Graduation thesis

Enabling the eCMR signing process by implementing e-signature software for Vervo

University of Twente
Bachelor's thesis Industrial Engineering and Management

Ruta Ērgle
s2290146

UNIVERSITY OF TWENTE.

April 2023

University of Twente
Bachelor Industrial Engineering and Management
Faculty of Behavioral, Management, and Social Sciences
Department of Industrial Engineering and Business Information Systems
Drienerlolaan 5
7522 NB Enschede

Author:
Ruta Ērgle
s2290146
r.ergle@student.utwente.nl

First University of Twente supervisor: **Dr. Rer. Nat. Daniel Braun**
Second University of Twente supervisor: **Ir. R.L.A. Rogier Harmelink**

Vervo supervisor: **Andris Žīgurs**
SIA Vervo
Tīraines iela 1, LV-1058,
Rīga, Latvia

UNIVERSITY OF TWENTE.

Preface

Dear reader, before you lay my hard-worked thesis. I am very grateful and extremely proud that after three years of intense studies at the University of Twente and almost one-year-long research at Vervo, I can proudly say that “It's done!”.

I am very thankful to Vervo because they were the only ones who opened their arms and took me into their company, not only to help me to do the research for them and helped to finish the University of Twente but also they took me as a full-time employee. That is why the research took me longer than expected. Although it took me more than 10 weeks to do the research, it was worth it, because as an employee I could better learn and understand the industry, such as how cargo transportation works and what the CMR process looks like. This opportunity to be able to do the research and work in Vervo is very appreciated. A huge thank you is to my advisor Andris Žīgurs, who gave me tips, helped me to better understand the industry, and guided me through the research when necessary.

Further, this thesis would not be done without my first supervisor dr. Daniel Braun, I am very fortunate to have such a great supervisor, he greatly supported me throughout the research and gave me constructive feedback when needed. And without Ir. Rogier Harmelink’s supportive suggestions and critique, my thesis would not look like this.

Lastly, the past four years would not be possible without the support of my family and loved ones. They gave the push and cheers when needed.

Thank you!

Ruta Ērgle
June 2023
Rīga

Management summary

The research was carried out at the freight forwarding logistics company Vervo, based in Latvia. Vervo SIA is developing a unified platform called Onfrex to bring together all transportation industry participating parties: consignors, consignees, and carriers. The use of electronic CMR note (eCMR) can solve many issues related to the traditional hard copy CMR, such as high fraud activities, extra material and administrative costs, and additional paperwork for employees. However, the implementation of eCMR is still limited in many countries and companies due to challenges with e-signatures, such as different e-document formats, validity, weight, and sensitivity of the information. Additionally, the consignment note cannot be signed digitally in cross-border situations due to differences in their local regulations for e-signature and the e-document has to be encrypted and decrypted. Hence, Vervo managers are interested in combining eCMR and e-signatures and are keen to explore how technology can facilitate this process.

As Vervo is creating Onfrex, they need an outsource, which could help sign the eCMR digitally and do it safely. In order to determine which system to choose and the criteria to consider for making the selection, the research focused on studying existing literature. This exploration highlighted specific factors, such as differences between CMR and eCMR, as well as the nature of e-signatures, that should be considered when initiating the software system selection process. Additionally, the study revealed several options for possible digital signature software and features of these systems, which facilitated the elicitation of requirements from stakeholders within the company. Through interviews, these requirements were collected and subsequently used to formulate different criteria for identifying a suitable software system for Vervo.

After eliciting requirements from Vervo managers and what are their priorities as to what the software has to have, the research continues with evaluation and detailed examination of founded e-signature software platforms. It was concluded that eID Easy Docs suits the best for Vervo, as the costs are per document, in the case of Vervo, per eCMR, and there is no limit to the number of users and transactions of documents. As well as the eID Easy Docs provides strong authentication methods and has worldwide availability.

Further, to show the Vervo management, how CMR is being signed now, and what the process would be like by signing with eID Easy Docs, process flow diagrams were made for both signing CMR and eCMR.

Finally, recommendations are given to the managers of Vervo, to introduce them to the idea to try the eID Easy Docs software while still Onfrex is being developed, as well as, train the users and encourage them to use the digital signature software in other daily activities.

Table of contents

Reader’s guide

The reader's guide is to inform how the research is carried out in the freight forwarding company Vervo. Each chapter is described shortly with the main points that each chapter contains.

Chapter 1. Introduction

In the first chapter, the description of Vervo and the problem context is given, along with the problem cluster with research questions and sub-research questions. Later, the research design with methodology, variables, and research limitations and scope are explained.

Chapter 2. Theoretical Framework

In the second chapter, the literature review of CMR, eCMR, and e-signatures is executed. The requirements of what e-signature software platform has to have and possible e-signature software platforms are investigated. A review of methods, requirements engineering, multi-criteria decision-making, and BPMN, used in the operationalizing is described.

Chapter 3. Operationalizing the method

Before comparing the e-signature software platforms, requirements are elicited from Vervo, a comparison criterion is created and the comparison table with the researched requirements per e-signature software is presented. Afterward, evaluation per requirement per software is conducted. After evaluating each software and how these software platforms satisfied or not Vervo's needs, two final e-signature software platforms are examined and compared based on priority, and finally, an e-signature software that suits the best Vervo is elected.

Chapter 5. Process flow diagrams

The process of signing CMR and eCMR with the chosen software is explained and visualized with a process flow.

Chapter 6. Conclusions and recommendations

In the final chapter, conclusions of the research, together with recommendations and advice for future work are given.

List of abbreviations

CMR: (Convention relative au contrat de transport international de Merchandises par Route) Convention on the Contract for the International Carriage of Goods by Road
eCMR: Electronic Consignment Note
eIDAS: Electronic Identification and Trust Services for Electronic Transactions
MPSM: Managerial Problem-Solving Method
BPMN: Business Process Model Notation
RE: Requirements engineering
SaaS: Software as a Service
PaaS: Platform-as-a-service
IaaS: Infrastructure-as-a-service
eFTI: Electronic freight transport information
GDPR: General Data Protection Regulation
SES: Simple Electronic Signatures
AdES: Advanced Electronic Signatures
QES: Qualified Electronic Signatures
QTSP: Qualified Trust Service Provider
UETA: Uniform Electronic Transactions Act
ESIGN Act: Electronic Signatures in Global and National Commerce Act
eID: Electronic Identification
ISO: International Organization for Standardization
SOC: System and Organization Control
HIPAA: Health Insurance Portability and Accountability Act
CCPA: California Consumer Privacy Act
FIPS: Federal Information Processing Standards
FISMA: Federal Information Security Modernization Act
PKI: Public Key Infrastructure
MFA: Multi-Factor Authentication
IDaaS: Identity as a Service
GSMA: (Groupe Spécial Mobile) Global System for Mobile Communications
OTP: One Time Pad
API: Application Programming Interface
JSON: JavaScript Object Notation
CA: Certificate Authority
RA: Registration Authority
RSA algorithm: Rivest-Shamir-Adleman algorithm
RO: Registration Officer
SIR: Standard Identification Record
URL: Uniform Resource Locator

1. Introduction

In the first chapter the company's background and description of the situation is presented, afterwards, the problem context with the problem cluster is introduced, from where the core problem and research questions are derived. Furthermore, the methodology, research design, and variables are shown. And lastly, limitations and scope are given.

1.1. Company background and context

Vervo SIA (Ltd.) is one of the leading freight forwarding and logistics companies in the cargo transportation industry in Latvia, with its subsidiary offices in Estonia, Poland, and recently in the United Arab Emirates. It was established in 2008 and since then has helped more than 4000 companies and individual consignors in more than 120 countries.

Transporting cargo over borders has to be noted with the consignment note called CMR, which describes what is being carried and which is signed between the shipper, cargo receiver, and carrier. This consignment note, CMR, fully known as a Convention on the Contract for the International Carriage of Goods by Road was established by the United Nations in 1956, Geneva, to provide a uniform legal framework for national and international road transport. So far 58 countries in the world are part of the convention. In 2008 an additional e-protocol, an updated electronic consignment note - eCMR, was added to the CMR convention, where in 2011 it entered into force. However, only 31 countries have confirmed and are part of the eCMR protocol, and just recently, at the beginning of September, this year, 2022, Germany ratified the eCMR protocol. The protocol should be fully applied by all countries of the European Union latest by 2025 (Ratia, 2022).

Vervo is currently developing a unified platform called Onfrex where transport, clients, and freight agents come together, and where electronic consignment note (eCMR) is standard practice. However, in the process of developing this product, stakeholders have encountered another problem - the e-signing process is challenging to perform. If an order is made in Latvia and the cargo has to be transported, for example, to Poland, the eCMR is signed here in Latvia with e-signature, but the consignment note cannot be signed in Poland due to the difference in specific legal and regulatory requirements. Therefore, the goal of the research is to find out and present to the management of Vervo, what digital signature software to implement and integrate with Onfrex so that the eCMR signing process would be enabled.

1.2. Problem context

Many countries and businesses are working on eCMR platforms and systems. For example, the Estonian Ministry of Economic Affairs and Communications is working on a project called DINNOCAP where so far they have made a prototype to experiment with how their eCMR system works between Baltic countries and Poland logistics companies (Hurt, 2021). Besides Estonia, also Benelux countries and others are developing and presenting their pilot projects, and many others (Tumel, 2022). However, as there have been no specific calculations conducted regarding the implementation of e-CMR in Latvia, to show if the eCMR pays off, the Latvian Information Communication and Technology Association is currently engaged in a pilot project to explore its introduction. To estimate the costs associated with implementing a similar eCMR system, the research by Licite-Kurbe and Ozolina (2022) relies on data from TransFollow, a Dutch company. The research concludes that an investment of approximately EUR 27,600 is required, but it proves to be profitable within a few years given the number of shipments increases. From 2016 to 2020, the international

manufacturing company experienced a 50% growth in the number of freight shipments that were analyzed, and it is believed that number of shipments will increase (Licite-Kurbe & Ozolina 2022).

Meanwhile, the eCMR is being ratified and technology developed to ensure eCMR usage, the e-signature is rapidly becoming a common practice in Europe and the rest of the world. The first public directives for Electronic signatures were established in 1999 (eSignatures Directive 1999/93/EC). This directive allowed EU member states to start using the digital signature, however, this resulted in poor execution because each country interpreted the legislation differently, and there was no standard procedure. Therefore, in 2014 the European Parliament repealed the directive into a standardized legal framework. The EU Parliament introduced a regulation Nr. 910/2014 known as Electronic Identification and Trust Services for Electronic Transactions (eIDAS). It officially entered into force across all member states on the 1st of July, 2016 (Foxit Esign, 2018). Since then EU countries have slowly shifted towards the digital signature, and with every year the technology has developed, so as to make digital signing easier and more efficient. With regulation Nr. 910/2014 documents signed with e-signature have equal legal effect as those signed by hand. This regulation allows the possibility to sign contracts, transactions, and administrative procedures, even in cross-border situations (European Commission, n.d.). So far the application of e-signature in Latvia has increased rapidly, in 2020 alone Latvian residents used the eID card 3.2 million times, whereas, the mobile application eParaksts 2.2 million times, with the number of eParaksts mobile users reaching 100,000 (Pala, 2021).

For both eCMRs and e-signatures, technology is developing rapidly to ensure that these processes can be carried out effectively, hence, Vervo managers are curious about how both these digital enhancements can be combined.

1.3. Methodology

To solve the core problem and answer the research question we will use the Managerial Problem-Solving Method (MPSM). This method is effective and straightforward. It consists of seven phases:

1. Definite the problem
2. Formulating the approach
3. Analyzing the problem
4. Formulating (alternative) solutions
5. Choosing a solution
6. Implementing the solution
7. Evaluating the solution

In the first phase the problem is introduced together with the problem cluster and core problem with the research question and the context of the problem is given. In the second phase, the problem-solving approach is presented, with a description of research methods and design. In the third phase, the problem is analyzed and researched deeper, however, in this step knowledge is needed, so we move to a research cycle, to obtain more information and answer sub-research questions that were developed in phase 2. As well as in the fourth phase, information is needed to formulate possible solutions, so we enter the research cycle again to evaluate and present solutions together with criteria, with which the final decision will be made. And in the fifth phase, based on made criteria, we conclude which would be the best decision or solution for the core problem. And finally, phase six and seven is where we implement the solution and see how the solution works in reality, and we evaluate the solution and, if needed, go back to phase 1 (Heerkens & Winden, 2017). The research is carried out until phase 5 and including. Phases 6 and 7 will not be done in this research, considering the limitations.

1.4. Problem identification

In an organization problem can be starting from every-day minor issues to major organizational problems, so it is advised to search the core problem, which solution will make a real difference to every level. To find a core problem, first, a problem inventory is carried out, then cause-and-effect relationship with problem cluster is identified, and lastly, the core problem is derived, and research questions is presented (Heerkens & Winden, 2017).

1.4.1 Problem cluster

Although eCMR was established more than 10 years ago, the problem is that the CMR is still being signed by all mentioned parties - shipper, receiver, and transport - as a hard copy document. This leads to many problems, such as high fraud activities because data is difficult to control and oversee, that is, for example, the CMR can be signed by anyone, and it is challenging to know for sure if the signature is legitimate. Because it is a physical paper, there are extra material and administrative costs, and additional paperwork for employees. In Latvia alone, approximately 2 million CMRs are printed each year, costing 5 EUR per CMR in Latvia, and 10 EUR in Europe (based on Vervo internal research about the approximate CMR costs). With eCMR, these problems can be solved. By using eCMR the costs are estimated to decrease two to three times, which should be around 1-2 EUR, mainly paper costs, are gone, sending costs via post is terminated, if the stakeholder needs original copies, and archiving the consignment notes are not needed. However, there are still some reasons why eCMR is still not fully used in many companies and countries. One of the main reasons is that some countries are working on ratifying the new protocol, as mentioned, only 31 countries are part of it, and without the eCMR protocol, CMR is used. And secondary, some companies are reluctant about implementing and shifting to eCMR systems. Although CMR is less efficient, many companies have even optimized their own ERP systems to manage print-based CMR (Ratia, 2022).

One thing is to implement the eCMR, but with this challenge comes another one - how can clients and partners sign this eCMR? It is not that simple to just sign a document with an e-signature and pass it on via email to another country due to safety reasons, and electronically signed documents have to be encrypted and decrypted. Hence, it is important to address certain issues associated with e-signatures. One such concern is the variation in e-document formats across different countries as the document. For instance, in Latvia, the e-document format is eDoc, while other countries may utilize their local e-document file formats, such as PDF or other formats. Additionally, challenges arise concerning the validity of e-documents and the significance of e-signatures. Local jurisdictions may require specific forms of e-signatures for certain documents, particularly when it comes to security documents that necessitate robust authentication and full admissibility in court. Given that eCMR notes contain cargo information, it is advised to evaluate the sensitivity of this data. Furthermore, stakeholders might request additional elements on e-documents such as stamps or dates, in addition to the signature.

After researching and gathering problems by making a problem inventory, we need to see the relationships between these problems, which can be done with a problem cluster. (Figure 1). A problem cluster is a helpful tool to visualize the problems, and the cause-and-effect relationship that has been identified, and that can help us to narrow down to the core problem (Heerkens & Winden, 2017).

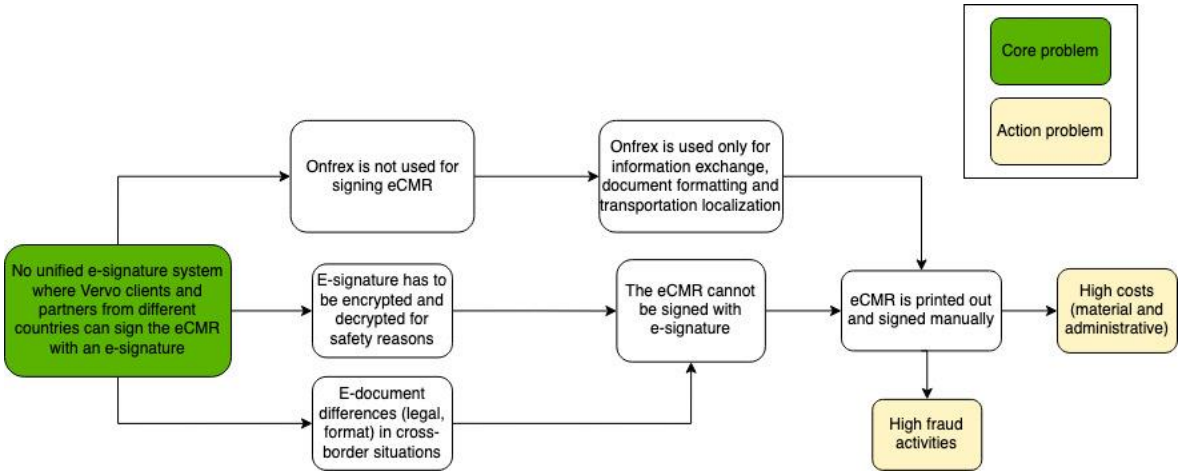


Figure 1. Problem cluster

1.4.2. Core problem

To identify the core problem, we must understand the difference between action and core problem, and how to conclude which is our core problem. An action problem is a situation that we do not want it to be in, it is a difference between norm and reality (Heerkens & Winden, 2017). In our case, the action problems, in reality, are high fraud activities, high material, and high administrative costs, which are 5 EUR in Latvia, and 10 EUR in Europe. Whereas we aim for a sustainable and efficient way to deal with CMRs, which should be our norm: 1- 2 EUR.

A core problem is a problem that we can influence, has no direct cause in itself, and has the greatest impact effect at the lowest cost (Heerkens & Winden, 2017). Therefore, we conclude that we cannot influence other companies to implement and shift towards eCMR systems, as well as persuade the EU and other countries to ratify the eCMR protocol. However, we can influence our position in digitalization towards the shift to eCMRs, and by doing so, we indirectly affect other companies. But in order to fully move to eCMR practices, we need a tool to be able to sign them. Hence, the core problem is:

There is no unified e-signature software that Vervo clients and partners from different countries can use to sign the eCMR with an e-signature.

1.4.3. Research question

A problem statement is formulated as a question, as a research question, that explains what we intend to research and by answering it we have the necessary knowledge that we need to implement appropriate measures in the organization (Heerkens & Winden, 2017). Hence, an e-signing platform is needed to combine all signatures of stakeholders and parties to ensure a safe and fast eCMR signing procedure. Therefore, the **research question** is:

Which e-signature software supports the integration of e-signatures for eCMR documents signed by shippers, receivers, and carriers and that can be compatible with freight forwarding and logistics company Vervo's Onfrex platform?

1.4.4. Sub-research questions

To solve the research problem, the research question is split into sub-research questions that make the problem more accessible and systematic (Heerkens & Winden, 2017). The sub-research questions are:

1. **How is the CMR signing process carried out now?**

By asking this question, we can better see and understand how the process of signing CMR is being done right now, which will also help us to get insight into other challenges and opportunities that might not be fully realized.

2. **What are the requirements for the e-signature software?**

After literature studies and interviewing Vervo stakeholders, we can better grasp what Vervo is looking for and what an e-signing software should provide, so a list of requirements is presented.

3. **What e-signature software platforms are in the market?**

Since many e-signature software platforms can be found and are available, we analyze the most suitable e-signatures software platforms, by listing their characteristics, costs, advantages, and disadvantages. A list of e-signature software is given.

4. **Which e-signature software suits the best for Vervo based on their requirements?**

By taking into account the requirements given by Vervo and found in the literature, we deduct and conclude which software would suit the best for Vervo.

5. **How the eCMR signing process would be carried out with the selected e-signing software?**

Based on literature studies and our and management perspectives, we can visualize the process, if we implement the chosen e-signing software. By seeing the relationship between different stakeholders and the software, we can acknowledge what could be the requirements and/or challenges when we implement the software.

1.5. Problem-solving approach

After identifying the core problem, and presenting the research question, the research methodology is established, with sub-research questions and the research design.

1.5.1. Research design

The research question can be answered by using a conclusive research design, more specifically, a descriptive cross-sectional design. This research design helps to answer questions about the who, what, when, where, why, and how of the research at a specific point in time: cross-sectional research. Descriptive research is used to obtain information concerning the current status of the phenomena and to describe "what exists" with respect to variables or conditions in a situation (Shukla, 2008). The “who” is Vervo stakeholders and clients, the “what” is e-signature software, as the “when” is now, currently, “where” is Latvia, but the overall scope is Europe, as how clients will use the e-signature over Europe. And finally the “how” is the documents being signed right now and “how” it will be done with the e-signature software. Therefore, the research is done with three blocks: analysis of the current situation, research requirements, finding the best e-signature software for Vervo, and finally analysis and predictions of how the process will be carried out when the e-signature software is implemented.

Data is gathered by primary and secondary data collection methods, primary: interviews and observations. And secondary: reports, books, research papers, government publications, etc. And the research population contains of Vervo managers and employees, and literature studies.

In order to answer the research question and find a solution to the core problem, we will conduct an analysis by answering sub-research questions. A description of each sub-research question is shown in Table 1.

Nr.	Type of research	Data type	Research population	Data collection methods and activities	Deliverables
1.	Descriptive	Qualitative	Vervo managers/ employees; Literature studies	1. Observations 2. Open unstructured interviews 3. Literature studies 4. Draw the process flow	- Process flow diagram
2.	Descriptive, cross-sectional	Qualitative	Vervo managers; Literature studies	1. Conduct expert, structured, in-depth interviews 2. Literature studies	- List of requirements and criteria
3.	Descriptive	Qualitative	Literature studies	1. Search e-signing software 2. Note characteristics of each e-signature	- Table of e-signature software with their characteristics
4.	Descriptive, cross-sectional	Qualitative	Literature studies	1. Analyze the e-signature software 2. Choose a software 3. Try the software with a trial version 4. Receive feedback from the management	- Chosen e-signature software is presented - Feedback of the software from the management
5.	Descriptive	Qualitative	Literature studies	1. Literature studies 2. Draw the process flow 3. Present the process flow to the management	- Process flow diagram - Feedback of the process flow from the management

Table 1. Research design

1.5.2. Deliverables

At the end of the research we will present to the management of Vervo deliverables listed below:

- Process flow of the current CMR signing process and a process flow with the implemented e-signature software;
- Based on the requirements of Vervo and developed criteria, a suitable e-signature software;
- Conclusions and recommendations to the Vervo management of the selected e-signature software.

1.5.3. Reliability and validity

To show if the research results are accurate, reliable, and valid, we need to indicate potential factors that might influence reliability and validity (Heerkens & Winden, 2017).

Reliability is the degree to which a measurement is free of random or unstable error, that is, by doing the same research method, the result will be the same (Schindler, 2019). In this research, the reliability is constrained by a time factor, that is, we will find, analyze and decide which e-signature software to use based on the requirements and what e-signature software platforms are available on the market right now. In a few years, the development of e-signatures and technology will be improved, such that the needs and requirements now probably will not be the same as later. And as considering reliability in the interviews, to ensure that the data gained is reliable we need to develop appropriate questions that can measure the competency level of the participants, as well as, introduce the participants to the assessment criteria beforehand (Nicolas, 2022). However, for data to have high reliability, requirement engineering introduces the following phases: elicitation, analysis, specification and documentation, validation, and management. By going through each phase, the requirements are extracted, documented, managed correctly, and comply with users' needs (Ahmad, et al., 2023). By using RE we can minimize error and miscommunication with the management. Additionally, interviews should be performed after a while again, which will not be possible, as the decision on which software to use will be done only once. Although, after implementing the software, the management might have new requirements or preferences, however, that are out of the scope of the research.

Whereas validity is a criterion concerned with the content of the research and can be divided into three types of validity: content validity, criterion-related validity, and construct validity. Content validity is the degree to which the measurement instrument or design provides adequate coverage of the research question (Heerkens & Winden, 2017; Schindler, 2019). In the context of the research, the problem analysis and identification are researched to such a degree that the research question covers the topic of interest. As well as the questions for the interviews will be created carefully to ensure that the right questions asked will cover the research question. The second type of validity is criterion-related validity, which reflects that the measurement tool or method measures what it intends to measure, and is relevant and reproducible (Schindler, 2019). In our case, the criterion for selecting e-signature software will be established exclusively for Vervo, based on the literature study and interviews. Therefore, the questions of the interviews that will be carried out should be made such that the answers to the questions deliver the necessary information, and that companies similar to Vervo can use our analysis as well.

Lastly, construct validity concerns that the concepts used in the research are properly operationalized, and logical and can be explained with the available literature, shortly, that the research is not abstract (Heerkens & Winden, 2017). In relation to the research, new information about the eCMRs and regulations towards the e-signatures is released daily, because this is a relatively new concept and eCMRs are slowly being ratified by countries. For this reason, we might encounter challenges because there may not be enough information about eCMR being signed with e-signatures, or what other companies and countries are using or doing, which brings us to the limitations of the research.

1.5.4. Limitations and scope

The scope of the research explains the range of the research, whereas limitations are the boundaries of the research (Brown, 2020). The scope of the research is challenging to express because the requirements and the final decision of the software will take place in Latvia, however, the decision that will be made will affect not only clients and partners in Latvia but also outside Latvia. Unfortunately, we cannot invite every client and partner of Vervo to participate in the research as it would be costly and more time-consuming. Nevertheless, feedback from clients and partners is needed, therefore, that can be considered as future research.

The limitation of the research is that the e-signing software will be chosen, based on the Vervo stakeholder preferences and requirements in Latvia and the literature studies. This leads to the constraint that we cannot fully experiment with how the process will be carried out in real life because we need clients and carriers who are open to trying out the software and seeing how the document signing can be done. Due to the time, constraint of 10 weeks will not implement and evaluate the software in reality. Also, we can only hypothetically decide and conclude what clients and carriers prefer or require because the Vervo employees and managers in Latvia will decide which software to implement.

In the research we will look only at CMRs and eCMRs, which are consignment notes for goods transported by road, we will not include research about the Bill of Landing - a contract for the carriage of goods by sea, and neither analysis of Air Waybill which is a document for goods transported by air.

2. Theoretical framework

A theoretical framework is built upon an established theory (or theories) found in the existing literature. These theories have already been tested and validated by other researchers and are widely accepted within the scholarly community. The theoretical framework acts as a foundation and provides essential structure and support for justifying the research and answering the research question (Grant & Osanloo, 2014). Hence, this chapter focuses on understanding the concepts of CMR, eCMR, and e-signature, and presents e-signature software features found in the literature and e-signature software platforms. Together with a literature review of methods used for selecting the e-signature software.

2.1. CMR consignment note

The most important document for the international transport of goods is the CMR consignment note. In 1956 the Convention on the Contract for the International Carriage of Goods by Road (CMR) was established to unify rules and transportation regulations, as without a standard framework for the goods carried cross-border, the carriers would have to know national transport regulations which would lead to misunderstandings and wrongly interpretations (Poliak et al., 2020).

CMR consignment note specifies the rules, obligations, and responsibilities of the carrier and as well as regulates the conclusion and performance of transport and controls the procedure for claiming damages and liability of the carrier (Poliak et al., 2020; Poliak & Tomicová, 2021). CMR convention is also an insurance for carriers and haulers to transport cargo legally in Europe (Drevinskaitė et al., 2019). However, the CMR Convention does not allow to transport of three types of goods, such as postal goods (cards and letters), dead bodies, and furniture (household) removal goods because these packages are difficult to objectively value (Convention on the Contract for the international carriage of goods by road (CMR) and Protocol of signature, 1956). The CMR consignment note as indicated in Article 6 of the CMR Convention Contract (1956), has to contain:

- Date and place where the consignment note is issued;
- Name and address of the consignor;
- Name and address of the carrier;
- Place and date where goods are received;
- Place and date where goods are delivered;
- Name and address of the consignee;
- Description of the goods and method of packaging, and in case of dangerous goods, their recognized description;
- The number of packages and their special marks and numbers;
- The gross mass of the goods and their quantity;
- Charges to the carrier, such as transport costs, additional costs, duties, and other charges incurred between the time of making the contract and delivery;
- Additional instructions for customs and other formalities;
- A statement that the carriage is subject to the provision of the Convention, notwithstanding any clause to the contrary;
- Signatures of consignors, consignees and carriers (Convention on the Contract for the international carriage of goods by road (CMR) and Protocol of signature, 1956).

The consignment note is issued in three original copies, for each participating stakeholder: carrier, consignor, and consignee. The first (red) copy is for the consignor as proof that the goods have been collected by the carrier. The second (blue) copy is for the consignee, to know how much goods to take from the carrier, and the third (green) copy is for the carrier, which is also a document that shows

the goods have been handed over to the consignee. The CMR consignment note can be issued in other copies (colors) as well for a third party, for example, an insurance company, customs office, or bank (Poliak & Tomicová, 2021). In practice, there is also an original document of the CMR note, which is given (sent) to the transport service buyer.

Figure 2. Different copies of the CMR consignment note (Poliak & Tomicová, 2021)

The CMR consignment note is usually issued by the carrier at the place of loading or the consignor. The consignor can be either the place where the goods are loaded or an entity that orders the goods from a different place (Poliak & Tomicová, 2021). As mentioned previously, the CMR consignment note can be in more than three copies. In the context of the research, the process flow will be carried out with the three stakeholders, that is, the consignor, carrier, and consignee, and the shipment service buyer is the consignor. Although, the cargo transportation service buyer can be anyone of the stakeholders. Either way, their roles and sequence of activities as the sender, receiver, and carrier are the same as whoever places the order. As well, we assume that the cargo is transported all at once, and is not being transferred to another truck or intermediate stakeholder.

2.2. Electronic CMR note

The most important aspect that Vervo management pointed out at the beginning of the research was that the e-signature software could be used to sign the eCMR consignment note.

For eCMR to work, a digital platform has to be implemented, where all the necessary information is accessible, and each participating process stakeholder can get a hold of the data. The carrier registers the information, data is stored in a platform that can automatically generate the eCMR note (Ponzoa Casado, Gómez Funes & García-Doncel, 2021). In the case of Vervo, the digital platform is Onfrex, where the eCMR process will be present.

So far 32 countries have ratified the eCMR protocol: Belarus, Bulgaria, Belgium, Denmark, Czech Republic, Estonia, Finland, France, Germany, Iran, Latvia, Lithuania, Luxembourg, Moldova, The Netherlands, Norway, Oman, Poland, Portugal, Russia, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Tajikistan, Ukraine, United Kingdom of Great Britain and Northern Ireland, Uzbekistan, and Kyrgyzstan. Many other countries are in the process of ratifying the protocol, for example, Italy. The majority of transportation within Europe does cross borders, sometimes through countries that have not yet ratified the eCMR protocol, therefore, the paper CMR note is used. Carriers might adopt a hybrid version, to practice the digital CMR protocol and increase supply chain visibility (Transfollow, 2022).

As of August 21, 2025, EU Member States are required to be able to accept transportation information in a standardized electronic format that can be read by machines, as dictated by the eFTI

regulation. While the use of eFTI is not mandatory for economic operators, those who wish to electronically share data with EU authorities must use certified eFTI service providers and platforms. The eFTI regulation allows economic operators to retain control over their data by allowing them to share it at the source and grant or revoke access as they see fit. This allows logistics operators to use the same source data for commercial, transport, and compliance purposes, while authorities can "pull" datasets of information as needed. The eFTI regulation is the first step towards fully digital data-sharing processes, including sharing licenses and permits in electronic format. It is also a step towards a federated data-sharing architecture and a future EU mobility data space, where participants can trust each other due to shared identities, authentication methods, and access policies, and use a common language with interoperable semantics (Hemeleers, 2022; Willems, 2021).

2.3. E-signature concept

For us to be able to sign the eCMR, we need to understand how the digital signature process is done. An e-signature is created by using a public key that is used to encrypt data, and a private key (also known as the signature key) that is used to decrypt data, this process is called the public key infrastructure (PKI) which is a cryptographic system. The PKI system is used to provide confidentiality, integrity, and authenticity of digital information. The public key infrastructure consists of various components such as a certificate authority (CA), registration authority (RA), certificate database, and certificate management system. In a PKI system, a user's public key is stored in a digital certificate issued by a trusted certificate authority. When a user wants to send a message or transaction, they use the recipient's public key to encrypt the message or transaction, ensuring that only the intended recipient can decrypt and access it is using their private key. The private key is kept secret and is used to create the e-signature, while the public key is used by external parties to verify the signature. The public key is open data and is used to decrypt the encrypted e-signature data at the recipient's end. The RSA algorithm is used as the public key algorithm, and the SHA algorithm is used as the digest algorithm in this process (Bensghir & Topcan, 2008). Figure 4 illustrates the concept of using the public key cryptographic algorithm, and is shown how the public key is to create and verify an e-signature (Arnaut, 2022).

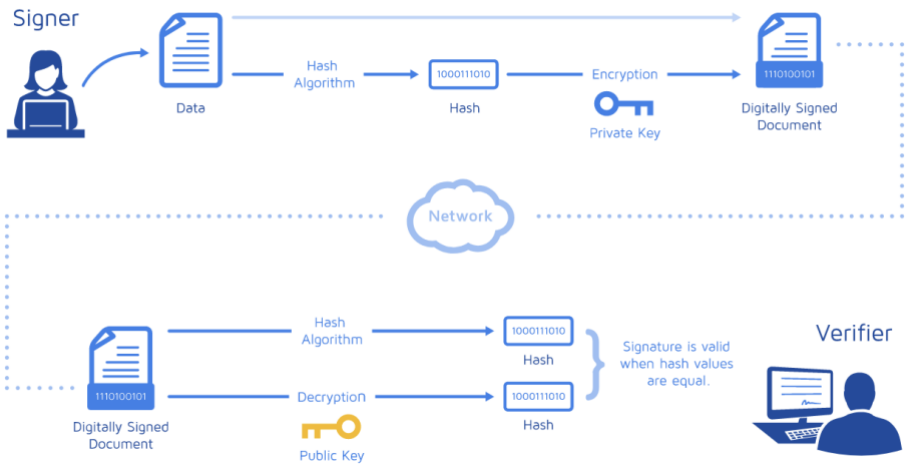


Figure 3. E-signature verification with private-public key algorithm (Arnaut, 2022)

2.5. E-signature software platforms

Since many e-signature software platforms can be found and are available, we analyze the most suitable e-signatures software platforms, based on ratings in the most recognized evaluation and review platforms dedicated explicitly to software for businesses, such as Capterra, GetApp, G2 Crowd, and SoftwareAdvice. Criteria that are being rated are ease of use, customer services, functionality, the value of money, and the likelihood of a recommendation (Kevens, 2022). We selected e-signature software platforms which are above 4.5 ratings. The list of digital signature software platforms based on their ratings and the number of reviews per software review site can be seen in Table 2.

Capterra		GetApp		G2 Crowd		SoftwareAdvice	
Software	Rating	Software	Rating	Software	Rating	Software	Rating
DocuSign	4.8 (8023)	eID Easy	5.0 (1)	eversign	4.8 (2469)	eversign	4.84 (2472)
eversign	4.8 (2474)	DocuSign	4.8 (7800)	PandaDoc	4.7 (1932)	DocuSign	4.75 (8022)
eID Easy	4.8 (4)	eversign	4.8 (2400)	Dropbox Sign (HelloSign)	4.7 (2095)	eID Easy	4.75 (4)
Adobe Acrobat	4.7 (1661)	Adobe Acrobat	4.7 (1600)	Foxit eSign	4.6 (862)	iLovePDF	4.74 (1129)
iLovePDF	4.7 (1125)	Dropbox Sign	4.7 (1000)	signNow	4.6 (1586)	Dropbox Sign (HelloSign)	4.72 (1034)
Dropbox Sign (HelloSign)	4.7 (1034)	iLovePDF	4.7 (1000)	SignRequest	4.6 (1575)	Adobe Acrobat	4.71 (1661)
signNow	4.6 (497)	Jotform	4.6 (1200)	DocuSign	4.5 (1989)	signNow	4.62 (497)
Jotform	4.6 (1263)	SignNow	4.6 (496)	Adobe Acrobat	4.5 (2867)	Jotform	4.61 (1266)

Table 2. Top e-signature software platforms per software review site

There are many electronic signature software platforms available, however, we are searching for platforms that can be used to sign eCMR documents. Based on ratings and number of reviews per review site, we will analyze the most popular and used software platforms that can be used in any industry, and those are eversign, Adobe Acrobat Sign, DocuSign, and Dropbox Sign (HelloSign). Besides the most reviewed platforms, we will also consider and look into less-used digital signature

software platforms which are made for the supply chain, such as eID Easy Docs and SignNow (Capterra, n.d.; GetApp, n.d.; G2 Crowd, n.d.; Software Advice, n.d.).

Each platform has its strengths, such as DocuSign's ease of use and integration capabilities, Eversign's custom form templates, Dropbox Sign's user-friendly interface and flexible pricing, Adobe Sign's advanced security features and integration with Adobe's document management tools, and SignNow's legally recognized e-signatures and free mobile app (DocuSign, n.d.; eversign, n.d., Adobe Acrobat Sign, n.d. & SignNow, n.d.). eID Easy Docs is a specialized platform designed for the transportation and logistics industry, simplifying the process of implementing electronic ID authentication and signature methods onto websites (eID Easy, n.d.)

2.6. Requirements engineering

Requirements engineering involves carefully assessing and understanding the distinct requirements and needs of stakeholders and subsequently refining them into specific and detailed requirements. These requirements are then documented and specified in a manner that enables them to serve as the foundation for all subsequent activities in system development (Pohl, 2010; Lapouchnian, 2005). Requirement engineering (RE) goes through the following phases: elicitation, analysis, specification and documentation, validation, and management (Ahmad, et al., 2023).

Requirements engineering is a two-phase process. In the early phase, the focus is on understanding the organizational context, stakeholders, and their relationships to determine the correct requirements for the system. In the late phase, the system is integrated into the organization, and the boundaries between the system and its environment are established. System requirements and assumptions about the environment are specified, aiming to achieve stakeholders' goals. Striking a balance is important to avoid excessive complexity or unrealistic assumptions (Lapouchnian, 2005).

In requirements engineering (RE), requirements are categorized as either functional or non-functional. Functional requirements pertain to the system's features and business rules, specifying what the system should include. On the other hand, non-functional requirements encompass system qualities and constraints (Ahmad, et al., 2023).

2.6.1. Requirements elicitation using interviews

To gather information about Vervo's e-signature software requirements, structured interviews were used after literature studies. Structured interviews involve asking predetermined questions in a specific order and are commonly used in quantitative research. They typically involve closed-ended questions, such as yes or no questions, or provide multiple options to choose from. While structured interviews can be used in qualitative research, it is less common. The advantage of structured interviews is that they allow for easy comparison of answers between participants, providing uniformity in the data, and reducing bias and ambiguity. Structured interviews have the advantage of providing uniformity in the data collected, making it easy to compare answers between participants, and identify patterns and areas for further study. This method is valuable for both explanatory and exploratory research, and it is simple to carry out and analyze. It is most effective when the researcher has a strong understanding of the topic, and when time or resources are limited, and quick analysis of data is required. With proper organization, structured interviews can be easily managed by an individual (George, 2022).

2.6.2. Requirement identification

Firstly, we need to understand what type of e-signature solutions are available and possible to use. There are three types of software solutions: Software as a Service (SaaS), Platform-as-a-service (PaaS), and Infrastructure-as-a-service (IaaS).

Infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) are not typically the best options for electronic signature software because they do not include the actual software application. It is generally recommended to use software-as-a-service (SaaS) for electronic signature software. SaaS is a cloud computing model in which a provider hosts and maintains the software application and makes it available to users over the internet on a subscription basis. With SaaS, users can access the electronic signature software from any device with an internet connection, and they do not have to worry about installing or maintaining the software themselves. The provider handles all updates and technical support, so users can focus on using the software to meet their needs. IaaS provides access to infrastructure resources such as storage and virtualization, while PaaS provides a platform for building and deploying applications (Watts & Raza, 2019).

Godes and Mulik (2009) propose factors for SaaS selection, and those are functionality, architecture, usability, vendor reputation, and cost. Specifically, integration, scalability, reliability, security, user interface, help, support for mobile devices, offline support, number of users, and annual or one-time implementation cost (Godse & Mulik, 2009). However, these criteria are for general SaaS platforms, therefore, we should also consider factors related to e-signature software platforms. Therefore, based on evaluation and review platforms dedicated explicitly to software for businesses, which were previously mentioned: Capterra, GetApp, G2 Crowd, and SoftwareAdvice, we can add criteria that they think are important for e-signature software platforms to contain (Capterra, n.d.; GetApp, n.d.; G2 Crowd, n.d.; Software Advice, n.d.). The list of features can be seen in Table 3.

Access Controls/Permissions	Document Automation	Real Time Notifications
Activity Dashboard	Document Capture	Regulatory Compliance
Activity Tracking	Document Generation	Reminders and Expirations
Alerts/Notifications	Document Management	Reporting & Statistics
API	Document Review	Reporting/Analytics
Approval Process Control	Document Signing	RFP Management
Archiving & Retention	Document Storage	Search/Filter
Audit Management	Document Templates	Secure Data Storage
Audit Trail	Drag & Drop	Security and Scalability
Authentication	Email Reminders	Sell Side (Customers)
Bulk Digital Signatures	Enterprise Scalability	Sign-In Process
Buy Side (Suppliers)	File Recovery	Signature Document Creation
Collaboration Tools	File Sharing	Signature History and Audit
Commenting/Notes	File Storage	Signature Process
Completion Tracking	Forms Management	Signature Workflow
Compliance Management	Full Text Search	Specialty Contracts
Compliance Tracking	Government Contracts	Status Tracking
Configurable Workflow	Internationalization	Tagging
Content Library	Mobile Signature Capture	Task Management
Content Management	Mobile Signatures	Task Progress Tracking
Contract Drafting	Multi-Party Signing	Team Collaboration
Contract/License Management	Performance and Reliability	Template Management
Customizable Templates	Pre-built Templates	Templates
Data Extraction	Process/Workflow Automation	Third Party Integrations
Data Security	Progress Tracking	User, Role, and Access Management

Deployment	Proposal Generation	Version Control
Digital Signature	Quotes/Estimates	Workflow Management
Document Analytics	Real Time Data	

Table 3. List of features used in e-signature software platforms

The list of features (Table 3) used in e-signature software platforms can be narrowed down to a more concise list combined with the SaaS factors, that can be easier to compare to and analyze. See Table 4.

Requirements
1. Security
2. Legal compliance
3. Authentication
4. User experiences
5. Integration
6. Deployment
7. Mobile accessibility (priority)
8. Cost
9. Customization
10. Technical support
11. Multiple signatories
12. Support for multiple languages
13. Scalability
14. Worldwide availability

Table 4. The reduced list of requirements

For us to better understand the characteristics and be able to compare the e-signature software platforms, each requirement is researched in more detail.

Legal compliance

Electronic signatures are commonly used in the European Union for a range of purposes, both in the public and private sectors. In order to ensure a reliable and collaborative electronic signature process, certain steps must be taken at both the national and international levels. At the national level, it is necessary to establish a legal and technical infrastructure for a reliable and problem-free national e-signature system, which includes setting up the necessary legal frameworks and technical systems (Bensghir & Topcan, 2008). The General Data Protection Regulation (GDPR) also requires that all companies that process and hold the personal data of individuals in the EU comply with the GDPR, including e-signature providers that assist organizations around the world in digitizing their paper-based processes (Kaba, 2018).

The EU's eIDAS regulation establishes a framework for electronic signatures and trust services across the EU and distinguishes between three categories of electronic signatures: simple electronic signatures, advanced electronic signatures (AdES), and qualified electronic signatures (QES). Simple electronic signatures, also known as baseline signatures, are the most basic form and can include a signatory typing their name into an electronic document or using an online e-signing platform. AdES

are more advanced and meet additional requirements, such as being uniquely linked to the signatory and capable of identifying them. QES is the most secure form of electronic signature and is based on a qualified certificate issued by a qualified trust service provider (QTSP). QES have the same legal effect as a handwritten signature and are recognized in all EU member states and the UK. However, national law still determines the legal effect of electronic signatures, and some categories of contracts may be exempt from the general rule that contracts can be concluded electronically. It is important to understand the interaction between eIDAS and national law when using electronic and digital signatures (McNeal, 2019).

The ESIGN Act, which was enacted by US Congress on June 30, 2000, establishes regulations that make electronic signatures uniformly recognized throughout the United States. Signatures that meet the criteria outlined in the ESIGN Act are considered as legally valid as those made by hand. Before the ESIGN Act, the Uniform Electronic Transactions Act (UETA) was passed by the National Conference of Commissioners on Uniform State Laws in 1999 to establish a legal framework for electronic signatures in the U.S. While the UETA is enacted at the state level, the ESIGN Act is a federal regulation. Currently, 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted the UETA, and New York, Illinois, and Washington have adopted comparable laws concerning electronic signatures (Lamachenka, 2022).

Security

For the e-signature software to be secure, we need to consider what are the possible threats and risks, how can we ensure safety, and what measurements should be taken into account for e-signature.

The use of electronic signatures comes with risks that companies need to be aware of. Some of these risks include signers claiming that they signed a different document, man-in-the-middle attacks, internal fraud, and signers not understanding the legal implications of their signature. These risks can be mitigated by presenting documents in PDF/A format, having service providers sign documents before presenting them to signers, demonstrating industry best practices, and creating long-term digital signatures with embedded timestamps. Additionally storing user keys in tamper-resistant hardware security modules, including legal notices for signers to approve, allowing initials to be used against important paragraphs or on each page, and displaying a clear sign, approve, and decline buttons in appropriate languages (Crook, 2018).

Government-issued electronic identification (eID) typically consists of three main components: identification data, user profile data, and authentication credentials. Privacy concerns can arise due to the collection and processing of personal information in eID systems, so it is important to minimize the amount of personal information collected and protect against unauthorized access to identity tokens. To ensure appropriate identity validation and verification, it is necessary to associate the claimed identity with the applicant providing identity evidence and limit the collection and processing of personal information to the minimum necessary to validate the claimed identity (Erdogan & Saran, 2021). Additionally, the e-signature software should have audit trails, cloud security, and authentication methods. Companies must provide evidence of their business processes during compliance audits, and it is essential to capture a thorough audit trail of the signing process. An ideal e-signature solution should record various details about the signature process. Such as IP addresses, timestamps of all events, all documents presented, time spent reviewing each document, and all actions taken during the transaction, including what each party acknowledged, agreed to and signed (Mulliner, 2022).

The e-signature platform should as well employ robust encryption methods to secure data during transit and storage, and that data is stored within an encrypted database volume to ensure secure communication. It is advisable to consider software that collaborates with reputable cloud infrastructure services providers such as Amazon Web Services, IBM Cloud, or Microsoft Azure. As these providers adhere to security best practices and comply with various regulatory, industry, and IT standards for

security and data protection, including ISO 27001, SOC 1/2/3, HIPAA, FIPS 140-2, FISMA, and others (Mulliner, 2022).

Another encryption method is 256-bit encryption. This encryption is a highly secure technology that uses a 256-bit key to encrypt and decrypt data exchanged between a server and a client. By encrypting data with a 256-bit long key, this technology ensures the security of online communication between two nodes. Additionally, 256-bit encryption is among the most advanced and secure technologies available today due to its key length and computational complexity (Ahmad, 2022).

The software must have strong encryption mechanisms and authentication measures to ensure that the e-signature is secure and protected from unauthorized access, as well as the software should provide a reliable audit trail and log of all activities related to the signing of documents. So, to ensure security, an authentication process has to be incorporated.

Authentication methods

Authentication factors are used to verify a person's or device's identity. These factors can be divided into three categories: knowledge-based (something the user knows, like a password), possession-based (something the user has, like a physical token or a phone), and inherent (something the user is, like a fingerprint). The number of factors used in an authentication system can vary, with two-factor systems using two factors and three-factor systems using three, or multi-factor authentication (MFA) systems (Erdogan & Saran, 2021).

Multi-factor authentication (MFA) requires more than two authentication factors for access and offers higher security. However, it can result in a negative user experience and be challenging to manage for IT teams. Adaptive authentication adjusts its security level based on the user's risk level, allowing for a range of access options based on the context of the user and the situation. Based on the confidentiality level of the document, a number of authentication methods can be assigned to ensure the safety of the document. This approach provides a more robust authentication measure, which is essential as more companies use the cloud and security breaches become more common (Karlinsky, 2021).

Identity as a Service (IDaaS) is a cloud-based authentication managed by a third-party provider. Enterprises subscribe to the services of IDaaS companies for cloud-based identity management to verify user identities and grant appropriate access to resources. Implementing an in-house identity management system can be challenging and time-consuming, whereas a centralized, cloud-based system provided by experts in the field offers a simpler solution and has already been tested and refined by numerous organizations (Karlinsky, 2021).

One of the authentication methods is electronic identification. There have been several technologies proposed for electronic identification (eID) credentials, including smart card-based identification, mobile identification, and citizen card concepts. These solutions can be further divided into different types, such as contact smart cards and contactless smart cards, which connect to a reader through physical contact or short-range interfaces. Making eID systems usable is important for their widespread adoption, and according to a commission report, eID systems should be useful, easy to use, desirable, findable, and credible. Ensuring usability is a challenge, as eIDAS promotes the widespread and seamless use of secure eID throughout the European Union (Erdogan & Saran, 2021).

Integration

Interoperability refers to the ability of a system or product to work with other systems or products without requiring special effort from the user. This includes both the holder of the electronic identification (eID) and the recipient of electronic communication. There are two main issues related to interoperability: cross-border operability and fragmentation. Cross-border operability refers to the ability of citizens to access applications in other countries, which is important for Vervo as many clients and partners are international. Fragmentation, on the other hand, is a common issue with identification

systems, as it involves separating identification structures to meet sector-specific needs without establishing standards. This can lead to confusion and difficulty in cases that require interoperability across national boundaries. Additionally, the use of different implementations and sector-based solutions for identity validation can make the system more complicated for end-users (Erdogan & Saran, 2021).

The European Committee for Standardization has developed an architecture for an interoperable eID system using a smart card infrastructure in Europe. In 2019, a number of notified schemes based on eID cards with a high level of assurance were in use in several European countries, including Italy, Estonia, Spain, Croatia, Luxembourg, Belgium, Czech Republic, Latvia, Lithuania, Slovakia, Germany, and Portugal. In addition to smart card-based solutions, mobile technologies also have a range of international standards for secure cryptographic applications, such as OTP (One Time Pad) and Mobile Connect (an initiative from the GSMA that aims to establish new digital authentication standards) (Erdogan & Saran, 2021).

Because the e-signature software has to be interoperable with Onfrex, an API is a must. The electronic signature application programming interface (API) makes it easier to request signatures, track status updates, and manage important documents. An e-signature API is a Representational State Transfer (REST) web service that allows subscribers to securely request electronic signatures online, obtain status updates, and download completed documents. Developers use API endpoints to make API calls, and the responses are returned in JSON format. Digital signature APIs are authenticated and binding and are useful for businesses that require a secure and efficient way to obtain signatures on their contracts. These APIs provide a secure way to transmit files and sign multiple PDF documents at once. Developers can expect to create applications with document signing functionality faster, while businesses can free up their time and complete more projects on schedule (Fang, 2021).

Usability and mobile accessibility

Usability-related attributes include the user interface, help options, support for mobile devices, and offline support. The user interface should be intuitive and easy to use, with aesthetically pleasing graphical elements. Help options should include user manuals, eLearning modules, and context-sensitive help. Support for mobile devices is important so the software is accessible anywhere. Offline support allows users to continue working on the system even when they are not connected to the internet, and then synchronize their work once they are back online (Godse & Mulik, 2009). Overall, software deployment should be taken into account. Software deployment refers to the process of getting a new computer program or software up and running, which includes activities such as installation, setup, testing, and editing. Additionally, deployment can also refer to the implementation of software updates, patches, or new features to existing software or applications. The software has to be accessible not only via the web, but also through different operating systems, such as Windows, Mac, or Linux (Altvater, 2020).

Cost

The cost factor for software systems consists of annual subscription fees and one-time implementation costs. In case of SaaS the the costs are with subscription. Annual or monthly subscription fees often cover the cost of software and support staff, while one-time implementation costs cover the expenses of initial consulting and configuration (Godse & Mulik, 2009).

Scalability

Scalability in software systems refers to the ability of a system to handle increased demands without negatively affecting performance or requiring major changes to the system's design. A system that can adapt to changes in the environment and still meet the needs of stakeholders is considered

scalable. Different factors can describe scalability. These factors denote the features of the application domain and machine that can influence the system's behavior. These factors include the input data volume, the work arrival rate, the number of simultaneous users, the maximum cache and thread pool size, the number of nodes in a server cluster, algorithm selection, and cost (Duboc, Rosenblum & Wicks, 2007).

2.7. Multiple Criteria Decision Making

Real-life problem-solving often involves considering multiple perspectives that compete with one another, requiring careful consideration to reach a reasonable decision. Formally, a decision can be defined as a choice made based on available information or an action plan aimed at resolving a specific problem. In practical terms, multiple-criteria decision analysis (MCDA) is used to assess various courses of action or options by selecting the most preferable alternative or arranging the options from best to worst. MCDA plays a crucial role in guiding decision-makers by identifying the best rational alternative, particularly when allocating limited resources among competing and alternative interests (Basilio, et al., 2022).

Multiple Criteria Decision Making (MCDM) encompasses various elements and concepts that are tailored to the specific decision-making problem at hand. These elements include alternatives, attributes, aggregation, decision variables, decision space, measures, criteria, preferences, and different types of decisions. By considering these elements, MCDM provides a framework for evaluating and selecting the most appropriate alternative based on multiple criteria. It enables decision-makers to assess the performances of alternatives, quantify their attributes, and compare them based on desired consequences. Ultimately, MCDM aids in making informed decisions that align with decision-makers needs and objectives (Taherdoost & Madanchian, 2023).

2.8. BPMN

The process flows of signing CMR and eCMR are drawn by using Business Process Model Notation 2.0 (BPMN 2.0). BPMN is an international standard (ISO/IEC 19510) that describes a process in a structured, coherent, and consistent way that helps to understand, document, analyze and execute business processes (Häußler & Borrmann, 2021). BPMN diagrams enable diverse stakeholders to visually comprehend business processes, simplifying the task of improving workflow effectiveness and efficiency. Whether it's business analysts, developers, or business managers, all individuals involved can effectively communicate and understand the processes, allowing them to confidently adapt to new situations. This shared understanding ensures seamless collaboration and empowers stakeholders to navigate changing circumstances with utmost assurance (IBM, 2022). Therefore, to show to the management of Vervo the process of CMR convention and signing eCMR, BPMN is used, as it is a universal and comprehensive notation.

The process of signing the CMR note is explained by using activities, such as making an order and transporting the goods. The main events used in the process are: start and end events, throwing and catching events, in our case, the message is thrown and caught, and the CMR note is given/sent and received, respectively. A parallel gateway shows that the activities "give goods" and "sign CMR" can happen simultaneously because in practice the goods might be given before or after signing the CMR note. All participating parties are put in a pool and divided into lanes. At last, the flow objects are connected with sequence flow and message flow.

In the case of signing eCMR, the main activities and events are the same as it was in the CMR note signing process. Additionally, the parallel gateway is used to show that, for example, the consignor

can give the goods and sign the eCMR at the same time. The participant parties, consignor, carrier, and consignee, as well as, the e-signature software has their own lanes, to show the relationship between each other, and how they are connected by using sequence flow and message flow. To visualize the process in a readable and understandable manner, subprocesses are made, where we show the process of what happens in the e-signature software when a user wants to authenticate or verify their e-signature and how the signing process is carried out.

3. Operationalizing the Method

In the following chapter, firstly, we will elicit requirements from Vervo, construct a comparison criterion, and rate each e-signature software. Afterward, we will analyze and evaluate, which digital signature is the best possible option for Vervo.

3.1. Requirement elicitation

The task of selecting a suitable software platform poses challenges due to the multitude of factors and criteria that decision-makers must consider. The goal is to identify the most optimal solution that aligns with the organization's specific requirements (Krisnawijaya, et al., 2023). Therefore, interviews are conducted, so we elicit requirements and find the best option for signing documents digitally.

3.1.1. Data collection method

Interviews were performed with Vervo's CEO and Business Development Manager, other employees of Vervo did not participate in the research because they do not sign consignment notes. In the case of Vervo, the questions are made both closed-ended and opened-ended, for example, different methods of authentication are available and Vervo has to choose which ones to use, whereas the budget can only be determined by asking an open-ended question. The interview questions can be seen in Appendix 1.

3.1.2. Vervo requirements

Taking into account all the features and requirements found in the literature, by eliciting requirements from Vervo, we learn what Vervo wants that the e-signature software platform should provide.

As Vervo prefers to not be responsible for maintaining or developing its own e-signature software, the SaaS is the best option to consider as the service is provided by a third party. Therefore, the characteristics of a SaaS model are considered. Besides general requirements of a SaaS, such as functionality, usability, costs, and others, we asked about characteristics specific to e-signature software, namely, legal aspect, authentication possibilities (Watts & Raza, 2019), and most importantly, it can be used for signing eCMR.

Hence, for Vervo the e-signature software has to provide the possibility to sign the eCMR, which means that eCMR has to be signed by three different parties, and that can be from three different countries. Hence, e-signature software has to be available worldwide and can ensure local legal regulations.

In order to provide a safe authentication process and ensure that the signing person has the authority to sign, Vervo notes that the authentication should be made with two authentication methods, which can be a combination of passwords, smart cards, biometrics, or through bank accounts, and clients and users can choose with methods to use.

The software should be able to integrate with other systems and processes used by the organization, in the context of Vervo, that is Onfrex with API. The e-signature software should be easy to use and understand, with clear instructions and a user-friendly interface that allows users to sign documents quickly and efficiently. Especially, consignors and consignees, as well as the driver should be able to sign the eCMR from anywhere, to have the possibility to sign the document on the go, that is, by having mobile accessibility, which can be either through a Web browser or an app.

The software should be cost-effective, with pricing that is transparent and fair and provide a reasonable return on investment for Vervo. Vervo cannot tell us the precise budget as it is confidential, however, they can inform us that they rather pay for a number of transactions of documents rather than a software user. And for one digital document, the maximum they are willing to spend is between 0.15 EUR to 0.50 EUR to the service provider.

For Vervo, the e-signature software platform should be able to process thousands or even hundreds of thousands of users just to sign one eCMR document, as three different parties have to sign it. In Latvia alone, around 2 million CMRs are signed each year (Licite-Kurbe & Ozolina 2022). This indicates that e-signature software has to process approximately this amount of eCMR documents, and with growing demand for import and export, the number of shipments will increase, meaning, the e-signature software has to be able to adjust and grow.

3.1.3. Specified requirements

After literature studies and interviews, a list of requirements is presented (Table 5). For each specific requirement, a summarized description is added of what exactly Vervo wants.

Requirements	Vervo requirements
1. Security	Compliance with all necessary regulations and standards: ISO 27001, SOC 1/2/3, HIPAA, FIPS 140-2, FISMA, SSAE 16, 256-bit HTTPS encryption
2. Legal compliance	Compliance with all necessary regulations and laws locally and nationally: GDPR, eIDAS, HIPAA, UETA, CCPA, and others
3. Authentication	Users can choose any 2-factor authentication method
4. User experiences	High customer satisfaction (closer to 5 stars) and positive reviews
5. Integration	Can be integrated with Onfrex via API
6. Deployment	The software can be accessed from the Web or can be installed on any desktop (Windows, Mac, Linux)
7. Mobile accessibility	Can be accessed from Web or App
8. Cost	For one document costs is from 0.15 EUR to 0.50 EUR.
9. Customization	The document can be customized with logos, dates, etc.
10. Technical support	For technical difficulties, Vervo can reach the software provider in short time
11. Multiple signatories	The document can be signed by at least 3 different persons
12. Support for multiple languages	The software is translated into many languages, mainly should be available in English, Russian, Polish, Estonian, Lithuanian, and Latvian.
13. Scalability	The software can adjust and integrate Vervo needs: unlimited users and document transactions
14. Worldwide availability	The software can be used and is available anywhere in the world

Table 5. List of requirements of Vervo for the e-signature software platform

3.2. Comparison criterion

In this section, a comparison between the chosen five e-signature software platforms will be performed. Comparison is achieved by assigning a value from 0 or 1. The legend of values and their meanings is in Table 6. The value “0” means that does not fulfill the needs of Vervo, whereas the value “1” is assigned to a requirement that is fulfilled.

Value	Meaning
1	Fulfill Vervo requirements
0	Does not fulfill Vervo requirements
–	Information could not be found

Table 6. Values and their meanings

3.3. Comparing software platforms

After constructing the scale, we can now assign values to each requirement corresponding to each e-signature software platform. The comparison can be seen in Table 7. For requirements that cannot be valued, such as the average rate out of 5 stars (user experience), the number of countries where the software is available or the number of languages that this software provides, the exact number is given. Furthermore, in the “Costs” section, an abbreviation for the internal user and month is shown by “u” and “m”, respectively.

Requirements/Characteristics		DocuSign	eversign	Dropbox Sign (HelloSign)	Adobe Acrobat Sign	SignNow	eID Easy Docs
Location		USA	Austria	USA	USA	USA	Estonia
Security		**1**	**1**	**1**	**1**	**1**	**1**
Legal compliance		**1**	**1**	**1**	**1**	**1**	**1**
Authentication	**User can choose different methods**	**0**	**0**	**0**	**1**	**0**	**1**
Deployment	**SaaS, Cloud, Web-based**	**1**	**1**	**1**	**1**	**1**	**1**
	Is available on desktop	**1**	**1**	**0**	**1**	**1**	**0**
Integration	**API**	**1**	**1**	**1**	**1**	**1**	**1**
Mobile accessibility	**Web**	**1**	**1**	**1**	**1**	**1**	**1**
	App	**1**	**0**	**0**	**1**	**0**	**0**
Customization		**1**	**1**	**1**	**1**	**1**	**1**
Technical support	Email/Help Desk, FAQs/ Forum, Chat	**1**	**1**	**1**	**1**	**1**	**1**
Multiple signatories		**1**	**1**	**1**	**1**	**1**	**1**
Scalability	**Unlimited users and transactions**	**0**	**0**	**1**	**0**	**0**	**1**
User experience		4.7	4.8	4.7	4.65	4.6	4.8
Multiple languages	Supports needed languages	1	0	0	0	0	0
Worldwide availability		180 countries	150 countries	180 countries	**–**	**–**	**–**
Costs		**$20/u/m – $125/u/m** DocuSign Enterprise: negotiable	**$9.99/u/m – $79.99/u/m**, Volume pricing: negotiable Extra costs for API.	**$15/u/m – $25/u/m** API: starts at **$75/month** Premium: negotiable	**€18,14/u/m – €29,03/u/m** Acrobat Sign Solutions: contact for quote	**$8/u/m – $50/u/m** Specific plan: negotiable	Cost differs per country and signature levels: **€0.00 – €1.50**

Table 7. Comparison between e-signature software and their corresponding characteristics

3.4. E-signature software evaluation

In Table 5 at first glance, it may seem that the best option would be Adobe Acrobat Sign, however, we cannot make a conclusion without considering other alternatives, therefore, to clearly see which software would be the best option, we will evaluate every requirement per software.

Firstly, for Vervo security and legal compliance aspects are very important, from the table, we can see that every software fulfills the need (Software Advice, n.d.).

Furthermore, the best authentication is for Adobe Sign and eID Easy, because the client (user) can choose which authentication method to use: via bank account, smart ID, or another strong and safe method. Whereas for other e-signature software platforms, only limited two-factor authentication is possible via e-mail and a unique access code or SMS. However, for eID Easy Docs to authorize it can cost, as can be seen in Appendix 2 (eID Easy Docs, n.d.).

In the case of deployment, every software is SaaS, Cloud-based and Web-based, however, only Adobe Acrobat Sign can be additionally installed on desktops of Windows, Mac, Linux, and Chromebook. The rest of the software platforms except eID Easy Docs, are available only on Windows and Mac. And eID Easy is available only as SaaS, Cloud, and Web (Software Advice, n.d.). In the context of Vervo's needs, it is not essential to have the platform on a desktop, as long as it is available on any device.

This brings us to the requirement of mobile availability, almost every software has an application, that is, it can be installed and is available on iPhones, Androids, and some even on iPads. However, only eID Easy Docs can be accessed through a web browser (Software Advice, n.d.). Because Vervo has many clients and partners, the collaboration dynamics between these parties change, that is, most of the time we work with the same carriers and clients. However, sometimes we cooperate with transport or client once, and the sender and receiver can be a different person or company than the service payer, which means that there is a possibility that any previously mentioned party will probably sign the eCMR once. Therefore, there is no need for everybody to install the app to sign the eCMR once, hence, if the software is available on the Web and can be reachable from any part of the world, then the Vervo requirement is fulfilled.

As for the feature of customization and the possibility to add multiple signatories, every digital signature software can provide this feature, which means that every software allows users to add logos and stamps to the document, as well as more than one person can sign it. Along with the possibility to specify the sequence of signers, for example, the receiver cannot sign the eCMR if the sender has not signed it yet. This constraint is exactly what Vervo needs, that the eCMR is signed in the right order and the process cannot proceed without a signature (Capterra, n.d.; Software Advice, n.d.).

As regards technical support, every software handles customer questions and problems, if those arise, through Email/Help Desk, FAQs/Forum, Knowledge Base, 24/7 (Live Rep), and Chat. Where eID Easy Docs helps their customers only via Email/Help Desk, FAQs/forum, and Chat (Software Advice, n.d.). However, in the first row of Table 5, we have added an extra characteristic: the location of the software provider. This is useful to know in this case, when Vervo needs technical support. Considering time zones, it is more convenient to choose a software company that is closer to Vervo headquarters. As can be seen, the headquarters of DocuSign, Dropbox Sign, Adobe Acrobat Sign, and SignNow are located in the USA, where eversign is from Austria and eID Easy Docs is from the neighboring country of Latvia: Estonia (Software Advice, n.d.). For Vervo it would be more convenient to choose eID Easy Docs, as technical activities, such as integrating Onfrex with eID Easy Docs, and other agreements can be done in person.

In the context of scalability, and how the digital signature software platform can adjust to the growing logistics industry, it can be seen that only Dropbox Sign and eID Easy Docs can provide what Vervo is looking for. Because the users can send, sign and receive an unlimited number of documents

per year (eID Easy Docs, n.d.). This aspect for Vervo is very pivotal. Where, for example, in the case of DocuSign, the defaulted maximum number is 50 Signing Groups. 50 is also the maximum number of users that can be added to a single Signing Group. This limit cannot be raised. Additionally, the maximum number of documents that one user can sign is 150 documents per year (DocuSign, n.d.). For Vervo this is a major constraint because one manager in Vervo has at least 50 clients and there are hundreds of transport providers. This means that only a limited number of documents one manager can send, which leads us back to our core problem where the hard CMR copy is printed, scanned, and so on.

Moreover, DocuSign has its services in 44 languages, and Adobe Acrobat Sign and DropBox Sign are available in 34 and 22 languages, respectively. Further, eversign is in 13 languages, and eID Sign Docs is in 11 languages. Lastly, SignNow is available only in English (Software Advice, n.d.). Although the language aspect is not a priority for Vervo, they appreciate it if the software can be accessible in languages used daily by Vervo employees, clients, and partners, and those are, Latvian, English, Polish, Russian, Lithuanian, Estonian, and German. Other languages are a plus. Only DocuSign can provide their services in all mentioned languages.

Apart from the possibility of services in multiple languages, the software should be available in many countries as well. Both DocuSign and DropBox Sign are obtainable in 180 countries, and eversign in 150 countries (Software Advice, n.d.). Unfortunately, for Adobe Acrobat Sign and SignNow, the exact worldwide availability could not be found, as well as for eID Easy Docs, however, the approximate list of countries where eID Easy Docs is accessible depends on the digital signature authentication and signature methods. For example, Smart-ID is used only in Latvia, Estonia, and Lithuania, whereas, the identification platform that provides Qualified Electronic Signatures (QES) services, the ZealID app is available in 26 countries. The full list of each identification method and their converge, price and level of the signature for using eID Easy Docs can be seen in Appendix 4 (eID Easy Docs, n.d.).

The last requirement we discuss is cost. Every software besides eID Easy Docs is purchasable for one user for one month and as a subscription. A client can buy the services for a whole year as well, but we will analyze when we have a monthly purchase. Besides the available price options, the client can contact the service provider to negotiate for personalized features and a number of users. In the case of Vervo, we will evaluate the giving pricing options. As mentioned, every software delivers a subscription for one user, except, DocuSign has a possibility for $125/u/m, where are 10 service users and unlimited sends. Whereas eversign has a case where for $79.99/u/m 15 users (DocuSign, n.d.; eversign, n.d.). These alternatives do not work for Vervo, as there are more than 50 employees in the company and hundreds, even thousands of clients and carriers. On the other hand, eID Easy Docs might be a good option. For eID Easy Docs the number of users and the possibility to send documents is unlimited, however, each document and authentication method has its costs. To use a specific authentication method, the costs differ, for example, to use a Latvian ID card, costs nothing, whereas to verify using the mobile application eParaksts, costs €0,06. The costs for different authentication methods and digital signature methods that eID Easy Docs provides can be seen in Appendix 2 and Appendix 4. Overall, for Vervo it is essential that Vervo managers can send unlimited documents to sign and have the opportunity for Vervo service users to sign it anywhere and with any safe electronic signature method (eID Easy Docs, n.d.).

For us to better understand which requirement is crucial for Vervo and which are less, we asked Vervo management to assign priority levels for each criterion. Value “3” – high priority, value “1” – low priority. See Table 8.

Requirements/Characteristics	Priority
Security	3
Legal compliance	3
Authentication	3
Deployment	1
Integration	3
Mobile accessibility	2
Customization	1
Technical support	2
Multiple signatories	1
Scalability	3
User experience	1
Multiple languages	1
Worldwide availability	2
Costs	3

Table 8. Vervo priority levels per requirement

After assessing each requirement, we can compare the chosen e-signature software platforms against the priories that Vervo management has assigned. The scores are multiplied by the corresponding priority levels. The multiplied scores are then summed up to calculate a total score for each alternative. This total score represents the overall evaluation of the alternative, taking into account the priority of the criteria. See Table 9.

Requirements/ Characteristics		Priority	DocuSign	eversign	Dropbox Sign	Adobe Acrobat Sign	SignNow	eID Easy Docs
Security		3	**3**	**3**	**3**	**3**	**3**	**3**
Legal compliance		3	**3**	**3**	**3**	**3**	**3**	**3**
Authentication		3	**0**	**0**	**0**	**3**	**0**	**3**
Deployment	**Cloud, Web-based**	1	**1**	**1**	**1**	**1**	**1**	**1**
	Is available on desktop	1	**1**	**1**	**0**	**1**	**1**	**0**
Integration	**API**	3	**3**	**3**	**3**	**3**	**3**	**3**
Mobile accessibility	**Web**	2	**2**	**2**	**2**	**2**	**2**	**2**
	App	2	**2**	**0**	**0**	**2**	**0**	**0**
Customization		1	**1**	**1**	**1**	**1**	**1**	**1**
Technical support	Email/Help Desk, FAQs/ Forum, Chat	2	**2**	**2**	**2**	**2**	**2**	**2**
Multiple signatories		1	**2**	**2**	**2**	**2**	**2**	**2**
Scalability		3	**0**	**0**	**3**	**0**	**0**	**3**
Multiple languages		1	**1**	**0**	**0**	**0**	**0**	**0**
Total score			**21**	**18**	**20**	**23**	**18**	**23**

Table 9. Total scores for each option

Based on the comparison and evaluation section, and total sums scored from implementing priorities, we consider Dropbox Sign and eID Easy Docs. In Table 9, we have not assessed costs, worldwide availability and languages with values, as for each option it cannot be compared with a certain value.

The trade-off is that eID Easy Docs have better pricing options than Dropbox Sign because Vervo will not pay for every client and partner's profiles, Vervo can only settle the transactions of the authentication and signing methods, as well as that eID Easy Docs have safer and stronger authentication methods, whereas Dropbox Sign has only two-factor method: email and SMS.

Nevertheless, Dropbox Sign has better security. And both software platforms ensure legal compliance with all regulations and laws and can be integrated via API with Onfrex. Additionally, Dropbox Sign can be used through any device, whereas eID Easy Docs only be via the Web browser, which should not be an issue, as long as it can be reachable from anywhere. Comparing the scalability aspect, for Dropbox Sign, one user can send unlimited documents, however, the constraint is that Vervo cannot ensure for every Vervo service user has their personal profile. Alternatively, eID Easy Docs can be accessible with any authentication method depending on the user's location and preference. Therefore, after taking everything into consideration, and from the priority comparison, the software that fulfills most of the Vervo requirements is eID Easy Docs, because eID Easy Docs can provide the most important features that Vervo is looking for.

4. Process flow diagrams

By showing the process flow diagrams of the CMR and eCMR, we can better see and understand the differences in how the notes are being processed and signed, and passed on, starting from the carrier and later from the consignor to the consignee physically and digitally.

4.1. The process flow of CMR convention

In theory, the process flow of signing the CMR note is not explicitly described, therefore, the process is drawn based on our perspective and understanding of the process, as well as with unstructured interviews gained knowledge of Vervo employees. Overall, the process flow shows how the CMR note is being signed when the service buyer is the consignor and what happens with the CMR note throughout the process of shipment.

The process (Figure 2) starts when an order is being placed, in the context of research, we assume that the order is made by the consignor. In that case, the consignor sends the order with all the information about the cargo and other formalities to the carrier, and that is when the process starts for the carrier. Mostly carrier issues the CMR consignment note, however, consignor or consignee can publish it as well. When collecting the goods from the consignor, the consignor checks that everything is correct and signs the CMR note. And when delivering the goods at the destination, the CMR note is given to the consignee, and the CMR note is signed when the shipment has been received and the order is finalized. Lastly, the last copy with all the signatures from all three parties is sent to the consignor via post. The one who orders and pays for the shipment service will need the original documents, therefore, in our case, the consignor will require not only their copy but the original CMR note as well.

In the case of research, the neutralization of the CMR note is not considered. A neutralization is an exchange of the original copies of the consignment note with other transport consignment notes or documents. Shortly, the first transport note is canceled. This activity is not defined in the law or CMR Convention, therefore, it is difficult to evaluate the effect the neutralization has on the sender, receiver, and carrier (Poliak et al., 2020). Hence, in the research, we look only at the process when the original consignment note is made by the carrier and it is signed by the consignee when goods are received at the destination.

Challenges and problems that arise from this type of process and activities are that the information on the CMR note is not always clear and readable, especially if the paper document is damaged (smudged), and the CMR note can be easily lost. As this can lead to a debate between seller and buyer and transportation companies (Licite-Kurbe & Ozolina 2022). In the research, the process is simplified, however, in reality, we need to consider occasions when the CMR note might not provide clear evidence of the actual transfer to another party at a particular time and place, for example, when neutralization takes place. And moreover, the cost of one CMR note is relatively high, that is, the documentation process costs and the material costs to produce the CMR consignment note can cost more than 5 EUR (Licite-Kurbe & Ozolina 2022). Overall, by executing such a process, there is no transparency, transportation control, and monitoring, and the information cannot be easily accessed, actually the opposite, can be defrauded.

As a service buyer, Vervo typically receives the CMR note via email or post and then has to scan it to make it available in digital form. In some cases, the CMR note may be photographed, but the resulting image is often blurry and unreadable. When information is missing from the CMR note and it is scanned, it has to be printed out, manually add the missing information, scan it again, and send it via email. This creates unnecessary and time-consuming extra work. Vervo is not the only logistics company facing this paperwork problem, which is why the EU has established the eCMR protocol and e-signature protocol to make the signing and executing of the CMR convention process more efficient.

While the current process has some advantages, the disadvantages outweigh them, making it critical to shift toward the eCMR system.

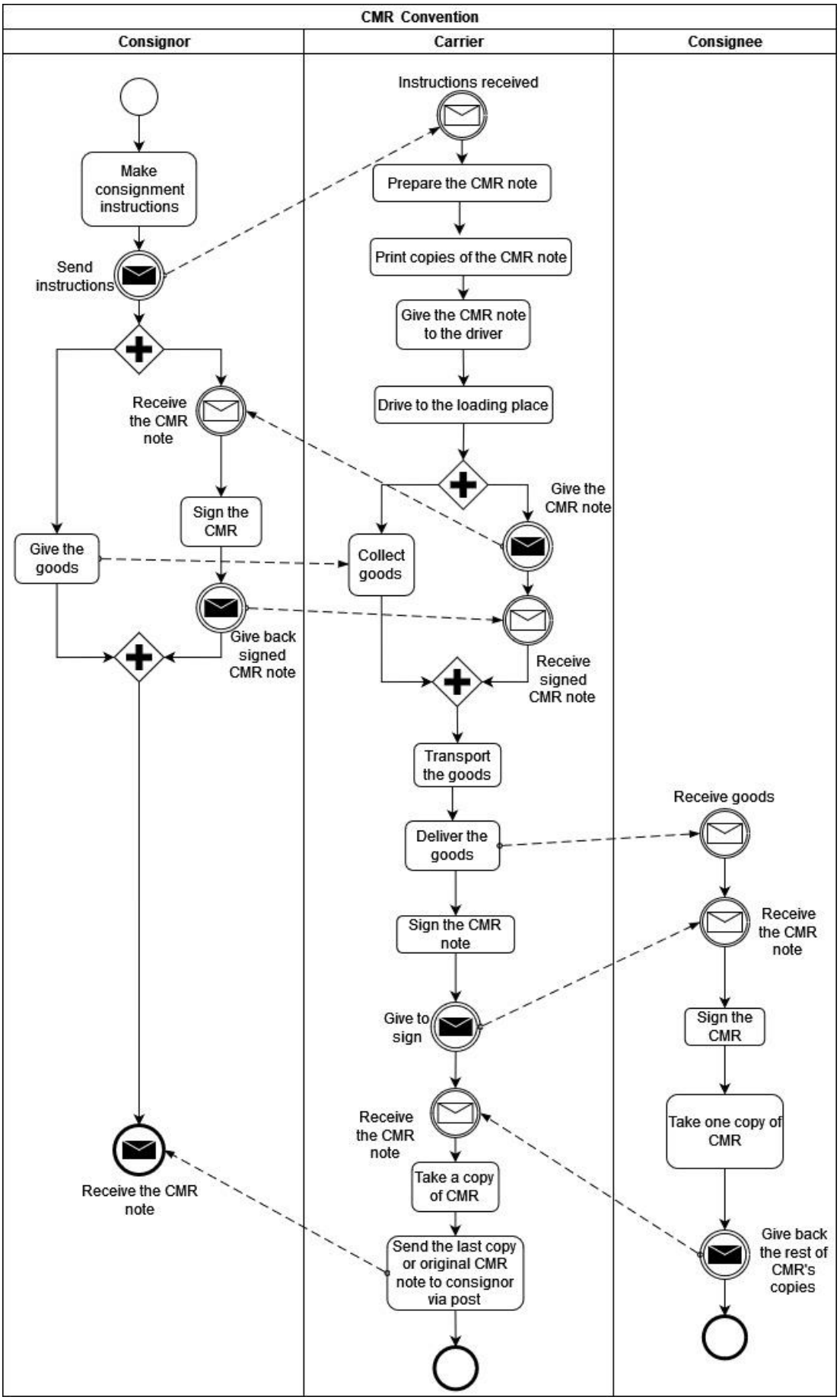


Figure 4. Process flow of CMR Convention

4.2. The process flow of signing eCMR using the chosen e-signature software

After selecting the electronic signature software, we can show the process flow of how the eCMR can be signed using eID Easy Docs.

In the case of our research, the process starts when the consignor sends information to the carrier. Therefore, for all participating parties to be able to sign the document, we assume that the carrier uploads the eCMR note through eID Easy Docs provided API. However, before uploading the document, the carrier has to authenticate.

To sign a document electronically, they must authenticate their identity before beginning the process. This step is crucial to ensure the security of the electronic signing process. The appropriate authentication method to use depends on factors such as the associated risk, the type of transaction, and whether the signatory is new or existing (Felix, 2020). Using public and private keys is considered a best practice for the authentication stage of an electronic signing process. It is done by the Person Register obtaining identity-related information from an external database. A signed data structure is returned with a unique eID and public key for the created signature key pair, without embedding the unique eID in the signing certificate to ensure privacy (Bensghir & Topcan, 2008; Rath et al., 2014). This is used to authenticate a user through the use of a private key, which is unique to the signer and can only be authenticated using a public key that has a mathematical link to the private key (Bensghir & Topcan, 2008). Appendix 3 shows all the possible authentication methods that eID Easy Docs provides and what the costs are for each method.

After the carrier has authenticated himself, they can upload the eCMR note as a PDF file through API. At this stage, the approach for presenting the documents to the signatories is determined to facilitate reading before signing (Felix, 2020).

Additionally, the e-signature solution provider can also include other signatories who are required to sign a particular document. To establish a logical sequence of events from the document's creation to its review, signing, and acceptance, a specific course of action can be triggered by certain events (Felix, 2020). It is feasible to combine different levels of signatures on a single document. However, it is preferable to let the signature requester determine whether the document should contain only Certificate-based Qualified and Advanced signatures or utilize the user's current Simple Electronic Signature process. Since a Qualified Electronic Signature does not require an audit trail, the user can avoid modifying the signed PDF in the subsequent stages. If Signature Portal lacks Qualified Electronic Signature (QES) support, it is probable that the user is altering the original PDF by appending an extra audit trail page to the end of the document. However, with QES, the signer must view the final document without any further modifications. Once a signature has been applied, the only permissible change is the addition of more signatures (Pala, 2022). In Appendix 4 can be seen every available e-signature method with their worldwide availability, signature type (SES, AdES, or QES) as well as the price per method.

When transport has uploaded the document and has arrived to collect the goods from the consignor, it is time for the consignor to sign the eCMR, to show that they agree of giving away the goods, therefore, they receive a notification. The most common method for granting access is through email invitations, which have been widely used and tested. However, in some cases, the e-signature process is integrated with a mobile or web application, allowing signatories to be invited through requests to log into a web application or portal. Other practices observed in this step include using embedded links with mobile or third-party applications, shortened URLs or QR codes on printed documents, and the involvement of a representative who starts the signing process through an enterprise dashboard or application portal (Felix, 2020). The private-pubic key algorithm is used to authenticate the user and to verify the e-signature, therefore, the subprocess as shown in Figure 6 is the same for both activities.

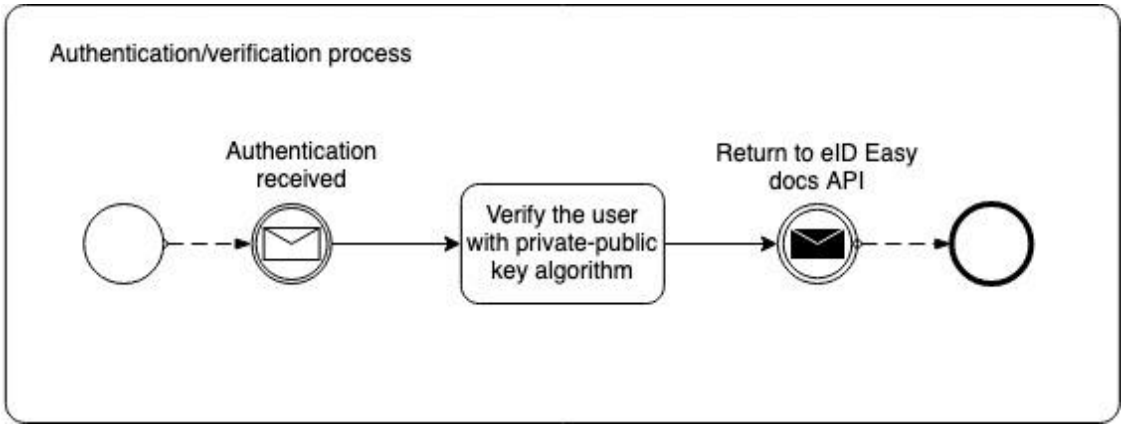


Figure 5. Authentication/verification subprocess through eID Easy Docs API

The next step in the electronic signature workflow involves obtaining the signatory's consent and acceptance, which is a crucial stage in the entire process. This is where the 'click' comes into play, and it is a common assumption about electronic signatures. Some of the best methods used for this stage include digital handwritten signatures, smartcard signing, and 'click to sign' options (Felix, 2020). For eID Easy it is explained as such, the acceptance of signing the document involves modifying the signature page based on whether the user has chosen SES or QES. If SES has been selected, nothing changes, but if QES has been chosen, a button will be displayed that initiates the signing process using eID Easy. When the user clicks on the sign button, a POST query must be made to prepare everything for QES signing. In return, a doc_id will be received, which should be used along with the previously saved client_id to set the URL parameter in the signature_redirect URL. This will allow identification of the transaction when the user returns (Pala, 2022).

The doc_id and client_id should be used to open a popup page or redirect the user to a URL template. On this page, eID Easy will show the user a preview of the document to be signed and allow them to choose the QTSP and signature solution for creating the signature. Once the signature is complete, the user can be redirected back or the popup can be closed. eID Easy will also send a server-to-server webhook notification about the completion of the signature (Pala, 2022). The signing process is presented in Figure 7.

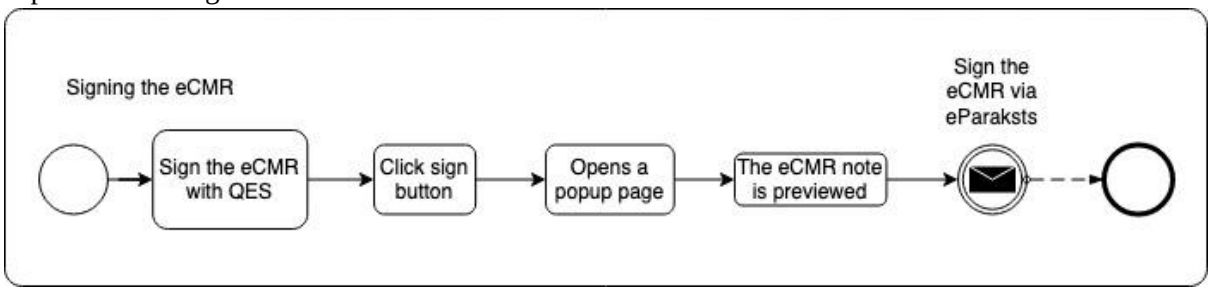


Figure 6. Signing subprocess the eCMR through eID Easy Docs API

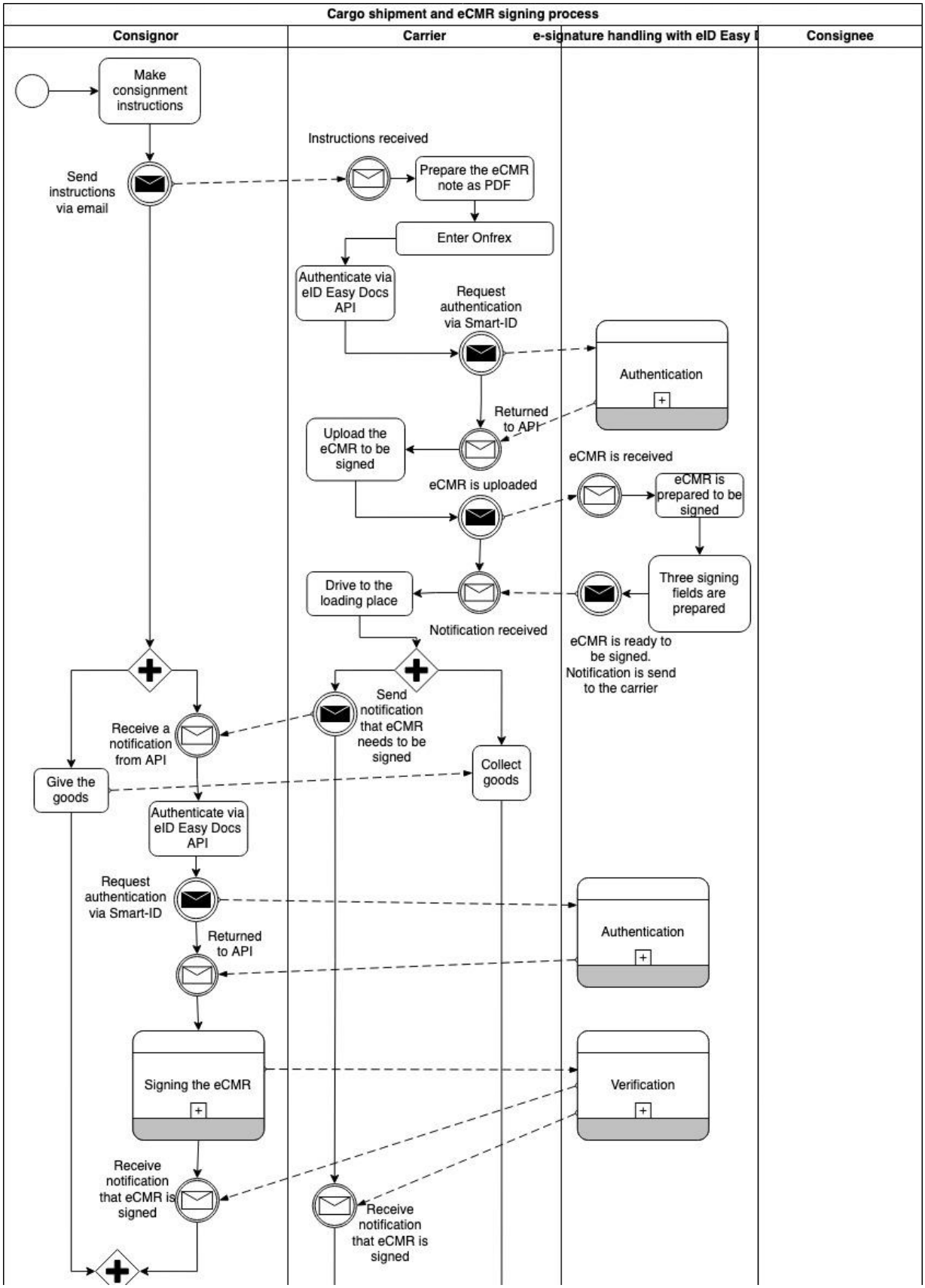
The carrier and consignor receive the message that the eCMR has been signed. The goods afterward are transported to the consignee, where the carrier signs the eCMR by first going through an authentication process and then the signing process. When the transport provider has done it, the consignee can finally sign the eCMR, that the goods have been received.

The delivery of signed documents to the relevant signatories marks the final step in the electronic signature workflow. Typically, a cloud-based storage solution is used to upload the signed documents, which can then be accessed by the signatories using their previously established credentials.

Apart from delivering signed documents, the audit trail also plays a vital role in this final stage. It serves as evidence for all the events that occurred during the transaction and must be verified before finalizing the electronic signature process. Once the audit trail is verified, each signatory is sent a URL link to the completed document, confirming that the process has been completed (Felix, 2020).

The whole signing process is shown in Figure 8. In the process, we assume that every participating party uses Smart-ID to authenticate, which is available in Latvia, Lithuania, and Estonia, and to sign the eCMR with QES an e-signature app called eParakasts, which is available only in Latvia, this means that in this process as an example, the cargo transportation is carried out in Latvia. Nevertheless, the process would be the same, if the participating parties use authentication methods to their liking. A list of all possible authentication methods and their worldwide availability can be seen in Appendix 4.

For using eID Easy Docs, there are prices for every authentication and e-signing method, hence, all the costs are calculated, and an invoice is sent to Vervo at the end of the process. It is not shown specifically in the process because charging customers for signatures may require modifying the billing system, which could be complicated and inconvenient. Therefore, it is suggested to maintain the current pricing structure, such as per user or per envelope, to avoid any such changes. To facilitate this, users can sign up at eID Easy and register their credentials on the configuration page (Pala, 2022). The pricing for eID Easy is clear and comparable to the direct integration cost of the Qualified Trust Service Provider (QTSP). The costs per method and country can be seen in Appendix 2, Appendix 3, and Appendix 4.


Cargo shipment and eCMR signing process
Consignor
Carrier
e-signature handling with eID Easy
Consignee
Make consignment instructions
Send instructions via email
Instructions received
Prepare the eCMR note as PDF
Enter Onfrex
Authenticate via eID Easy Docs API
Request authentication via Smart-ID
Authentication
Returned to API
Upload the eCMR to be signed
eCMR is received
eCMR is uploaded
eCMR is prepared to be signed
Three signing fields are prepared
Drive to the loading place
Notification received
eCMR is ready to be signed. Notification is send to the carrier
Send notification that eCMR needs to be signed
Receive a notification from API
Give the goods
Collect goods
Authenticate via eID Easy Docs API
Request authentication via Smart-ID
Authentication
Returned to API
Signing the eCMR
Verification
Receive notification that eCMR is signed
Receive notification that eCMR is signed

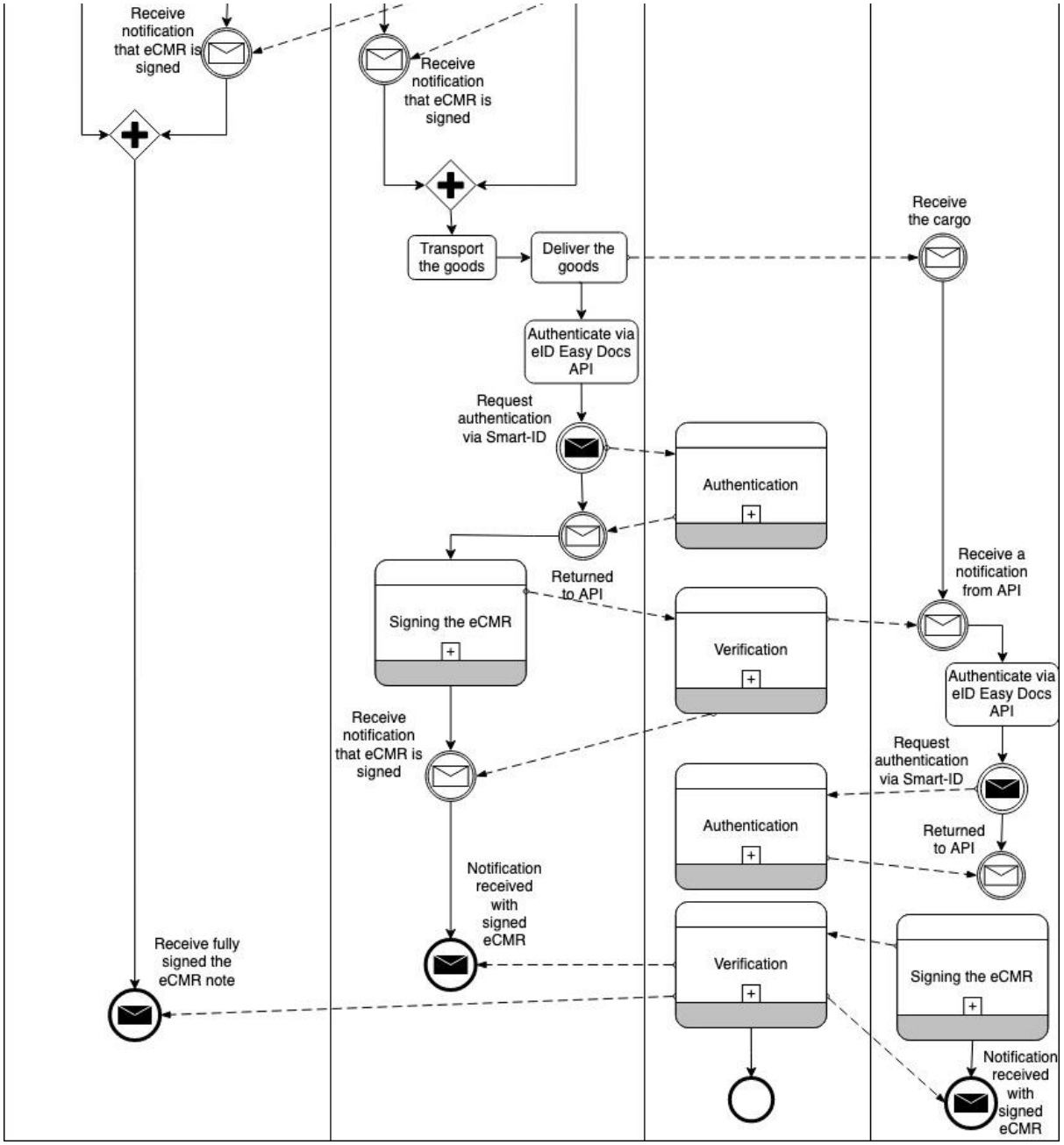


Figure 7. Visualization of signing the eCMR with eID Easy Docs

5. Conclusions and recommendations

In the final chapter, conclusions by answering the main research question, and recommendations with comments for future work are given.

5.1. Conclusions

The research aimed to find an e-signature software platform that can be used worldwide can be integrated with Vervo's software Onfrex, can be easily used for all transportation industry parties - consignors, consignees, and carriers, and has all the necessary security and legal compliances. The research question presented at the beginning of the thesis was:

Which e-signature software supports the integration of e-signatures for eCMR documents signed by shippers, receivers, and carriers and that can be compatible with freight forwarding and logistics company Vervo's Onfrex platform?

To answer the research question, first, we had to conduct a literature review to understand what exactly CMR and eCMR are, additionally learn about the e-signatures and how the algorithm of digital signing is performed. The selection of a suitable e-signature software platform started with collecting and analyzing the requirements of what e-signature software should have. We gathered list of all possible features, however, for us to compare and analyze the list was narrowed down to 15 requirements.

After researching and listing all the necessary requirements, a list of possible e-signature software platforms were given. Software platforms were selected based on their ratings and number of reviews, as well as noted the industries where these platforms are used the most. Many of them are used for simple document signing and for small user groups, which was not the case for Vervo. This software has to be able to process thousands of documents and be reachable to many users. Out of all e-signature software platforms, a comparison was made between Adobe Acrobat Sign, DocuSign, Dropbox Sign (HelloSign), eID Easy Docs, and SignNow. Every software besides eID Easy Docs had already determined subscription plans, and it was also possible to contact software providers for personalized quota. In the context of research, we did not consider the option for personalized features and price. We evaluate the platforms based on their established plans.

Next, an elaborate evaluation was made between all previously mentioned software platforms. Dropbox Sign and eID Easy Docs checked equally the requirements that Vervo managers are looking for based on priority. Therefore, a more detailed evaluation between Dropbox Sign and eID Easy Docs was executed. Although at first DropBox Sign might seem a better option, it was crucial for Vervo that the software is available for many users without extremely high costs, that is, due to thousands of clients and partners, for each user to have their own profile it would be a constraint for everybody to install such software. Therefore, a favor was towards eID Easy Docs because costs are made from different authentication methods and signature levels, and not from a number of users, and can be accessed through the Web.

At last, it is important to comprehend the current situation as to how the CMR consignment note is signed now, therefore, an analysis and process flow was presented. This analysis helped to understand better that costs and workload are high as the CMR note is printed and scanned many times, sent via post, and can be easily forged. This helped to better reason that eCMR is needed, but the challenge arose to learn how exactly the eCMR should be signed and with what tool.

Although, it was not possible for Vervo managers to try the eID Easy Docs, and because Onfrex is currently a work in progress, it is not possible to see how these two platforms exactly work together, however, what is clear is that the eID Easy Docs can be integrated with Onfrex through eID Easy Docs API. Hence, a visualization of how the eCMR can be signed using the eID Easy Docs API is presented.

5.2. Recommendations

The aim of the recommendations is to present Vervo management that before Onfrex is fully ready, it is advisable to test the eID Easy Docs and start using it in other daily activities, as well as, provide training to employees and others Vervo service users. Both these activities can help better understand the eID Easy Docs, how it works, and how to use it before it is implemented fully with Onfrex.

5.2.1 Start using eID Easy Docs

Because due to the time constraints of the research, we could not test the software during the study, and because the research was conducted for specifically signing the eCMR and how Onfrex will be used for signing it, it does not exclude the possibility that the software can be used for signing other documents besides eCMR, therefore, we advise starting using the software for signing order of shipments, invoices, and other agreements while Onfrex is still being made. As mentioned, the software was researched with eCMR in mind, however, because the eCMR system is slowly developing in Europe, it will be in force starting in the year 2026 (Ratification of the eCMR Protocol in Europe - Transfollow, 2022). Until then it would be helpful for clients and partners, and employees of Vervo to get customized with the eID Easy Docs. This will help to identify any issues or problems before they become widespread.

5.2.2. Provide support

Providing ongoing support is essential to ensuring that employees and software users are using the e-signature software effectively and efficiently. By offering ongoing training, providing a user manual, having a support team, conducting regular check-ins, addressing feedback, and keeping the software up-to-date, a company can maximize the benefits of the e-signature software while minimizing the risk of errors or issues.

5.3. Future work

The future research could be carried out in three ways, either look into the technical side as to how the software can better be integrated with Onfrex and what steps to take, that is, what commands and queries to use. Research to find out how to inform and introduce the software to employees of Vervo and their clients and partners, that is, what activities, training, and approaches so the users can feel encouraged to use such software. Additionally, investigate what clients and partners of Vervo think about the software, maybe in the scope of one country, as how they value the user experience, and what should be improved if needed.

Nonetheless, because technologies change rapidly and as mentioned previously very soon eCMR practices will be in force, this means, that when Onfrex is done, a pilot project of how the eCMR works, in reality, should be done, as how in other Europe countries many pilot projects are carried out. This might help Vervo managers to see what still needs to be added or changed to Onfrex, and how clients and transports feel about Onfrex.

6. References

Acrobat Sign. (n.d.). *e-Sign software: Electronic & digital signatures*. Retrieved February 20, 2023, from https://www.adobe.com/sign.html

Ahmad, K. (2022, June 20). *What Is AES-256 Encryption? How Does It Work?* MUO. Retrieved March 18, 2023, from https://www.makeuseof.com/what-is-aes-256-encryption-how-does-it-work/

Ahmad, K., Abdelrazek, M., Arora, C., Bano, M., & Grundy, J. (2023). Requirements engineering for artificial intelligence systems: A systematic mapping study. *Information & Software Technology*, *158*, 107176. https://doi.org/10.1016/j.infsof.2023.107176

Altvater, A. (2020, April 24). *Top Software Deployment Tools: 25 Useful Tools to Streamline Software Delivery*. Stackify. Retrieved March 18, 2023, from https://stackify.com/software-deployment-tools/

Arnaut, A. (2022, November 2). *What are Digital Signatures?* DocuSign. Retrieved April 4, 2023, from https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq
Basilio, M. P., Pereira, V., Alves, A. C., Santos, M. J. L., & Ghosh, A. (2022). A Systematic Review of the Applications of Multi-Criteria Decision Aid Methods (1977–2022). *Electronics*, *11*(11), 1720. https://doi.org/10.3390/electronics11111720

Bensghir, T. K., & Topcan, F. (2008). *E-Signature Infrastructure in Turkey and E-Signature Applications in Public Organizations.* TODAİE's Review of Public Administration. 41. 95-111. Retrieved December 27, 2022, from https://www.researchgate.net/profile/Turksel-Bensghir/publication/298463175_E-signature_infrastructure_in_Turkey_and_practices_in_public_institutions/links/5beb358c92851c6b27bd0431/E-signature-infrastructure-in-Turkey-and-practices-in-public-institutions.pdf

Brown, J. (2020, September 15). *What is scope and limitation in research?*. KnowledgeBurrow. Retrieved December 6, 2022, from https://knowledgeburrow.com/what-is-scope-and-limitation-in-research/

Capterra. (n.d.). *Digital Signature Software*. Retrieved March 3, 2023, from https://www.capterra.com/digital-signature-software/?sortOrder=most_reviews

Convention on the Contract for the international carriage of goods by road (CMR) and Protocol of signature, done at Geneva on 19 May 1956. United Nations.

Crook, S. (2018). *Get the full e-signature picture to avoid falling foul of the law.* Computer Fraud &Amp; Security, 2018(8), 12–14. https://doi.org/10.1016/s1361-3723(18)30075-7

Docusign (n.d.). *#1 in eSignature & Agreement Cloud*. Retrieved February 20, 2023, from https://www.docusign.com/

Drevinskaitė, J., Mackevičiūtė, S., Sorakaitė, G., & Jankauskaitė, S. (2019). *Peculiarities of CMR documentation in International Freight.* INDIVIDUAL. SOCIETY. STATE. Proceedings of the International Student and Teacher Scientific and Practical Conference, 28. https://doi.org/10.17770/iss2018.4248

Dropbox Sign. (n.d.). *Dropbox Sign (formerly HelloSign)*. Retrieved February 20, 2023, from https://www.hellosign.com/

Duboc, L., Rosenblum, D., & Wicks, T. (2007). *A framework for characterization and analysis of software system scalability*. Proceedings of the the 6th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering. https://doi.org/10.1145/1287624.1287679

eID Easy Docs. (n.d.). Retrieved February 20, 2023, from https://docs.eideasy.com/

Erdogan, O., & Saran, N. A. (2021). *A survey on server-based electronic identification and signature schemes to improve eIDAS: with a new proposal for Turkey*. PeerJ Computer Science, 7, e734. https://doi.org/10.7717/peerj-cs.734

European Commission. (n.d.). *What is eSignature*. Retrieved November 24, 2022, from https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/What+is+eSignature

Eversign. (n.d.). *Free Online Signatures - eversign*. Retrieved March 3, 2023, from https://eversign.com/

Fang, A. (2021, October 13). *Top 8 Best eSignature APIs & Alternatives (2021)*. Rapid Blog. Retrieved March 18, 2023, from https://rapidapi.com/blog/best-esignature-apis-alternatives/

Felix, B. (2020, April 20). *A Comprehensive Guide to Electronic Signature Workflow - LunarPen*. LunarPen. Retrieved April 5, 2023, from https://lunarpen.com/blog/electronic-signature-workflow/

Foxit Esign. (2018). *Electronic Signature EU Regulation.* Retrieved November 24, 2022, from https://www.esigngenie.com/blog/electronic-signature-eu-regulation/

Freight forwarding | Cargo | Vervo Ltd. (n.d.). Vervo SIA. Retrieved November 11, 2022, from https://vervo.lv/en/

G2 Crowd. (n.d.). *The Top 20 E-Signature Software*. Retrieved March 3, 2023, from https://www.g2.com/categories/e-signature?tab=highest_rated

George, T. (2022, December 7). *Structured Interview | Definition, Guide & Examples*. Scribbr. https://www.scribbr.com/methodology/structured-interview/

GetApp. (n.d.). *Digital Signature Software*. Retrieved March 3, 2023, from https://www.getapp.com/operations-management-software/digital-signatures/?sort=reviews

Godse, M., & Mulik, S. (2009). *An Approach for Selecting Software-as-a-Service (SaaS) Product.* 2009 IEEE International Conference on Cloud Computing. https://doi.org/10.1109/cloud.2009.74

Grant, C. A., & Osanloo, A. F. (2014). Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your "House." *Administrative Issues Journal*, *4*(2). https://doi.org/10.5929/2014.4.2.9

Häußler, M., & Borrmann, A. (2021). *Knowledge-based engineering in the context of railway design by integrating BIM, BPMN, DMN, and the methodology for knowledge-based engineering applications (MOKA).* Journal of Information Technology in Construction, 26, 193–226. https://doi.org/10.36680/j.itcon.2021.012

Heerkens, H., van Winden, A., & van Winden, A. (2021). *Solving Managerial Problems Systematically*. Taylor & Francis. ISBN: 978-90-01-88795-7

Hemeleers, R. (2022, March 14). *From document to e-CMR/eFTI dataset. The EU eFTI regulation as a unique opportunity. | 51Biz Luxembourg*. Retrieved January 6, 2023, from https://www.51biz.lu/article/eftiasanopportunity

Hurt, U. (2021). *SUMMARY OF TESTING OF THE eCMR INDEX REGISTRY PROTOTYPE VERSION 2.0 in DINNOCAP project in 2021*. ProtoTesting. Retrieved October 9, 2022, from https://www.dinnocapbsr.eu/_files/ugd/8cf6e6_c5ea4c04612441caa581a270007129d4.pdf

IBM. *The Basics of Business Process Modeling and Notation (BPMN)*. (2022, January 6). Retrieved June 10, 2023, from https://www.ibm.com/cloud/blog/bpmn

Kaba, R. (2018, July 9). *How the GDPR Will Impact E-Signatures*. Corporate Compliance Insights. https://www.corporatecomplianceinsights.com/gdpr-will-impact-e-signatures/

Karlinsky, E. (2021, April 9). *Two-Factor Authentication vs. Multi-Factor Authentication: What Are the Risks?* Okta, Inc. Retrieved February 12, 2023, from https://www.okta.com/blog/2016/12/two-factor-authentication-vs-multi-factor-authentication-what-are-the-risks/

Kevens, J. (2022, August 29). *10 Best Software Review Sites [2022]*. B2B SaaS Reviews. Retrieved March 3, 2023, from https://b2bsaasreviews.com/best-software-review-sites/

Krisnawijaya, N. N. K., Tekinerdogan, B., Catal, C., & Van Der Tol, R. (2023). Multi-Criteria decision analysis approach for selecting feasible data analytics platforms for precision farming. *Computers and Electronics in Agriculture*, *209*, 107869. https://doi.org/10.1016/j.compag.2023.107869

Lapouchnian, A. (2005). Goal-oriented requirements engineering: An overview of the current research. *University of Toronto*, *32*.

Licite-Kurbe, L., & Ozolina, Z. (2022). *Gains from introducing e-CMR by International Manufacturing Company*. 21st International Scientific Conference Engineering for Rural Development Proceedings. https://doi.org/10.22616/erdev.2022.21.tf042

McNeal, D. (2019). *eIDAS Electronic Signatures: Qualified vs Advanced - When to choose what and why*. Cryptomathic. Retrieved January 5, 2023, from https://www.cryptomathic.com/news-events/blog/eidas-electronic-signatures-qualified-vs-advanced-when-to-choose-what-and-why

Mulliner, J. (2022, May 20). *What is The Ultimate E-Signature Security Checklist?* OneSpan. Retrieved March 18, 2023, from https://www.onespan.com/blog/ultimate-e-signature-security-checklist

Nicolas, A. (2022, June 23). *Reliability and Validity*. Research Prospect. Retrieved December 6, 2022, from https://www.researchprospect.com/reliability-and-validity/

Pala, M. (2020, August 4). *Ask well designed and inclusive eID system for your country also!* Identity Based Advanced and Qualified Electronic Signature Marketplace. Retrieved March 31, 2023, from https://eideasy.com/well-designed-and-inclusive-eid-system-for-your-country/

Pala, M. (2020b, September 7). *How eID card signing works on the web*. Identity Based Advanced and Qualified Electronic Signature Marketplace. Retrieved April 6, 2023, from https://eideasy.com/how-eid-card-signing-works-on-the-web/

Pala, M. (2021, February 3). *EParaksts Latvijā*. Identity based Advanced and Qualified electronic signature marketplace. Retrieved November 24, 2022, from https://eideasy.com/eid-and-esignature-in-latvia/

Pala, M. (2022, September 10). *Qualified Electronic Signatures into your signature portal*. Identity Based Advanced and Qualified Electronic Signature Marketplace. Retrieved April 6, 2023, from https://eideasy.com/qualified-electronic-signatures-into-your-signature-portal/

Pohl, K. (2010). *Requirements engineering: fundamentals, principles, and techniques*. Springer Publishing Company, Incorporated. ISBN: 978-3-642-12577-5

Poliak, M., & Tomicová, J. (2021). *Transport document in road freight transport - paper versus electronic consignment note CMR.* The Archives of Automotive Engineering – Archiwum Motoryzacji, 90(4), 45–58. https://doi.org/10.14669/am.vol90.art4

Poliak, M., Tomicova, J., Jaskiewic, M., Drozdziel, P., & Lakhmetkina, N. (2020). *Identification of neutralization of the CMR documents in European Union conditions.* Communications - Scientific Letters of the University of Zilina, 22(4), 28–34. https://doi.org/10.26552/com.c.2020.4.28-34

Ponzoa Casado J.M., Gómez Funes A., & García-Doncel J.G. (2021). *Digital Transformation: Advantages and opportunities of E-CMR in international cargo logistics.* ESIC Digital Economy and Innovation Journal, 1(1), 84–102. https://doi.org/10.55234/edeij-1-1-004

Rath, C., Roth, S., Schallar, M., & Zefferer, T. (2014). A Secure and Flexible Server-Based Mobile eID and e-Signature Solution. In *The Eighth International Conference on Digital Society* (pp. 7-12). ISSN: 1942-2636.

Ratia, S. (2022, April 27). *Digital Transformation: ECMR – a digital future for the CMR document*. Vrio. Retrieved September 29, 2022, from https://vrioeurope.com/en/digital-transformation-ecmr-a-digital-future-for-the-cmr-document/

Schindler P. (2019). *Business Research Methods*, Mcgraw-Hill, 13th ed. ISBN 13: 9781259918933

Shukla, P. (2008). *Essentials of Marketing Research*. Ventus Publishing ApS. ISBN: 9788776814113

signNow. (n.d.). *Electronic signature - Custom eSignature workflows | signNow*. Retrieved February 19, 2023, from https://www.signnow.com/

SignRequest. (n.d.). Retrieved February 20, 2023, from https://signrequest.com/#/

Software Advice. (n.d.). *Best Electronic Signature Software - 2023 Reviews & Pricing*. Retrieved March 3, 2023, from https://www.softwareadvice.com/electronic-signature/

Taherdoost, H., & Madanchian, M. (2023). Multi-Criteria Decision Making (MCDM) Methods and Concepts. *Encyclopedia*, *3*(1), 77–87. MDPI AG. Retrieved from http://dx.doi.org/10.3390/encyclopedia3010006

Transfollow - Uniting Supply Chains. (2022, September 26). *Ratification of the eCMR protocol in Europe - Transfollow*. Retrieved December 27, 2022, from https://www.transfollow.org/ratification-ecmr-protocol-eu/

TransFollow. (2021, June 29). *How can I submit feedback to TransFollow? - Transfollow*. Transfollow - Uniting Supply Chains. https://www.transfollow.org/support/drive/signing-methods-the-ecmr/

Tumel S. (2022). *Report: Using the UN/CEFACT Multimodal Transport Reference Data Model and Semantic Standards In Roll-Out Projects, Notably for Road Transport.* UN Development Account multiagency project "Trade and Transport Connectivity in the Age of Pandemic". Retrieved October 9, 2022, from https://unttc.org/sites/unttc/files/2022-03/Using%20the%20UNCEFACT%20MMT%20RDM%20and%20Semantic%20Standards%20In%20Roll-Out%20Projects%2C%20Notably%20for%20Road%20Transport.pdf

Wang, J., Jing, Y., Zhang, C., & Zhao, J. (2009). Review on multi-criteria decision analysis aid in sustainable energy decision-making. *Renewable & Sustainable Energy Reviews*, *13*(9), 2263–2278. https://doi.org/10.1016/j.rser.2009.06.021

Watts, S. & Raza, M. (2019, June 15). *SaaS vs PaaS vs IaaS: What's The Difference & How To Choose*. BMC Blogs. Retrieved January 3, 2023, from https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

Willems, D. (2021). *EU Reg EU Regulation on electronic freight transport information (eFTI) & DTLF Paperless Transport.* Rapporteur Paperless Transport (SG1), Digital Transport & Logistics Forum (DTLF). Retrieved October 15, 2022, from https://unece.org/sites/default/files/2021-10/T%2BL10%20-%20EU%20Project%20eFTI%20-%20update.pdf

7. Appendix

Appendix 1. Interview Questions

1. What is your opinion on the current situation with signing CMR documents?
2. Who will be the main users of the e-signature system?
3. What is the expected number of users?
4. Do Vervo employees also need to sign e-documents?
5. Apart from CMR, is the e-signature system intended for signing other documents?
6. What kind of user interface would you like to see for the e-signature system?
7. What security procedures do you want the e-signature system to provide? That is, what authentication methods should clients and partners use? eID, biometrics, bank accounts?
8. Do you want the e-signature program to be paid for with a monthly subscription or a one-time purchase?
9. What budget do you want to allocate to the e-signature system?
10. Besides integrating with Onfrex, is there any other program that should also connect to the e-signature system?
11. Do you want the user to be able to personalize CMRs, i.e., add specific logos or stamps?
12. Should the e-signature system be available only within Europe or outside of it as well?
13. How important is availability outside the European Union?
14. Should the e-signature system be available in multiple languages or only, for example, in English?
15. Would the signature system need to be available in offline mode?
16. In what form should this system be? That is, as an application or in a web browser?

Appendix 2. Authentication methods for eID Easy Docs

Method	Price	Coverage
MojeID login	€0.06	CZ
Freja eID login	€0.06	FI, SE, NO, DK
Itsme login	contact for pricing	BE
Estonian ID card login	€0.00	EE
Estonian Mobile ID	€0.12	EE
Smart-ID login	€0.12	EE, LV, LT
Portugese Cartão de Cidadão	€0.00	PT
Belgium ID card login	€0.00	PT
Finnish Henkilökortti	€0.00	FI
eParaksts Mobile login	€0.06	LV
eParaksts Smart Card	€0.00	LV
Austrian Handy-signatur login	€0.06	AT
Lithuanian ID Card	€0.00	LT
Lithuanian Mobile ID	€0.12	LT
Serbian ID Card	€0.00	RS
Swedish Bank ID	€0.12	SE
IDIN	€0.50	NL

Appendix 3. Qualified Electronic Signature Prices for eID Easy Docs

Method	Price
Austrian HandySignatur (QES)	1.50 EUR
Danish MitID signature (AdES light)	0.40 EUR
Smart ID mobile app signature (QES)	0.20 EUR
Estonian ID card signature (QES)	0.15 EUR
Estonian Mobile ID signature (QES)	0.20 EUR
Evrotrust [supported countries] (QES)	1.50 EUR
D-Trust's Sign-me [several countries] (QES)	1.50 EUR
D-Trust's Sign-me [several countries] (AdES full) *	0.50 EUR
Latvian ID card signature (QES)	0.15 EUR
Latvian eParaksts Mobile signature (QES)	0.15 EUR
Lithuanian ID card signature (QES)	0.15 EUR
Lithuanian Mobile ID signature (QES)	0.20 EUR
Finnish ID card signature (QES)	0.15 EUR
Finnish Trust Network signature (AdES light)	0.40 EUR
Finnish Trust Network signature (AdES full)	0.89 EUR
Swedish BankID signature (AdES light)	0.40 EUR
Swedish BankID certificate-based signature (AdES full) *	0.89 EUR
Swedish BankID certificate-based signature (QES) *	1.50 EUR
France's CertEurope USB tokens (QES)	0.15 EUR
Romania's certSIGN USB tokens (QES)	0.15 EUR
Czech MojeID (AdES light)	0.40 EUR
Norwegian BankID signature (AdES-QC)	1.50 EUR
Freja eID seal-based signature [Se, Fi, No, Dk] (AdES light)	0.40 EUR
Freja eID+ certificate-based signature [SE] (AdES full)	0.89 EUR
Freja eID+ certificate-based signature [SE] (QES)*	1.50 EUR
Belgian ID card signature (QES)	0.15 EUR
Portuguese ID card signature (QES) *	0.15 EUR
Portuguese Chave Movel (QES)	0.60 EUR
Dutch iDIN signature (AdES light)	1.00 EUR
Unataca (QES)	0.30 EUR
German Yes.com (through German banks) (QES)	4.50 EUR

Italian SPID signature (QES)	1.50 EUR
Benelux Itsme signature (QES) *	2.00 EUR
Halcom One (QES)	1.50 EUR
ZealiD [EU/EEC] (QES)	5.00 EUR **
Polish SimplySign signature (QES)	0.15 EUR
Ukrainian DIIA (non-eIDAS QES) *	0.15 EUR
Singaporean SingPass signature (AdES full) *	0.40 EUR
Document scanning based signature with Verifai (SES/AdES light)	1.50 EUR
Company e-Seal (QESeal)	0.15 EUR
Simple Electronic Signature (SES, SES 2FA)	0.15 EUR

Appendix 3. Signature methods for eID Easy Docs

Method	Price	Level	Supports visual signature	Supported container types	Coverage
Itsme	contact for activation and pricing	QES	Yes	pdf	BE
ZealID app	contact for activation and pricing	QES	Yes	pdf, asice, cades, xades	AT, BE, BG, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IT, LV, LT, NL, NO, PL, PT, RO, RS, SE, SI, SK
Estonian ID card	€0.15	QES	Yes	pdf, asice, cades, xades, pkcs1	EE
Estonian Mobile-ID	€0.20	QES	Yes	pdf, asice, cades, xades	EE
Lithuanian Mobile-ID	€0.20	QES	Yes	pdf, asice, cades, xades	LT
SPID	€1.50	QES	Yes	pdf	IT
Smart-ID	€0.20	QES	Yes	pdf, asice, cades, xades, pkcs1	EE, LV, LT
Belgian ID card	€0.15	QES	Yes	pdf, asice, cades, xades	BE
Lithuanian ID card	€0.15	QES	Yes	pdf, asice, cades, xades	LT
Latvian ID card	€0.15	QES	Yes	pdf, asice, cades, xades	LV
Finnish ID card	€0.15	QES	Yes	pdf, asice, cades, xades	FI, AX
Croatian ID Card	€0.15	QES	Yes	pdf, asice, cades, xades	HR

CertEurope USB token	€0.15	QES	Yes	pdf, asice, cades, xades	FR
certSIGN USB token	€0.15	QES	Yes	pdf, asice, cades, xades	RO
Austrian Handy-Signatur	€1.50	QES	Yes	pdf	AT
Latvian eParaksts Mobile	€0.15	QES	Yes	pdf, asice, cades, xades	LV
E-mail/ SMS	€0.15	SES	Yes	pdf	WORLD
Finnish Trust Network / Luottamusverkosto	€0.40	AdES	Yes	pdf, asice	FI, AX
Finnish Trust Network / Luottamusverkosto	€0.89	AdES	Yes	pdf	FI, AX
Evrotrust	€1.50	QES	Yes	pdf, asice, cades, xades	AL, AD, AM, AU, AT, AZ, BY, BE, BA, BG, CA, HR, CY, CZ, DK, EE, FI, FR, GE, DE, GR, HU, IS, IE, IT, IL, KZ, KE, XK, LV, LI, LT, LU, MT, MD, MC, ME, NL, NZ, NO, MK, PL, PT, RO, RU, SM, RS, SK, SI, ES, SE, CH, TW, TR, UA, GB, US, VA, AX
MojeId	€0.40	AdES	Yes	pdf, asice	CZ
Google	€0.50	SES	Yes	pdf, asice	WORLD
Swedish BankId	€0.40	AdES	Yes	pdf, asice	SE
D-Trust sign-me	€1.50	QES	Yes	pdf, cades	DE, CA, ZA, GR, NL, BE, FR, ES, PT, LU, IE, IS, MT, CY, AX, FI, US, BG, HU, LT, LV, EE, HR, SI, IT, RO, CH, CZ, SK, LI, AT, GG, DK, SE, NO, PL, MX, AR, BR, CL, AU, ID, PH, SG, RU, JP, KR, CN, TR, IN, SA, AE, QA

Chave Movel	€0.60	QES	Yes	pdf, asice	PT
Mit ID	€0.40	AdES	Yes	pdf, asice	DK, GL
Norwegian Bank ID	€1.50	AdES	Yes	pdf	NO
Freja eID	€0.40	AdES	Yes	pdf, asice	DK, EE, FI, LV, LT, NO, PL, RO, SK, SE, GL, AX
Audkenni	contact for activation and pricing	QES	Yes	pdf, asice, cades, xades	IS
SimplySign	€0.15	QES	Yes	pdf, asice, cades, xades	PL
Yes.com	€4.50	QES	No	pdf	DE
Uanataca	€0.30	QES	Yes	pdf, asice, cades, xades	ES
Halcom	€1.50	QES	No	pdf	SI
CertSIGN WebSign	€0.15	QES	No	pdf	RO
Swisscom	€1.70	QES	No	pdf	CH
IDIN	€1.00	SES	Yes	pdf, asice	NL
Verifai	€1.50	SES	Yes	pdf, asice	AF, AX, AL, DZ, AS, AD, AO, AI, AQ, AG, AR, AM, AW, AU, AT, AZ, BS, BH, BD, BB, BY, BE, BZ, BJ, BM, BT, BO, BA, BW, BV, BR, IO, BN, BG, BF, BI, CV, KH, CM, CA, KY, CF, TD, CL, CN, CX, CC, CO, KM, CG, CD, CK, CR, CI, HR, CU, CY, CZ, DK, DJ, DM, DO, EC, EG, ER, GQ, ER, EE, ET, FK, FO, FJ, FI, FR, GF, PF, TF, GA, GM, GE, GH, GI, GR, GL, GD, GP, GU, GT, GN, GW, GY, HT, HM, VA, HN, HK, HU, IS, IN, ID, IR, IQ, IE, IM, IL, IT, JM, JP, JE, JO, KZ, KE, KI, KW, KG, LA, LV, LB, LS, LR, LY, LI, LT, LU, MO, MK, MG, MW, MY, MV, ML, MT, MH, MQ, MR, MU, YT, MX, FM, MD, MC, MN, ME, MS, MA, MZ, MM, NA, NR, NP, NL, NC, NZ, NI, NE, NG, NU, NF,

					KP, MP, NO, OM, PK, PW, PS, PA, PG, PY, PE, PH, PN, PL, PT, PR, QA, RE, RO, RU, RW, BL, SH, KN, LC, MF, PM, VC, WS, SM, ST, SA, SN, RS, SC, SL, SG, SK, SI, SB, SO, GS, KR, SS, ES, LK, SD, SR, SJ, SZ, SE, CH, SY, TW, TJ, TZ, TH, TL, TG, TK, TO, TT, TN, TR, TM, TC, TV, UG, UA, AE, GB, UM, US, UY, UZ, VU, VE, VN, VG, VI, WF, EH, YE, ZM, ZW