das Sie für Ihre Organisation benötigen würden?
B: Was ist mit “Conditions for video based identification in Austria” gemeint? Aber das heißt einfach, ist es vom Regulator zulässig oder nicht. Das meinst du damit?

M: Genau, du weißt in Österreich haben sie es strenger ausgelegt, wie in der EU Richtlinie. Zum Beispiel musst du das Zimmer versperren können. Es dürfen nur Tonaufnahmen, keine Videoaufnahmen aufgenommen werden. Du musst den Pass, den Führerschein, den

Personalausweis kippen können, damit man die Sicherheitsmerkmale erkennt. Man muss einen Screenshot machen vom Pass, man muss einen Screenshot machen vom Gesicht und so weiter.
B: Da steht auch Mandatory, also das heißt das ist auf jeden Fall wichtig.

M: Wäre auch für dich Mandatory? Weil sonst kannst du es ja nicht einsetzten:
B: Ja. „Country support“, das habe ich auch vorher erwähnt, weil man muss natürlich wissen, welche Länder abgedeckt werden können, je mehr desto besser. Mit „Document Support“ ist jetzt gemeint, die Pässe und die Personalausweise und welche Typen von Legitimationen akzeptiert werden?

M: Richtig.
B: Natürlich wichtig. „Language Support“?
M: Da musst aufpassen. Beim Language Support geht es jetzt eher darum, wie das Tool aufbereitet ist. Sprich wenn du als Anbieter in einem anderen Land bist und quasi nur Englisch anbietest, aber in dem Land sprechen sie türkisch, dann ist es vielleicht schwierig für den Kunden ongeboarded zu werden. Erstens weil es ein sensibler Prozess ist, weil du gibst deine Daten weiter.
B: Aber inwieweit, wie ist es wenn man einen Mitarbeiter hat, der türkisch abdeckt?
M: Ja das kommt als nächstes beim Call Agent Support. Beim Language Support geht es darum, ob das Tool auch die Sprache unterstützt. Zum Beispiel wenn es keinen Call Agent gibt, muss es eigentlich geben, aber der Kunde anfängt auf der Landing Page und ist alleine, dann kann er sich nicht zurecht finden, wenn er die Sprache nicht spricht. Wie wichtig wäre dir dann, dass das Tool die Landessprache des Kunden auch unterstützt?
B: Ich dachte Language ist generell auf die Language bezogen, weil dass ist ja auch das was wir anbieten. Unser Service das wir Kollegen haben, die mehrere Sprachen abdecken und dementsprechend auch in der Muttersprache der Kunden agieren können. Deswegen „Call Agent“ ja. Es ist optional, es ist immer eine strategische Entscheidung. Will man sowas über einen Call Agent/Call Center outgesourced haben, wo höchstwahrscheinlich davon auszugehen ist, dass nicht alle Sprache abgedeckt werden können, oder halt nicht die Hauptsprachen abgedeckt werden können. Oder macht man das eben inhouse, so wie wir das machen. Wo man sagt, man deckt viele Sprachen unserer Hauptkunden, wo wir unsere Hauptmärkte haben, ab. Dann kann man dem Kunden auch gleich in seiner Muttersprache abholen.

M: Somit sehr wichtig, der Call Agent Support?
B:Ich finde es schon wichtig für die Entscheidung, wenn man sagen möchte, was möchte man. Möchte man es outsourcen und hat es in einem Call Center, wo jeder nur Englisch spricht, egal woher der Kunde ist. Oder sagt man eben, man macht es inhouse und dafür ein wenig Kundenorientierter, in dem man einige Sprachen abdeckt. Es muss nicht alles sein, weil es ist nicht machbar, dass jeder jede Sprache abdeckt. Aber zumindest von den Coremärkten, oder wo man die meiste Präsenz hat, aber es ist jetzt nicht verpflichtend.

B: „KYC Compliant“, das heißt mit einem Wort Compliant aus dem FM GWG heraus. Wo die persönliche Identifikation auch beschrieben ist, die durchgeführt werden muss.

Das spielt da dann mit. Natürlich muss das auch, sage ich jetzt einmal, KYC compliant, oder aus der Geldwäsche heraus zusammen passen.

M: Sonst kann man es ja nicht verwenden.
B: Korrekt, sonst kann man die persönliche Identifikation nicht durchführen und das würde dann ins Absurdum führen, weil dann brauche ich das Tool nicht, wenn das nicht compliant ist.

M: Kurze Erklärung zum „API Support“. Wenn man das Tool quasi in den Bankenprozess integriert.
B: Ich muss gestehen, was das technische betrifft, bei so einem Video ID Verfahren, bin ich jetzt nicht ganz bewandert. Ich hätte verstanden, dass es einfach eine separate Software ist, die man bei sich installiert hat, wo man eben die Videoidentifikation durchführt. Ich glaube nicht, dass wir eine API Anbindung haben, wo dass dann automatisch in irgendwelche Folder reingeschossen wird. Ich glaube dass gibt es nicht. Aber natürlich, wenn die Möglichkeit bestünde, und man möchte ja alle Prozesse so gut wie möglich auch automatisieren und manuelle Tätigkeiten reduzieren. Wenn das auch compliant ist, mit so einer API Anbindung, ist es sicher auch von Vorteil.

M: Die API Anbindung ist eigentlich für die Entwickler, die Funktionen, die in diesem Video Ident Tool wären, bei uns zum Beispiel im Kernbanksystem verlinken, mit dem du quasi das Videoidentool aufrufen und damit kommunizieren kannst.
B: Ich dachte es geht auch darum, um diese Sprachaufzeichnungen und diese Screenshots auch gleich abzulegen, weil wir müssen das aufbewahren und so eine API Verbindung könnte auch dazu dienen, dass das dann auch automatisiert in den Folder des jeweiligen Kunden hineingespielt wird. Nicht nur, dass man es automatisiert aufrufen kann.

M: Das ist natürlich auch eine Möglichkeit. Eine API ist eine Art Baukasten, wo du quasi die Software rausnimmst und damit was machen kannst. Wenn dass der Provider anbietet, kann man damit eigenständig die Prozesse automatisieren. Wenn er es nicht anbietet, bist auf ihn 100% angewiesen.
B: Das ist richtig, aber das ist irgendwie, was man sich vorher dann überlegt, ob man das unbedingt machen möchte. Ich glaube wie man sich damals dafür entschieden hat, war das jetzt nicht im Vordergrund. Wenn man jetzt aber weiter denkt in Richtung Digitalisierung, Automatisierung und man möchte hier auch vieles verändern von der IT Infrastruktur, dann ist es schon von Vorteil, wenn es so eine Möglichkeit gibt, so einen API Support. Den man dann natürlich auch verwenden kann.

M: „Sandbox Support“ vielleicht auch zum erläutern?
B: Das ist zum Testen, oder? Sandbox ist normalerweise wo man eine Funktion testet, bevor man sie dann live nimmt. Das war bei der PSD2 gab es auch Sandboxes, also Payment Service Directive bevor man die live genommen hat. Ja, aber dass ist etwas wo ich sage, diese Entscheidung obliegt eher den ITlern im Unternehmen. Kommt darauf an, was der Vendor anbietet. Wenn es eine Testumgebung gibt. Ich glaube das ist eine individuelle, Hausentscheidung, was man für Umgebungen hat und wo man das testet und dann live setzt. Würde ich mal sagen optional, wäre aber in der Entscheidung von

IT. „GDPR conform“ natürlich, auf jeden Fall.

M: Ein must have?
B: Ein must have auf jeden Fall.

M: Das gleiche wie mit KYC compliant bezüglich, wenn es nicht GDPR conform ist, dann ist es auch nicht einsetzbar, somit ist es auch mandatory.
B: Ja genau, vor allem bei GDPR gibt es sehr hohe Strafrahmen, wenn man es nicht einhält. Das heißt, es ist ganz wichtig, Datenschutz. Und noch dazu von natürlichen Personen und die persönlichen Daten. Ganz wichtig. „Database usage for KYC checks“ dass verstehe ich jetzt nicht ganz.

M: Kein Problem. Bei KYC Checks gibt es ja einen PEP Hit, oder gibt es keinen PEP Hit. Dass muss man ja quasi auch abdecken. Mit KYC Check ist gemeint es gibt Anbieter, die haben eigene Datenbanken zu Personen, zu Political Exposed Persons auf der ganzen Welt. Es gibt aber auch in Österreich im Compass, wo man die Personen ansehen kann. Und jetzt ist die Frage, wenn ein Tool so eine Datenbank integriert hat, ist das wichtig oder zum Beispiel inhouse hat man seine eigenen Sanktionslisten wo Personen versorgt sind.
B: Naja, ich bin jetzt ein wenig verwirrt, warum hier mandatory steht. Weil normalerweise, die Beispiele die du gebracht hast, sind in der Compliance Abteilung und da gibt es bestehende Liste gegen die gecheckt wird. Es gibt Sanktionslisten, es gibt PEP Listen, es gibt Whitelisten, es gibt OFAC Listen, etc. wogegen die Personen auch gematched werden. Warum sollte das jetzt ein Provider mit anbieten? Ich mein er kann es anbieten?

M: Weil es beispielsweise globale Listen gibt.
B: Ich weiß, aber normalerweise haben die Compliance Abteilungen schon ihre eigenen und tun diese sehr, sehr selten gegen andere einfach austauschen. Also das merke ich auch im Rahmen eines KYC Projektes. Da gibt es auch sehr viele Vendoren, wenn es darum geht den KYC Prozess zu automatisieren, zu digitalisieren. Also einen Orchistration Layer zu bauen. Da gibt es Vendoren die auch bereits solche PEP Checks, Sanktionschecks mitbringen und meine Erfahrung ist immer, dass da Compliance Abteilung immer relativ schnell abwinken und sagen danke dass interessiert uns nicht. Wir haben unsere eigenen Riskprüfungen, unsere eigenen Listen wogegen wir prüfen.

M: Die internen, die ihr selbst aufgebaut habt?
B: Die internen, selbstverwalteten, aufgebauten wo man prüft. Also das ist meine Erfahrung die ich gemacht habe, mit den Compliance Abteilungen wo ich zu tun hatte, wo ein Vendor gekommen ist und gesagt hatte, wir können auch das abdecken hat es immer geheißen nein, wir haben unsere eigenen, aber wir möchten uns gerne ansehen, was auf der KYC Seite angeboten wird.

M: Warum es mandatory ist, weil du natürlich identifizieren musst ob es eine Political Exposed Person gibt, oder nicht bei dieser Identifizierung. Das ist mit mandatory gemeint. Man muss verpflichtend überprüfen ist der Kunde ein PEP oder nicht. Aber ob es jetzt gegen die internen Datenbanken inhouse Solutions oder gegen die vom Vendor ist nicht mandatory. Der Check an sich ist mandatory. Dann sind wir bei „Data storage“.

B: Ja aber das ist dass was wir vorher besprochen haben. Die Ablage von diesen Screenshots und von den Sprachen, ist dass das gemeint?

M: Generischer denken. Eigentlich geht es Hand in Hand mit GDPR, also Datastorage. Weil du personenbezogene Daten auch Ablegen musst. Die müssen zum Beispiel in der Bank mindestens 13 Jahre aufbewahrt werden, mit Exceptions geht es auch länger und wenn du dir jetzt einen Vendor aussuchst und der speichert die Daten außerhalb der EU, wäre schwierig.
B: Ich weiß dass sind diese Thematiken mit Cloudspeichern, außerhalb der EU. Das ist diese ganze Facebook etc, Geschichte mit GDPR. Ok so ist das gemeint. Wo der Vendor die Daten speichert, ob er das in seiner eigenen Cloud hat, außerhalb der EU, etc. Optional? Würde ich jetzt nicht ganz als optional sehen, muss ich ganz ehrlich sagen. Das ist jetzt schon eine sehr wichtige Information. Wo er das abspeichert und wo nicht. Ich versuche jetzt herauszufinden, was optional und was mandatory ist.

M: Mandatory heißt das Kriterium muss erfüllt sein, damit man das Ident Tool verwenden kann.
B: Also wenn ich mir so ein Tool ansehe, vom Kriterium her und ich sehe dass das außerhalb von der EU abgespeichert wird, dann kann ich nicht einfach sagen, ja passt, ist mir egal, sondern das ist ja dann ein Konflikt mit GDPR Richtlinie. Es wäre ein no go defacto. Sich dann zu entscheiden, wenn dieser Vendor sagt, er speichert das nur außerhalb der EU. Außer man einigt auf, weiß ich nicht, dass die Speicherung hier erfolgt, also inhouse.

M: Also eigentlich ist das ein Mandatory Kriterium?
B: Hätte ich schon so gesehen. Zumindest meine Meinung.

M: Weil es Hand in Hand mit GDPR geht.
B: Ja korrekt, also so sehe ich das zumindest.

M: Du hast es schon angesprochen. „Cost effectiveness“. Damit ist gemeint, wenn du beispielsweise den Videoidentifizierungsprozess outsourced, was kostet dich das beim Provider. Zahlst du pro Identifikation, zahlst du eine Flatrate, quasi bis zu 1000 Kunden pro Monat kannst du verifizieren lassen?
B: Das ist schon wichtig, die Kosten. Man muss ja wissen mit welche Kosten man rechnen muss. Man hat ein Budget und dann muss man natürlich berechnen wie viele Fälle kommen rein. Zahlt man pro Fall, oder hat man eben auch eine Flat Fee. Also so wie ich es kenne, wir zahlen pro Fall und es gibt auch noch eine Flat Fee. Also eine Gesamtsumme und dann pro Fall. Aber die Gesamtsumme übernehmen nicht wir die Kosten, sondern wir zahlen wirklich pro Stückzahl. Aber natürlich haben wir auch, nachdem wir nicht nur unser Haus abdecken, sondern auch andere für die wir es machen SLAs natürlich. Wo die Kosten dann auch gegengerechnet werden.

M: Last but not least ist die “Platform dependency”. Da geht es darum, wo ist dieses Tool, diese Software für den Kunden aufrufbar. Ist es nur am Laptop möglich, oder ist es am Handy/Tablet auch möglich. Wie wichtig ist das aus deiner Sicht?
B: Also wenn ich jetzt von Customer Experience sprechen und jetzt in die Richtung denken

wo wir uns hinbewegen mit Automatisierung und Digitalisierung, fände ich es schon wichtig, oder ein wichtiges Kriterium. Dass der Kunde das auch multifunktional nutzen kann. Nicht nur am Laptop, sondern auch am Handy, aber auch dass es userfriendly ist. Nicht dass man wenn man am Handy einsteigen will, fünf Hände braucht um etwas eingeben zu können. Es muss so simple wie möglich sein, auch für den Kunden. Aber ich fände es schon gut wenn es mit mehreren Devices möglich wäre.

M: Also Platform unabhängig.
B: Ja genau.

M: Welche Kriterien fehlen im Katalog?
B: Du hast eigentlich alles angeführt. Was mir noch eingefallen wäre, in wie weit man abhängig von einem Vendor sein muss in Zukunft. Und ob man sowas nicht dann auch selber anbieten kann, oder selber machen kann.

M: Abhängigkeit zum Vendor. Wenn eine eigene Software gebaut werden könnte?
B: Zum Beispiel. Aber ich weiß nicht, ob das jemand für sich selber wirklich machen, oder anbieten würde. Also mir fällt jetzt nichts mehr ein. Es sind die Kosten abgedeckt, die Sprache, Agent.

M: Das ist ja auch schön, wenn etwas gut recherchiert ist, wenn man etwas braucht und was nicht. Wo sehen Sie Probleme mit dem Kriterienkatalog?
B: Naja Probleme, nicht jeder Vendor wird alles abdecken. Das heißt der eine oder andere wird vielleicht unterschiedliche Kriterien nicht erfüllen. Es kommt halt immer darauf an, was der Vendor anbietet und welches Gesamtpackage auch passt. Die Hauptkriterien die man braucht, dass diese auch erfüllt sind. Weil wenn ich einen Vendor habe und ich sage ich habe fünf Fixpunkte, die unbedingt erfüllt sein müssen und er kann aber nur zwei liefern, dann wird er wahrscheinlich nicht in Frage kommen.

M: Ich überlege selbst noch. Wir könnten noch ganz kurz darauf eingehen. Ein Problem könnte sein, du weißt wie die Call Agents ausgebildet sind. Wie die im Umgang mit dem Kunden sind.
B: Ja das stimmt. Das ist dass, was wir auch schon angesprochen haben. Dieser Customer Service, nehme ich einen Agent, nehme ich ein Call Center, oder mache ich es inhouse und liefere ein besseres Service. Wo die Leute auch dementsprechend trainiert werden und Sprachen abdecken. Oder verlasse ich mich auf ein Call Center, wo ich nicht weiß wie die Fluktuation aussieht, ich nicht weiß wie das Training aussieht. Da werde ich nur darauf kommen, wenn sich natürlich die Beschwerden häufen, dass irgendetwas nicht passt.

Transcript Gamma

Interviewer: Markus Wasserbauer (M)
Interviewee: Gamma (G)
Date: 27.09.2021
Point of presence: The interview has taken place physically

M: Welche Position haben Sie im Unternehmen? G: Ich bin Head of Corporate Customers Mid-Office. Brauchst du Details?

M: Was deckt die Abteilung ab?
G: Hauptsächlich bzw. der größte Teil meiner Mitarbeiter deckt Sales Support ab. Die sprechen mit dem Kunden im täglichen Leben, wenn dieser Probleme mit dem Konto hat, oder mit der Videoidentifikation, oder wenn er Identifiziert werden muss. Wer das übernimmt, wer sind die Zeichnungsberechtigen, Konto Änderungen, etc. Was haben wir noch? Was wir noch tun ist, wir kümmern uns um die „Run Projekte“ in der Bank, nicht die „Change Projekte“. Das heißt alle Dinge die bei uns reinlaufen zu optimieren, Prozesse optimieren, alles was regulatorisch ist und uns aufgedrückt wird sozusagen und diese Dinge auch umzusetzen und im gesamten Bereich auszurollen. Dann haben wir noch den sogenannten Transaktionalendesk. Hier kümmern wir uns um das Kommodity Geschäft. Vor allem arbeiten wir mit den Oil&Gas, Metals&Mining und Agricultural Kommodity Kunden zusammen. In den unkommentierten Linien sehen sie sich Dokumente an, machen Releases, etc,etc. Also das haben wir auf der Seite. Aber wie gesagt der größte Teil ist, alles was mit Sales Support zusammenhängt.

M: Wie wichtig ist das Thema Onboarding und darüber hinaus die Videoidentifikation von Kunden in Ihrem Finanzinstitut?
G: Also Onboarding ist einer der wichtigsten Prozesse, natürlich. Erst einmal hat es den Aspekt der Customer Experience. Wie super sind wir im Onboarding. Das ist der Eintritt in das Unternehmen. Da sieht er uns das erste Mal, lernt uns das erste Mal kennen und hat einmal gleich das erste Feeling wie läuft es eigentlich, wie läuft es nicht. Natürlich ist es für uns wichtig den Kunden onzuboarden und das erste Produkt mit dem Kunden zu haben. Das ist wirklich wichtig. Videoidentifikation hat in Zeiten von Covid-19 und Home Office noch wesentlich mehr Bedeutung bekommen. Weil die Leute ja nicht mehr durch die Gegend reisen und Menschen treffe und Passkopien sehen. Persönliche Identifikation ist natürlich in gewissen Zeiten fast nicht möglich gewesen. Was gibt es für alternativen? Alternativ ist eine notarielle Beglaubigung, aber so eine dass wir diese auch akzeptieren können, nach dem Österreichischen Gesetzt. Das heißt wirklich du musst die Person getroffen haben und du musst auch den Pass gesehen haben und das Beides muss übereinstimmten. Und da ist es eben nach der neuen Verordnung, oder nach dem Rundschreiben der FMA die Videoidentifikation zum Tragen gekommen. Wir haben es in Österreich relativ streng umgesetzt. Du darfst derzeit nur Audioaufzeichnungen machen, aber keine Videoaufzeichnungen. Das ist wichtig, denn im Gegensatz zu den Deutschen, diese machen auch Videoaufzeichnungen. Die müssen auch archiviert und weggespeichert werden. Bei uns ist es immer noch nur Audio. Es hat immer geheißen Video kommt noch, habe aber bis jetzt nichts davon gehört. Aber Videoidentifikation wie gesagt, ist bei uns extrem wichtig in Zeiten wie diesen. Kunde die wir wahrscheinlich auch nie treffen werden. Wir haben zum Beispiel einen großen Ölkunden, der die ganze Administration in China hat und die werden wir nie treffen. Aber die dürfen halt Zahlungen freigeben, etc. und das ist natürlich super praktisch.

M: Somit kommt man dann auch ein bisschen nach Übersee und kann ganz andere

Kunden akquirieren. (Zusatzkommentar)
G: Wie gesagt nach Übersee kommen wir auf jeden Fall. Überall wo wir eine Netzwerk Units, wo wir eine Repräsentants haben und so weiter und sofort. Aber wichtig ist, dass wir da nicht nur wegen so etwas hinreißen müssen. Und in manchen juristischen Zonen wie Vereinigte Arabische Emirate etc. gibt es das Prinzip des Notars gar nicht. Das heißt es braucht eine beglaubigte Passkopie ihres Außenministeriums und das ist gar nicht so einfach. Da muss man hingehen, den Pass vorlegen, oder in unsere Botschaft gehen, aber bei uns machen das natürlich nicht mehr alle Botschaften auf dieser Welt. Und noch dazu gibt es in Dubai keine Botschaft. Dann müssen sie extra nach Abu Dhabi reisen und dort gibt es auch nur einen Repräsentanten, oder sozusagen eine Außenhandelsdelegierten. Also wie gesagt das ist nicht so einfach heutzutage diese Identifikation umzusetzen.

M: Wird der Videoidentifizerungsprozess ausgelagert (warum/warum nicht)?
G: Also das haben wir uns einmal sehr genau überlegt. Wir haben gesagt ja, man könnte es auslagern. Man kann dann einfach sagen, man schickt den Kunden zu IDnow und hat das Ding. Oder wir hätten sagen können, wir machen jeden Kunden selber und programmieren uns eine Software bzw. wir machen es so wie wir es jetzt machen. Warum haben wir uns dafür entschieden? Wir haben uns dafür entschieden eine Software zu kaufen, zu nutzen, bei uns Leute auszubilden als Identifikationsagents. Die haben nach dem „Train the Trainer“ Prinzip andere ausgebildet und werden geschult auf dieses System. Warum haben wir uns dafür entschieden es selbst zu machen? Unsere Kunden sind jetzt keine privaten Personen, sind keine Retail Kunden, sondern sind große Konzerne. Bei den großen dieser Welt, wer ist da oft zu identifizieren? Die Direktoren, der CEO, der CFO, usw. Wenn ich sie nun an IDnow schicke, unterscheidet das Call Center nicht wer diese Person ist. Und dann schicke ich den CFO eines großen Konzerns, oder eines großen Konzerns in West- oder Osteuropa dort hin und der wird dort behandelt wie irgendeiner von der Straße, wo der sich vielleicht einen kleinen Kredit aufnehmen will um einen Fernseher zu kaufen und der IDnow Mitarbeiter wirklich darauf trainiert ist, hier einen Fraud zu verhindern. Wir kennen diese Personen in dem Sinne, dass wir wirklich wissen, das ist der CFO, CEO, Director oder was auch immer in diesem Unternehmen. Mit dem haben wir in den meisten Fällen vielleicht schon gesprochen und wir wollen den dort nicht in einer Warteschlange sitzen haben für 10 Minuten, 20 Minuten. Ich habe mit einem großen Deutschen Anbieter das selbst ausprobiert, wo ich mir auch eine QES zusätzlich geholt habe und bin 20 Minuten in der Warteschleife gehangen. Dann hat der Prozess nochmal fast eine Stunde gedauert

M: Nur die Videoidentifizierung?
G: Die Videoidentifikation mit nachher angehängter qualifizierten E-Signature zu bekommen. Aber das hat über eine Stunde gedauert. Bei uns dauert die Videoidentifizierung maximal, also wirklich maximal 20 Minuten. Und dann ist natürlich die Frage Auslagerung, Daten, Drittanbieter, etc. Das müsste man halt auch noch mal alles regeln. Aber wie gesagt bei uns machen dass die KYC Mitarbeiter gemacht, die sowieso in einer high-sensitive und vertraulichen Area arbeiten. Jetzt machen es die Kollegen aus dem Account Processing. Die wiederum natürlich auch mit diesen Personen zu tun haben

bzw. auch natürlich hochsensible Daten verarbeiten und daran sowieso gewöhnt sind. Wie gesagt wir haben uns dazu entschieden das bei uns zu machen, weil wir dadurch ein wesentlich besseres Customer Service bieten können und der Kunde dafür auch nichts bezahlt und wir den durchleiten von Anfang bis Ende. Wir machen einen individuellen Termin aus, wenn der Kunde zeit hat. Nicht der ruft dort an und wartet einmal. Also wir sagen ihm „Lieber Kunde wann hast du Zeit, wir machen den Termin aus“. Dann machen wir das auch und dann führen wir ihn auch durch bis zum Ende. Wie gesagt wir haben uns dann ja auch später dafür freischalten lassen, dass wir die Videoidentifikation weiter in einem Prozess machen, mit verpassen einer qualifizierten E-Signature. Also das ist natürlich schon ein großer Vorteil. Wir sind so ein Center, was so eine qualifizierte elektronische Signatur verpassen kann.

M: Ein Trusted Service Provider so zu sagen?
G: Ja genau und es kostet dem Kunden nichts extra.

M: Für welche Produkte wird die Videoidentifikation eingesetzt?
G: Für jedes. Es ist egal für welches Produkt. Onboarding in dem Sinne ist in unserem Unternehmen ein bisschen etwas anderes. Onboarding für einen Corporate heißt mehr die Identifizierung des Unternehmens und seiner Eigentümer. Aber das heißt noch nicht das ich den Eigentümer persönlich identifizieren muss. Ich muss denjenigen persönlich identifizieren der mir gegenüber auftritt. Das heißt als Vertretungsbefugter, Zeichnungsberechtigter oder sonst irgendwie autorisierter Auftritt. Der mit uns eine Geschäftsbeziehung eingeht, oder Verträge unterschreibt. Die muss ich persönlich identifizieren und das sind Vertreter eines Unternehmens. Wir haben jetzt nicht keine natürliche Person als Kunden, sondern die natürlichen Personen treten bei uns immer im Zusammenhang mit einem Unternehmen auf. Hinter dem Unternehmen steht immer eine Person und die Customer Experience dieser Person ist genau so wie deine oder meine. Also wenn ich mich irgendwo anmelde, dann ist die Usability wichtig. Wie werde ich durch den Prozess begleitet? Wie erfülle ich den ersten Kontakt mit der Bank? Der erste Kontakt ist der Kundenbetreuer. Der bannt das Geschäft an, etc. Aber dann geht es halt in den ersten Prozess mit uns. Da ist halt der Onboarding Prozess extrem wichtig. Da haben wir riesengroße Pain Points. Nicht mit der Videoidentifikation, aber mit dem KYC Prozess.

M: Und die Videoidentifizierung ist ja nur ein Teil des Onboardings.
G: Es ist in diesem Falle nur ein kleiner Teil. Bei einer natürlichen Person, besteht der KYC Prozess hauptsächlich oder zu einem sehr großen Teil aus der Videoidentifikation oder Identifikation. Bei einem Corporate Kunden hängt da ganz viel noch dahinter. Die komplette Eigentümerstruktur, die Verifikation der Eigentümerstruktur, die Herkunftsprüfung. Da hängen ganz viele Dinge dran, aber wie gesagt die Personen die wir im Zusammenhang mit Corporate Kunden oder Firmenkunden identifizierten sind immer Vertreter des Unternehmens in irgend einer Form.

M: Gibt es eine Alternative zur Videoidentifikation?
G: Du hast verschiedenste Möglichkeiten. Du kannst die Person selbst treffen, die Person sehen und den Pass ansehen. Du kannst dich eines qualifizierten Dritten bedienen.

Das wären Notare, Anwälte und Wirtschaftsprüfer. Was halt nicht gibt in Dubai. Ein Anwalt in Dubai ist kein qualifizierter Dritter. Bei uns sind Anwälte, Notare und Wirtschaftsprüfer eigentlich nur aus dem EWR qualifizierte Dritte. Also würde es das Prinzip des Notars in Dubai geben, könnten wir den gar nicht zulassen. Er könnte zum Beispiel zu einer Niederlassung einer Europäischen Bank gehen und sich dort identifizieren lassen und diese bestätigt uns diese. Ist aber oft schwierig. Weil wenn es nicht ihre Kunden sind, warum sollten sie das dann machen? Wir haben noch die Möglichkeit das über die Wirtschaftskammer zu machen. Wobei es aber dort keine Niederlassung gibt. In manchen Destinationen ist die Videoidentifikation fast unsere einzige Möglichkeit bzw. tatsächlich dort hinzureisen und den Pass und die Person anzusehen.

M: Was natürlich viel mehr Aufwand und Kosten bereitet, wie einfach Videoidentifizieren.
G: Natürlich, wenn ich mir ansehe, wir haben eine Repräsentanz in Bejing, aber ist der Kunde irgendwo anders in China, China ist ja riesengroß, wenn der nicht in der nähe ist, dann kann unser Repräsentant nicht ganz China abreisen. Es spart uns unheimlich viel Geld.

M: Videoidentifizierung spart Geld. Das ist ein Vorteil wo Videoidentifizierung einen Mehrwert bringt, im Gegensatz zum physischen treffen. Welche Vorteile hat die Videoidentifikation und warum wird diese in Ihrem Institut eingesetzt.
G: Wir sparen Reisekosten, wenn wir nicht sowieso dort hinfahren, dann würde ich nicht extra hinfahren müssen. Wir bieten dem Kunden ein Service, das relativ schnell geht, dass ich jederzeit machen kann. Völlig nach seinem Wunsch. In der Früh, am Abend. Die Identifikation, wenn der Kunde es freigibt, können wir sie auch mit anderen Banken teilen. Das heißt er könnte mit uns einmal machen und wir dürfen, wenn er es uns erlaubt, auch seine Daten weitergeben. Überall dort wo die Juristik Videoidentifikation das zulässt. Es schon auch Audit Proof. Es ist ein System. Es ist weggespeichert, es gibt ein File dazu und es gibt ein Audiofile dazu. Also wir können zu 100% bestätigen, dass wir ihn identifiziert haben. Weil sonst könnte man auch sagen, wenn man davon ausgeht, dass jemand das System missbrauchen möchte, der schickt mir seinen Pass und ich habe den vor 100 Jahren einmal gesehen, dann gebe ich meinen Stempel drauf. Ich sage das könnte gemacht worden sein, oder könnte irgendwo jemand gemacht haben. Weil es einfach und schnell ist. Aber mit der Videoidentifikation hast du einen Nachweis, es ist 100% Audit Proof und natürlich für die Aufsicht nachweisbar und es gibt das Audiofile. Die Software hat ganz bestimmte Merkmale. In Deutschland darfst du sogar biometrische Daten abmessen. Das ist bei uns nicht erlaubt. Dass kannst du nur zur Ergänzung hinterher machen. Aber das hat auch noch einen super Effekt. Es gibt gewisse biometrische Daten, die sich im Laufe des Lebens einer Person nicht verändern. Nur im Verhältnis. Also die Abstände zwischen den Augen, die Abstände zwischen Nase und Kinn. Das verändert sich und dass kann man berechnen. Aber am Ende des Tages verändert sich das Gesicht nicht komplett. Echt fälschungssicher. Ich würde nicht sagen fälschungssicherer, weil man eine natürliche Person treffen und einen Pass in der Hand zu haben hat auch etwas für sich. Aber es ist schon sehr gut heutzutage. Dass da jemand nur ein Bild hinhält, oder das ganze System austrickst ist schon unwahrscheinlich. Vor allem in der Corporate

Welt. Ich sage einmal bei einem Enduser, gibt es sicher noch Programmiermethoden oder irgendwelche IT Lösungen, die das austricksen können. Aber in der Corporate Welt ist das sehr unwahrscheinlich.

M: Das war jetzt ein Beispiel für die Retailwelt, wo wirklich nur eine Person dahinter steht.
G: Genau und wo es natürlich schon auch Hacker gibt. Da wird ein Videobild eingespielt und eine Stimme eingespielt. Da gibt es vieles.

M: Deepfakes zum Beispiel.
G: Ja, also da gibt es schon ganz viele Dinge. Aber es wird ja auch maschinell die Nummer vom Pass eingelesen. Die bedeutet ja was, diese Abfolge der Nummer. Die wird ja abgelesen und wenn das in irgendeinem Land nicht zum Sample passt, dass hat schon einen riesen Wert.

M: Wie haben Sie das richtige Videoidentifikationstool für Ihre Organisation ausgewählt?
G: Wir haben uns zwei, drei angesehen. Ich kann mich nicht mehr 100% erinnern, wie die Kriterien oder wie der Kriterienkatalog war. Was nicht so ideal gelaufen ist, wir dachten bei uns wäre das verarbeiten von biometrischen Daten, das lesen des Gesichts, das Abmessen ok. Das haben die uns quasi mitverkauft. Das war aber nur in Deutschland ok und in Österreich nicht. Es gab in Österreich damals noch nicht so einen riesengroßen Anbieter wie IDnow. Die haben das schon eine Zeit lang gemacht. Die waren kein komplettes Start-Up. Das war uns auch wichtig, dass die schon viel Erfahrung damit hatten. Und wir haben auch jemanden gebraucht, der uns hier ausbilden kann. Es ist nicht jeder bereit seine Software zur Verfügung zu stellen, die dann von jemanden Artfremden sozusagen genutzt wird. Also das waren schon Kriterien für uns. Kosten waren natürlich Kriterien, aber all diese Anbieter die erfüllen alle die regulatorischen Erfordernisse. Die erfüllen alle den Support der Dokumente, den Support der Jurisdiktionen. APIs, KYC Compliant, also alle diese Kriterien erfüllen alle diese großen Anbieter. Also haben wir gesagt, wir bauen uns gar nichts selber. Das ist total sinnlos, weil das gibt es. Die entwickeln das ja auch laufend weiter. Nicht nur für uns, sondern für die ganze Welt. Die haben begonnen mit einer gewissen Liste an Ländern und Dokumenten. Nicht jedes Land, jedes Dokument ist zulässig und das haben sie uns damals auch gesagt. Da gab es einen ganz klaren Plan, wie sie das ganze erweitern werden, wie die Entwicklung ist. Sie haben damals sehr gut präsentiert. Sie haben uns mehr verkauft, als notwendig ist. Sie waren wahrscheinlich damals der most advanced Anbieter und erfahren.

M: Für die EU zumindest, für Österreich?
G: Für die EU auf jeden Fall, aber sie haben ja nicht nur EU gehabt. Also es waren schon wesentlich mehr Nationen zulässig und in ihrem System hinterlegt. Wir haben damals gesagt, was ist für uns ganz wichtig? Das sind einmal alles unsere Netzwerkunit Länder.

M: Das sind quasi Kriterien jetzt, die euch wichtig waren.
G: Genau und da haben sie gesagt die können wir jetzt gleich umsetzen, und dann weitere und weitere. Also da haben sie schon relativ einen klaren Plan gehabt, welche da drinnen sind und welche sie schon können. Wir haben dann gesagt wir werden dann noch dieses

und jenes Land brauchen. Da haben sie sich dann erkundigt und gesagt dass werden sie zu dem und dem Zeitpunkt können. Also da waren sie sehr kooperativ und das hat gut funktioniert.

M: Welche Kriterien spielten eine Rolle? Du hast es jetzt schon kurz angesprochen, das größte Kriterium war jetzt wahrscheinlich Länderabdeckung?
G: Länderabdeckung, Erfahrung, wie leicht ist es das bei uns zu implementieren und wie leicht ist es für uns als interne User das Tool zu bearbeiten. Weil da musst du schon geschult werden auf das. Da musst du hier klicken und da klicken, dann bekommt der Kunde einen SMS Code. Den soll er dann irgendwo eintippen. Wenn er den Code eingetippt hat, dann scheint auf der anderen Seite ein grünes Licht auf. Es war schon ganz wichtig das die Usability passt, für den Kunden, aber auch für uns. Zu allererst für den Kunden, aber auch für uns.

M: Hilf Ihnen der bereitgestellte Kriterienkatalog bei der Suche nach dem Videoidentifikationstool, das Sie für Ihre Organisation benötigen würden?
G: Also „Condition for video based identification in Austria“ das muss sowieso gegeben sein. Aber es gibt eine Europäische Direktive dazu. Aber in Österreich hat sie ein paar Extrapunkte. Das System muss individualisierbar sein, das ist wichtig. Nicht nur Identification in Austria. Für uns war es wichtig, auch für unsere Netzwerkbanken zu individualisieren. Wir haben es ja nicht nur bei uns in Österreich, wir nutzen es ja auch für Retail auch überall in den Netzwerkbanken wo es schon zulässig ist. Also da war ganz wichtig dass es auf jede Jurisdiktion angepasst werden konnte. „Country support“ natürlich. Je mehr Countries umso besser. „Document support“ natürlich. Je mehr sie können, umso besser. Es gibt nur eine gewisse Anzahl an Dokumenten. Da gibt es eine Seite die heißt PRADO von der EU und da steht genau drinnen, welche Dokumente quasi die Merkmale gemäß der EU Richtlinie erfüllen. Kippeffekte, Sicherheitsmerkmale, Wasserzeichen und so weiter. Also da gibt es nur maximum Anzahl an Dokumenten. Die müssen sie halt abdecken. Je mehr desto besser. „Language Support“ ist für uns besonders wichtig.

M: Achtung da geht es um den Language Support von den Tools an sich.
G: Das ist mir schon klar. Das Tool muss gewisse Sprachen und Zeichen können. Nicht nur Language, sondern auch Zeichen. Wenn du mit dem Kunden sprichst, oder gewisse Zeichen drinnen hast, dann muss das Tool, diese Zeichen, wie ich sage jetzt mal was kyrillisches vielleicht. Oder vielleicht im Namen ein Accent, oder in den Nordics die verschieden Buchstaben, dass muss es supporten können. Und natürlich auch auf der Kundenseite. Wenn der Kunde sich die App installiert, dann will er sich in seiner eigenen Sprache.

M: Quasi wenn sie nur in Englisch wäre, für einen türkischen Kunden
G: Dann kann er vielleicht Englisch, aber vielleicht auch nicht ausreichend Englisch. Es muss die App die Language supporten. Und dann natürlich auch in der Sprache das ganze System, die ganze Durchführung durch das System.

M: Weil es ist ein sensibler Prozess mit sensiblen Daten.

G: Genau. Das heißt du musst aber auf der anderen Seite, da kommen wir zum nächsten Punkt, ist der „Call Agent Support“. Der Call Agent muss sicherstellen, dass er gewisse Sprachen kann. Was haben wir gemacht? Wir haben gesagt die wichtigsten sind Englisch, Deutsch und Russisch. Wir haben in IDnow Russisch nicht sofort drinnen gehabt. Ich weiß nicht ob wir es inzwischen drinnen haben. Aber wir haben die Videoidentifikation teilweise dann dem Kunden schon in Russisch erklärt. Und das wurde auch gut aufgenommen. Aber das ganze System und die App läuft auf Englisch. Aber wenn der Kunden nicht verstanden hat, was wir auf Englisch gesagt haben, mussten wir auch russische Agents dahinter setzen. „KYC Compliant“ das ist für mich jetzt die Frage, was meinst du damit? Das muss Gesetzeskonform und Prozesskonform sein. Wie es in den Regulatorien steht.

M: In dem Sinn ist mit „KYC Compliant“ gemeint, dass zum Beispiel bei der KYC Regulation, dass ist ja eine Regulierung, sprich die wird nicht in National Law umgesetzt, sondern ist von der EZB direkt vorgegeben. Also die eIDAS.
G: Aso, das meinst du. Das nenne ich natürlich nicht KYC Compliant. Das würde ich KYC Compliant nennen, sondern Gesetzeskonform, oder EU Konform. KYC ist für mich ein bisschen was anderes. Da hätte ich jetzt eher gesagt Gesetzeskonform, bzw. entspricht der eIDAS.

M: Genau , sprich bestes Beispiel was du gesagt hast, die Provider müssen Trust Services sein in der EU. Sprich sie müssen qualifiziert sein eine QES oder E-Signature zu approven.
G: Wenn es hier um E-Signature geht ja, aber wenn wir keine E-Signature brauchen, sondern nur die Identifikation muss es nach dieser Verordnung zur Identifikation gehen. Und da gibt es eine von der FMA in Österreich und so weiter und sofort zur elektronisch unterstütze Identifikation. „API Support“ ist natürlich wichtig. Wir hätten uns das schon bei uns gewünscht. Das kann auch der Anbieter, nur unser Doxis konnte es nicht. Es hatte keine Schnittstelle. Damals ganz zum Beginn. Ich meine jetzt glaube ich dass es direkt ins Doxis ladet. Früher war es so, da mussten wir einen gesperrte Sharepoint Seite verwenden. Da wurde es angeliefert und wir mussten es dann hochladen. Zu Beginn das System konnte es, wir konnten es nicht. Aber das ist natürlich ganz wichtig. Was meinst du mit „Sandbox Support“?

M: Das kann ich dir kurz erklären. Normalerweise, wenn du eine API verwendest, brauchst du ein Testenvironment wo du die API testen kannst. Eine Sandbox gibt dir quasi eine Testumgebung/Produktionsumgebung wo du versuchen kannst herauszufinden wie mächtig die API ist. Du kannst ein wenig herumspielen, was das Tool kann. Das kann nicht jeder Provider. Aber normalerweise, wenn du eine API brauchst, geht das Hand in Hand mit der Sandbox. Weil die quasi dazu da ist zum testen.
G: Wir hatten eine Testumgebung. Aber nicht jetzt für die API, sondern für das ganze System. Also es gab eine Testumgebung und da konnten wir Herumdoktern und spielen und halt auch schulen. „GDPR Conform“ natürlich. Ich meine es muss alle Regulatorien spielen. Wir haben folgendes getan. Wir haben vor das System geschalten, unsere eigene Landingpage, wo der Kunde seinen Namen und Daten alles eingibt und sagt ja du darfst teilen, oder nein du darfst nicht teilen. Oder du darfst teilen mit und das ist unsere GDPR Klausel. Also das haben wir schon extra drinnen gehabt. Weil GDPR Konform,

das System teilt nicht. Das heißt es ist prinzipiell GDPR Konform.

M: Weil es In-House ist?
G: Also IDnow bietet das als Service an. Da bekommt nur der Kunde die Daten. That's it. Das ist GDPR Konform, also wenn das System so aufgesetzt ist. Das ist natürlich klar, das ist eine Grundvoraussetzung. „Database usage for KYC checks"

M: Sprich da geht es jetzt um PEP Personen, also Political Exposed Person zum Beispiel. Wie bekommt das Tool mit das zum Beispiel Herr so und so ein PEP ist?
G: Das war für uns kein Kriterium, ist auch keins, weil wir selbst unsere eigenen Checks machen. Als Bank bist du verpflichtet noch viel mehr als nur einen PEP check zu machen. Du brauchst advised media, du brauchst PEP, du brauchst wealth check, etc, etc. Das war für uns kein Kriterium. Das machen wir selber. Was sie für uns schon machen ist, wenn sie für uns prüfen, ob es schon mal auf einer Video ID Plattform einen Fraud Versuch unter diesem Namen gegeben hat. „Data Storage" war für uns auch kein Thema.

M: War das ein Service von IDnow?
G: Nein, die dürfen unsere Daten überhaupt nicht speichern. Die liefern sie uns nur an, da wird gar nichts gespeichert.

M: Ihr habt alles selbst in der Hand?
G: Wir haben alles selbst in der Hand. Das wollten wir auch gar nicht. „Cost effectiveness" natürlich es musst cost efficient sein. Für uns völlig klar. Es muss für uns in einem gewissen Verhältnis stehen. Allerdings ist es so dass wir es Kunden nicht weiter verrechnen, sondern als additional Service verstehen.

M: Ja, bei „Cost effectiveness" soll es eher darum gehen, wenn man Videoidentifizierung as a Service verwendet. Sprich wenn man einen Third Party Anbieter hat, muss man wahrscheinlich pro Identifizierung, pro 100 Identifikationen, etc. zahlen.
G: Wir haben einen fixen Vertrag. Ich weiß jetzt nicht mehr wie der Vertrag ausgehandelt wurde, das kann ich dir nicht sagen. Aber natürlich brauchst du eine gewissen Turnaround, dass es sich auszahlt. Nur wir haben gesagt, es muss für uns keinen Break-Even geben. Der Kunde zahlt 5€ für die Identifikation und wir zahlen davon 3,50€ und dazwischen ist auch noch der Service. So sehen wir das nicht. Wir sehen das als Benefit for the customer. Als spezielles Service am Kunden und natürlich über Umwege rechnet es sich wieder, wenn man nicht reisen, etc. muss. Aber so die direkt proportional oder im direkten Zusammenhang haben wir das nicht gerechnet.

M: Last but not least wäre gewesen "Platform dependency".Das heißt zum Beispiel, ist es für euch wichtig dass der Kunde die Identifizierung über das Handy machen kann, mit dem Laptop, dem Tablet. Spielt das eine Rolle?
G: Zu Beginn haben wir uns gedacht, wir brauchen unbedingt die Möglichkeit das am Handy, Tablet und am Computer zu machen. Dann sind wir darauf gekommen, dass die meisten Firewalls des Kunden das nicht zugelassen haben bzw. zum damaligen Zeitung wie wir das begonnen haben, haben die meisten Stand PCs gehabt, ohne Kameras. Das heißt du hättest das nie über deinen Stand PC machen können, weil du keine Kamera hattest. Oder du hast einen Laptop gehabt ohne Kamera. Also zu Beginn haben wir das

ein bisschen falsch eingeschätzt, mit es muss unbedingt am Computer funktionieren und am Handy und und und. Dann sind wir darauf gekommen, dass ist ein völliger Blödsinn und wir bieten es heute überhaupt nicht mehr über den Laptop an. Wir bieten es gar nicht mehr für den Browser an. Sondern wir bieten nur mehr die App über das Handy an und für das Tablet. Aber überhaupt nicht über den Computer, weil das gar nicht genutzt wurde. Vor allem war das Ganze wesentlich einfacher am Handy. Dann poppt da das SMS auf. Weißt du so wie, wenn du freigibst Paypal und dann erscheint automatisch die Nummer/SMS und du sagst nur confirm. Und die Kunden haben auch gar nicht großartig nachgefragt. Weil meistens hat es die Firewall überhaupt nicht zugelassen das zu machen bzw. wie gesagt hatten die Kunden keine Kameras. Heute ist das etwas anderes. Aber jeder hat inzwischen ein Smartphone mit Kamera, mit allem drum und dran und tausende Apps installiert. So gesehen war das für uns dann auch kein Thema. Prinzipiell hatten wir gedacht, wir brauchen es für alle Varianten. Dann hat es sich herausgestellt es ist ein völliger Blödsinn, weil der Kunde es gar nicht braucht.

M: Aber dann ist eigentlich die Plattformunabhängigkeit sehr wichtig, weil quasi das Handy ist eine eigene Plattform.
G: Also es ist wichtig dass es so easy wie möglich handlebar ist. Customer Experience ist einer der wichtigsten Dinge. Die Usability ist eines der wichtigsten Dinge und dass es auf jedem simplen Handy funktioniert. Nicht jeder hat einen Computer, dass ist auch heute noch so. Einen eigenen Computer sag ich mal.

M: Wir sind fast am Ende. Welche Kriterien fehlen im Katalog?
G: Also wenn man einen Anbieter nutzt, nicht so wie wir ihn nutzen. Sondern es einfach auslagert zu dem Anbieter, dann ist es wichtig dass die Personen dort freundlich, höflich und positiv sind. Das sie halt natürlich vor allem im direkten Kundenkontakt geschult, lösungsorientiert und dass die Personen die dort sitzen auch verstehen würden, mit wem sie es zu tun haben. Wie gesagt wir haben es dann nicht so gemacht, weil der Anbieter gesagt hat, der kann nicht unterscheiden ob der jetzt von der Bank als CEO kommt, oder von der Straße weg ist. Der klingt sich dort ein und los geht's. Aber wenn man es so nutzt wie es ist, ist es schon ganz wichtig dass das alles auch fälschungssicher ist. Nämlich fälschungssicher in dem Zusammenhang, dass dort nicht ein Mitarbeiter bereichert. Also bei IDnow ist es so, dass die Mitarbeiter die das dort machen, die sitzen in einem Raum, wo sie keinen eigenen Laptop haben. Wo sie auch ihr Handy nicht dabei haben dürfen. Wo sie ein Blatt weißes Papier und einen Bleistift haben, aber das dürfen sie nicht mitnehmen. Und all diese Dinge. Es muss auch ein abgeschlossener Raum sein, wo nicht jeder Zugang hat. Und natürlich auch das Video oder die Tonaufnahme muss abgesicherter Modus sein. Also höchste Sicherheitsstandards sind schon sehr wichtig. Also das müsste man vielleicht noch dazunehmen, dass die höchsten Sicherheitsstandards eingehalten werden. Und die Mitarbeiter wie die halt den Kunden behandeln. Da hängt wirklich sehr viel am Personal.

M: Wir kommen zur letzten Frage. Wo sehen Sie Probleme mit dem Kriterienkatalog? Du hast gesagt was dir fehlt, zum Beispiel die Personen müssen geschult sein, freundlich sein, das Auftreten quasi. Die Sicherheitsstandards bei der Durchführung müssen gegeben

sein. Aber wenn du jetzt quasi diesen Kriterienkatalog hernehmen würdest und anhand diesem versuchst Entscheidungen zu treffen, siehst du das eher kritisch oder sagst du das hilft?
G: Also uns war es sehr wichtig und was problematisch wäre, wenn wir nicht alle Länder abgedeckt gehabt hätten die wir brauchen. Das war einmal eine ganz wichtige Sache. Und Language Support. Wo uns gar nichts eingefallen wäre, das ein System nicht kyrillisch kann. Wir haben uns gedacht dass ist easy übersetzt. Aber das System dahinter zum Beispiel muss es auch können. Das darf man nicht vergessen. Also man darf jetzt nicht irgend ein veraltetes Kundenmanagementsystem anschließen. Was waren die Probleme im Kriterienkatalog? Also wichtig ist, dass sie relativ flexibel sind, die nächste Jurisdiktion aufzunehmen. Wir haben zum Beispiel irgend ein Land gehabt, dass war nicht drinnen. Dann haben wir gesagt, dass brauchen wir dringen. Das kommt ständig bei uns. Das müsst ihr da hineinbringen. Wir haben es dann bei uns mit Compliance abgestimmt. Und haben gesagt, liebe Leute von Compliance passt für euch dieses Land, ist es zulässig, sind die Reisepässe dort zulässig, gemäß Kriterienkatalog PRADO. Und dann haben wir gesagt so IDnow ihr müsst das implementieren. Das heißt es muss aber auch der Pass automatisch lesbar sein. Wenn du einen Pass liest und die Software ist nicht richtig eingestellt, dann liest er dir vielleicht die falsche Zeile ein. Das geht natürlich gar nicht. Der Prozess muss soweit wie möglich automatisch unterstützt sein. Nicht sehr viel tippen. Es gibt Kontrollschleifen, die müssen sein, die müssen extra getippt werden. Alles andere muss automatisch durchlaufen. Und eine Supporthotline fehlt mir. Eine super Supporthotline vom Anbieter. Nämlich für den Kunden ist einmal der erste wichtige und wenn du es so aufsetzt wie wir, dann brauchen wir eine super Supporthotline, einen VIP Service sozusagen. Also wenn du dann dort in einer Warteschleife hängst, während der Kunde in deinem Call hängt, hast ein Problem.

M: Das spielt sich auf die Customer Experience ab.
G: Also wie gesagt, hier eine der höchsten Kriterien Customer Experience.

M: Ich würde sagen Gamma wir sind fertig. Fast eine Punktlandung. Vielen vielen Dank!

List of Figures

List of Tables

Bibliography

[1] Ingrid Schirmer Julian Schmidt, Paul Drews. Digitalization of the banking industry: A multiple sakeholder analysis on stratecic alignment. https://aisel.aisnet.org/amcis2017/StrategicIT/Presentations/27/. Accessed: 2019-08-30.

[2] Otto Brauckmann. *Digitale Revolution in der industriellen Fertigung-Denkansätze*. Springer Vieweg, 2019.

[3] DerStandard. Rbi bekommt fma-strafe von 2,7 millionen euro zurück. *DerStandard*. Accessed: 2020-12-30.

[4] Dennis Kinyua. Kyc – client onboarding: Leveraging blockchain technology. *SSRN*.

[5] Sundareswaran, Sasirekha, Joe Louis Paul, Balakrishnan, and Swaminathan. Optimised kyc blockchain system. *IEEE*.

[6] Study on eid and digital on-boarding: mapping and analysis of existing on-boarding bank practices across the eu. https://op.europa.eu/en/publication-detail/-/publication/8da08249-49cd-11e8-be1d-01aa75ed71a1/language-en. Accessed: 2021-07-04.

[7] Statement by first vice-president timmermans, vice-president dombrovskis and commissioner jourovà on the adoption by the european parliament of the 5th anti-money laundering directive. http://europa.eu/rapid/press-release_STATEMENT-18-3429_en.htm. Accessed: 2019-06-24.

[8] Directive (eu) 2018/1673 of the european parliament and of the council of 23 october 2018 on combating money laundering by criminal law. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN. Accessed: 2021-03-04.

[9] Barbara Kitchenham, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey, and Stephen Linkman. Systematic literature reviews in software engineering – a systematic literature review.

[10] Regulation (eu) no 910/2014 of the european parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec. https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32014R0910. Accessed: 2020-01-11.

[11] Directive (eu) 2018/843 of the european parliament and of the council of 30 may 2018 amending directive (eu) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843. Accessed: 2020-01-11.

[12] Roy F. Baumeister and Mark R. Leary. Writing narrative literature reviews. *Review of General Psychology*, 1(3):311–320, 1997.

[13] Signotec e-signature solutions. https://en.signotec.com/. Accessed: 2020-09-01.

[14] Namirial trust service provider. https://www.namirial.com/de/. Accessed: 2021-02-19.

[15] Idnow. https://www.idnow.io/. Accessed: 2020-09-01.

[16] Fully-verified. https://fully-verified.com/. Accessed: 2020-09-01.

[17] Omri Ross José Parra Moyano. Kyc optimization using distributed ledger technology. https://link.springer.com/article/10.1007/s12599-017-0504-2.

[18] Ross P. Buckley Douglas W. Arner, Jànos Barberis. The emergence of regtech 2.0: From know your customer to know your data. *SSRN*.

[19] 10 biggest austrian banks according to their balance 2019. https://de.statista.com/statistik/daten/studie/288090/umfrage/banken-in-oesterreich-nach-ihrer-bilanzsumme/. Accessed: 2021-03-20.

[20] Ann Blandford, Dominic Furniss, and Stephann Makri. *Qualitative HCI Research - Going Behing the Scenes*. Morgan & Claypool, 2016.

[21] Stuart Bretschneider, Frederick J. Marc-Aurele, and Jiannan Wu. "best practices" research: A methodological guide for the perplexed. *Journal of Public Administration Research and Theory: J-PART*, 2005.

[22] Arnost Vesely. Theory and methodology of best practice research: A critical review of the current state. *Central European Journal of Public Policy*, 5:98–117, 2011.

[23] Online kyc providers: how to choose yours. https://justcoded.com/blog/leveraging-technology. Accessed: 2021-03-20.

[24] Lisa M Vaughn Melissa DeJonckheere. Semistructured interviewing in primary care research: a balance of elationship and rigour. *BMJ Specialist Journals*.

[25] The lamfalussy architecture. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/. Accessed: 2020-09-05.

[26] Committee of european banking supervisors. https://eba.europa.eu/. Accessed: 2020-10-18.

[27] Google scholar. https://scholar.google.de/. Accessed: 2020-09-11.

[28] Directive (eu) 2008/20/ec of the european parliament and of the council of 11 march 2008 amending directive (eu) 2005/60/ec on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:076:0046:0047:EN:PDF. Accessed: 2020-09-05.

[29] The united nations, office of drugs and crime. https://www.unodc.org/. Accessed: 2020-10-18.

[30] The history of anti money laundering directives in europe. https://www.anti-moneylaundering.org/Europe.aspx. Accessed: 2020-10-23.

[31] Introducing the 6th aml directive in 2021. https://complyadvantage.com/knowledgebase/eu-anti-money-laundering-directive/. Accessed: 2020-10-23.

[32] Directive (eu) 2015/849 of the european parliament and of the council of 20 may 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN. Accessed: 2020-01-11.

[33] Difference between kyc and aml. https://complyadvantage.com/knowledgebase/eu-anti-money-launder. Accessed: 2020-10-25.

[34] Jason Andress, editor. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, chapter 2, pages 23–38. Elsevier, 2011.

[35] Signicat. https://www.signicat.com/de/. Accessed: 2021-02-19.

[36] webid. https://webid-solutions.de/. Accessed: 2021-05-12.

[37] Youniqx. https://www.youniqx.com/. Accessed: 2021-05-12.

[38] Nect. https://nect.com/de/. Accessed: 2021-05-12.

[39] Id austria. https://www.oesterreich.gv.at/themen/dokumente_und_recht/id-austria.html. Accessed: 2022-03-02.

[40] eidas regulation. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation. Accessed: 2022-03-05.

[41] N. Sundareswaran, S. Sasirekha, I. Joe Louis Paul, S. Balakrishnan, and G. Swaminathan. Optimised kyc blockchain system. *2020 International Conference on Innovative Trends in Information Technology (ICITIIT)*, pages 1–6, 2020.

[42] Kyc-chain. https://kyc-chain.com/. Accessed: 2021-05-21.

[43] Kycstart. https://bitcoinmagazine.com/culture/deloittes-regtech. Accessed: 2021-05-21.

[44] Openid connect. https://openid.net/connect/. Accessed: 2021-07-09.

[45] Openid connect ekyc & identity assurance wg. https://openid.net/wg/ekyc-ida/. Accessed: 2021-07-09.

[46] Openid providers. https://openid.net/certification/. Accessed: 2022-03-05.

[47] Feedback from openid ekyc & identity assurance wg to the eidas regulation review. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe/F548976_en. Accessed: 2022-03-05.

[48] Electronic signature in e-governemnt in austria. https://www.bmdw.gv.at/en/Topics/Digitalisation/Digitised-Austria/Electronic-Signature.html. Accessed: 2021-05-15.

[49] Priya Seetharaman. Business models shifts: Impact of covid-19. *International Journal of Information Management*, 2020.

[50] Ris: Austrian pass law §11, §19. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005798. Accessed: 2021-05-12.

[51] Ris: Austrian driver licence law (fsg) §17a. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10012723. Accessed: 2021-05-12.

[52] Eps transaction. https://eservice.stuzza.at/de/e-identifikation-dokumentation/send/13-dokumentation/16-e-identifikation-pflichtenheft.html. Accessed: 2021-05-12.

[53] C. Baicu, I. Gardan, D. Gardan, and G. Epuran. The impact of covid-19 on consumer behavior in retail banking. evidence from romania. *Management and Marketing. Challenges for the Knowledge Society*, 15:534–556, 2020.

[54] Wan-Rung Lin, Yi-Hsien Wang, and Yi-Min Hung. Analyzing the factors influencing adoption intention of internet banking: Applying dematel-anp-sem approach. *PLOS ONE*, 2020.

[55] Eugene Bardach. Comment: The problem of "best practice" research. *Journal of Policy Analysis and Management*, 13(2):260–268, 1994.

[56] Eugene Bardach. The extrapolation problem: How can we learn from the experience of others? *Journal of Policy Analysis and Management*, 23(2):205–220, 2004.

[57] Gale, editor. *"Best Practices" Encyclopedia of Management 6th ed*, pages 40–41. Detroit:Gale, 2009.

[58] Arsen J. Darnay and Monique D. Magee, editors. *"Best Practices" Encyclopedia of Small Business*, pages 90–92. Thomson Gale, 2007.

[59] E. Sam Overman and Kathy J. Boyd. Best practice research and postbureaucratic reform. *Journal of Public Administration Research and Theory: J-PART*, pages 67–83, 1994.

[60] Edoardo Ongaro. A protocol for the extrapolation of 'best' practices: How to draw lessons from one experience to improve public management in another situation. 05 2021.

[61] Bonginkosi Gina and Adheesh Budree. A review of literature on critical factors that drive the selection of business intelligence tools. pages 1–7, 2020.

[62] Anil S. Jadhav and Rajendra M. Sonar. Framework for evaluation and selection of the software packages: A hybrid knowledge based system approach. *Journal of Systems and Software*, 84(8):1394–1407, 2011.

[63] Anthony J. Onwuegbuzie, Nancy L. Leech, and Kathleen M. T. Collins. Qualitative analysis techniques for the review of the literature. *The Qualitative Report*, 17(56):1–28, 2012.

[64] Markid. `https://trello.com/de`. Accessed: 2021-11-03.

[65] Shufti pro. `https://shuftipro.com/`. Accessed: 2021-11-03.

[66] Swiftdil. `https://www.swiftdil.com/`. Accessed: 2021-11-03.

[67] Global radar. `https://www.globalradar.com/`. Accessed: 2021-11-03.

[68] acuant. `https://www.acuant.com/`. Accessed: 2021-11-03.

[69] Electronic identification. `https://www.electronicid.eu/en`. Accessed: 2021-11-03.

[70] Fma enables online customer identification. https://www.fma.gv.at/en/fma-enables-online-customer-identification/. Accessed: 2021-05-30.

[71] Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Accessed: 2021-06-24.

[72] Adrian Thornhill Mark Saunders, Philip Lewis, editor. *Research Methods for Business Students*, chapter 10, pages 318–359. Pearson Education, 2009.

[73] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 2006.

[74] Elizabeth J. Halcomb and Patricia M. Davidson. Is verbatim transcription of interview data always necessary? *Applied Nursing Research*, 19(1):38–42, 2006.