Expertise
and insight
for the future

Tinja Puistosalo

Introduction of Digital Signing to Case Company

Metropolia University of Applied Sciences

Bachelor of Engineering

Industrial Management and Engineering

Bachelor's Thesis

31 December 2023

Author Title Number of Pages Date	Tinja Puistosalo Introduction of Digital Signing to Case Company 37 pages + 3 appendices 31 December 2023
Degree	Bachelor of Engineering
Degree Programme	Industrial Management and Engineering
Professional Major	Double Degree
Instructors	Harri Hiljanen, Senior Lecturer

The case company's existing signature process follows the traditional manual signing approach, where the client signs the contract first, followed by the supplier. This method necessitates both the client and the supplier to be physically present in the office, assuming that most companies do not provide printers and scanners for home offices. While this classic signing method may have been effective in a pre-Covid-19 world, the evolving work landscape calls for the implementation of new methods for daily tasks.

This thesis is a report aimed at implementing a digital signature process for agreement approvals between the case company and its clients. The thesis focuses on the utilization of a specific Digital Signature platform within the case company, and additionally introduces two major Digital Signature platforms as per the case company's request.

The objective of the thesis was to explore various solutions for digital signature processes and highlight the key distinctions among them. While the testing phase involved a case company, this thesis aims to provide a neutral perspective, serving as a manual or concise introduction to digital signing practices.

The research method for this case is statistical analysis, data is collected in statistically valid manners via experiments, surveys and observations. Four client representatives took part in the surveys and provided their opinion about digital signature.

Keywords	Electronic Signature, Digital Signature

Contents

Appendices

Appendix 1. Feedback reports. Only for use of the case company.

Appendix 2. Detailed process map of order handling process. Only for use of the case company.

Appendix 2. Submission form for Signing solution team. Only for use of the case company.

List of Abbreviations

SOW	Statement of work
PKI	Public Key Infrastructure
TSP	Trust service provider

1. Introduction

In today's increasingly digitalized and evolving world, the value of efficiency and streamlined processes are held in high regard. Companies strive to minimize time-consuming and unproductive tasks, continually seeking innovative solutions to reduce such burdens. One significant development from the past that is now gaining prominence in the world's digitalized landscape is the digital signature.

The thesis is based on the case company's need to implement digital signing platform to use with their clients. The case company was a part of a larger entity referred to as the "parent company" which, too, will remain anonymous throughout this thesis.

This thesis aimed at implementing a digital signature process for agreement approval between the case company and their clients. At the onset of the Covid-19 pandemic and subsequent lockdowns, the case company no longer required signed agreements from their clients. Instead, client offers were approved via email messages. However, as the Covid-19 lockdowns persisted, and remote work became the norm, it became necessary to explore alternative processes.

The case company also looked solutions outside of the parent company. The parent company employed Adobe Sign as their chosen platform, and according to the parent company guidelines, the case company was restricted from adopting an alternative solution without substantial justification.

1.1. Business Challenge

The existing signature process is a traditional manual signing procedure, with the client signing the contract before the supplier. This approach necessitates the physical presence of both the customer and the supplier in an office setting, given that most companies do not provide printers and scanners for home offices. While this classic signing method may have sufficed in a pre-Covid-19 world, the evolving work dynamics in the present require the adoption of new methods for daily tasks.

When the signing process relies on emails and scanning attachments, companies expose themselves to the risk of misunderstandings. In the absence of a final agreement bearing signatures, both clients and suppliers can encounter challenges where deliverables and outcomes fall short of expectations. For instance, when a supplier receives a simple email note from a client stating, "Ok, approved," it can create a situation where the supplier might be tempted to commence the project without an official Statement of Work.

When multiple individuals are involved in approving work agreements, there is a risk of misunderstanding the agreed-upon terms and conditions. If modifications to the terms and conditions occur during agreement negotiations and are not appended to the confirmation response, it introduces vulnerability to the project process. This oversight may lead to actions being taken that were not part of the agreement or result in overlooked elements of the agreed-upon terms.

An agreement conducted solely through email may lack the robust legal protection afforded by a formal contract. In the event of a dispute, substantiating the terms and obligations becomes challenging without a written contract. This difficulty in proving the original agreement extends to enforcing the terms of an informal email agreement, making it more arduous to demonstrate what was initially agreed upon in case of a disagreement.

1.2. Objective and Scope

The aim of this thesis is to propose an alternative to traditional handwritten signatures through the use of digital signatures in agreements. Legal requirements mandate the keeping and archiving of contracts, and at times, agreements may fail to meet quality standards without a proper signature or a record of the agreement. By implementing a signed digital document, all parties involved will have a clear and reliable record of what has been agreed upon, ensuring that everyone is on the same page regarding the terms of the agreement.

The scope of the thesis is to research different solutions for digital signature solutions and the main differences between them. While a specific case company has been utilized as a testing ground for one such solution, the overarching aim of this thesis is to

transcend company-specific contexts. It aspires to serve as an impartial and comprehensive resource, accessible as both a manual and a concise introduction to digital signing, tailored for a diverse audience.

The expected outcome of this thesis is an introduction about different ways of signing an agreement, which can help different organizations when digitalizing office routines. The thesis provides an overview of three major electronic signing platform providers, equipping readers with insights into various electronic signing practices. By offering this comprehensive view, the thesis aims to empower different organizations seeking to navigate the intricate landscape of digital signatures within their unique operational contexts.

1.2. Outline of thesis report

This thesis is organized into five main sections: existing knowledge, current state analysis, updated process, alternative solutions, and conclusion. Prior to the writing of the thesis, the case company found itself in the midst of a global pandemic. With no clear resolution in sight, a decision was made within the case company to explore a new solution for agreement approval. The thesis begins with a theoretical exploration of existing knowledge on the subject of digital signing.

The second section delves into the current state analysis, providing insights into how the process was managed during the pandemic. The updated process is then introduced, encompassing a testing phase. During this phase, testing was conducted jointly by the case company and the parent company.

In the fourth section, various alternative solutions are presented, addressing the case company's expressed preferences. The final section, the conclusion, encapsulates recommendations tailored to the case company's specific circumstances.

2. Method and Material

The research is carried out as an implementation project, given that the author was employed at the case company when the project was planned and implemented. This employment facilitated access to testing opportunities, especially during a crucial period when a change in the process was deemed essential.

Figure 1 outlines the research design, depicting the project's stages and the data utilized to achieve outcomes at each step. As shown in the Figure 1, the initial phase involved a current state analysis conducted prior to the writing process, serving as a foundational step. To ensure the project's direction was sound and to propose alternative solutions for supporting the integrated process's unstable usage, a literature review was undertaken.

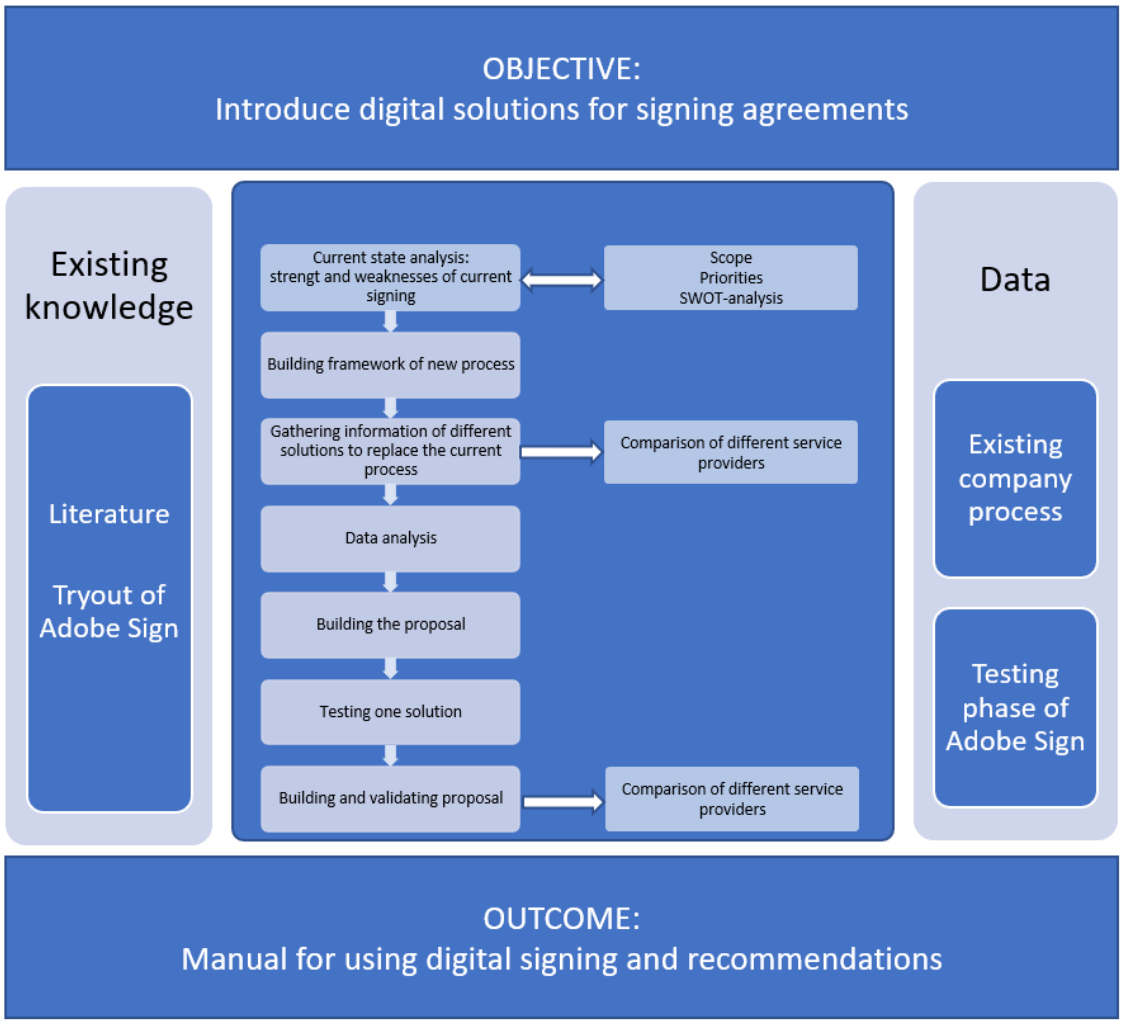

Figure 1. The Research Design

The results of the current state analysis provided a detailed account of the process at the inception of this thesis, including its strengths and weaknesses. This analysis generated insights into how the process could be optimally enhanced. Subsequently, the current state analysis was followed by a literature review focused on the identified development areas.

2.1. Data collecting

The research method for this case is statistical analysis, data is collected in statistically valid manners via experiments, surveys and observations. Data collection types, content and outcome are displayed on Table 1.

Table 1. Data Plan

Data Collection Type	Content	Outcome
Processing SOW with standard method	Current process	Current process steps
Processing SOW with temporary method	Current process, Future state	Current process steps, Strengths and weaknesses Improvement ideas
Introducing electronic signature solution to customers	Current process, Future state	Current process steps, Strengths and weaknesses Improvement ideas
Processing SOW with Adobe Sign	Current process, Future state	Current process steps, Strengths and weaknesses Improvement ideas
Feedback questions	Future state	Strengths and weaknesses Improvement ideas

The author has personally undertaken the task of observing data for the Current State Analysis, as this endeavor has been treated as an independent project. In addition to the author's observations, brief interviews were conducted to gather feedback from the customers of the case company, who constitute the other party involved in this analysis. The

data collection type column in the report outlines the specific phases during which experimental data was collected.

The primary objective of this initiative was to foster efficiency and continuity in operations. The initial process involving Statements of Work (SOWs) underwent a replacement necessitated by the shift to remote work forced by the Covid-19 pandemic. Although initially conceived as a temporary solution, this altered process has persisted for over a year. With an eye towards digitalization, the implementation of digital signatures is outstanding way to step forward with something that may not have been done without external force in the near future.

3. Digital Signing

There are two types of digital signing:

- Electronic signature
- Digital signature

According to the eIDAS Regulation, an electronic signature is defined as follows: *"'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;"* (eIDAS Article 3.10)

A digital signature refers to a mathematical and cryptographic scheme that is used to provide concrete and practical instances of electronic signatures. The definition given by ETSI TR 119 100 is that of *'data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.' (European Commission. 2022)*

Digital signatures are commonly utilized to implement electronic signatures, but it is crucial to note that not all electronic signatures qualify as digital signatures. In this thesis, the concept of digital signatures is expounded upon in this chapter. Generally, the term "digital signature" is used as a reference to a signature created digitally.

A digital signature serves as the electronic counterpart to a handwritten signature, offering assurance that the asserted signatory has endorsed the information or agreement. In electronic transactions, authenticating and verifying electronic data is paramount. The use of a digital signature allows for the verification of whether the information has undergone any alterations since it was signed. This attribute ensures the integrity of shared information, fostering trust and consistency among involved parties. An appropriately implemented digital signature algorithm adheres to the standards and regulations stipulated by each party and government (Gallagher, 2009).

A Digital Signature is generated through cryptographic methods, primarily aiming to establish the authenticity of the originator. The fundamental purpose is to enable the recipient of a message or document to authenticate the sender. A Digital Signature is unique

to a specific user, ensuring that a valid one can verify the origin of a message from that user. This characteristic allows for the verification of the initiator's authenticity at any point following the creation of digital material. Additionally, it is crucial that the initiator cannot later deny authorship of the document (Gallagher, 2009).

A digitally signed message or document cannot be altered without invalidating the signature. This principle holds true whether the message is encrypted or not. The presence of a valid digital signature upon receiving a message or document assures that no unauthorized alterations occurred during transit. Many platforms allow configuration specifying which data the signatory (in this case, the client) can modify. This mechanism is mutually applied to ensure that the initiator cannot modify or alter the data after the signature is added. (Gallagher, 2009.)

Ultimately, a digital signature serves as the electronic equivalent of a handwritten signature, signifying that a message or document has been acknowledged. When someone digitally signs a document, they are unable to later deny their association with it. This comprehensive mechanism ensures that both the document and the identity verification process remain secure, preventing any possibility of denial of responsibility and liability at a later stage. For the initiator, it safeguards against repudiation of their creation, and for the recipient, it ensures they cannot, in any way, modify the content created by the originator. (Pooja, 2018.)

3.1. Digital Signing in theory

With digital signatures, audit trail plays a central role in providing indisputable verification of both the originality and integrity of the document. Through this meticulous record, the initiator of the signature invitation gains the ability to scrutinize crucial details, including the IP addresses of the signatories and the timestamps associated with each signature. Essentially, the audit trail acts as an invaluable footprint, offering transparency and accountability throughout the signing process. (SecureKey, 2023)

A digital signature algorithm comprises two primary processes: signature generation and signature verification. The generation process is carried out by a signatory, while the verification process is conducted by a verifier to authenticate the signature's validity. Every signatory possesses a unique public and private key, serving as the owner of that

specific key pair. During the signatory's signature generation process, the private key is employed, as illustrated in Figure 2. (Gallagher, 2009, Pooja, 2018.)

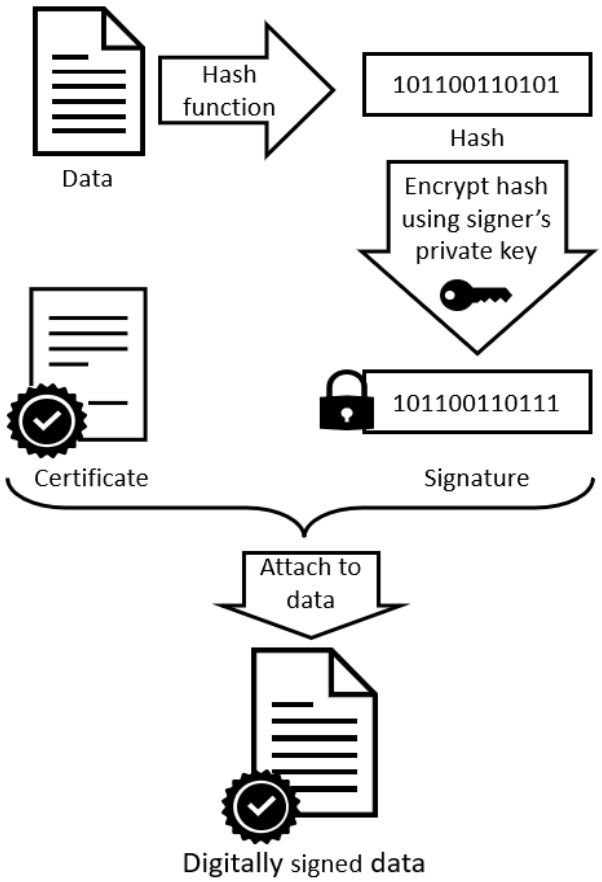

Figure 2. Generation process of a digitally signed data. (V Skills Certified, 2022.)

The exclusive entity authorized to utilize the private key for generating digital signatures is the owner of the key pair. To demonstrate the data's integrity, the public key is employed to decrypt the signature into a hash. The validation process involves comparing the hash derived from the data with the hash obtained from the signature. If these two hashes match, as illustrated in Figure 3, it confirms that the digitally signed data has remained unaltered and is deemed valid. (Gallagher, 2009.)

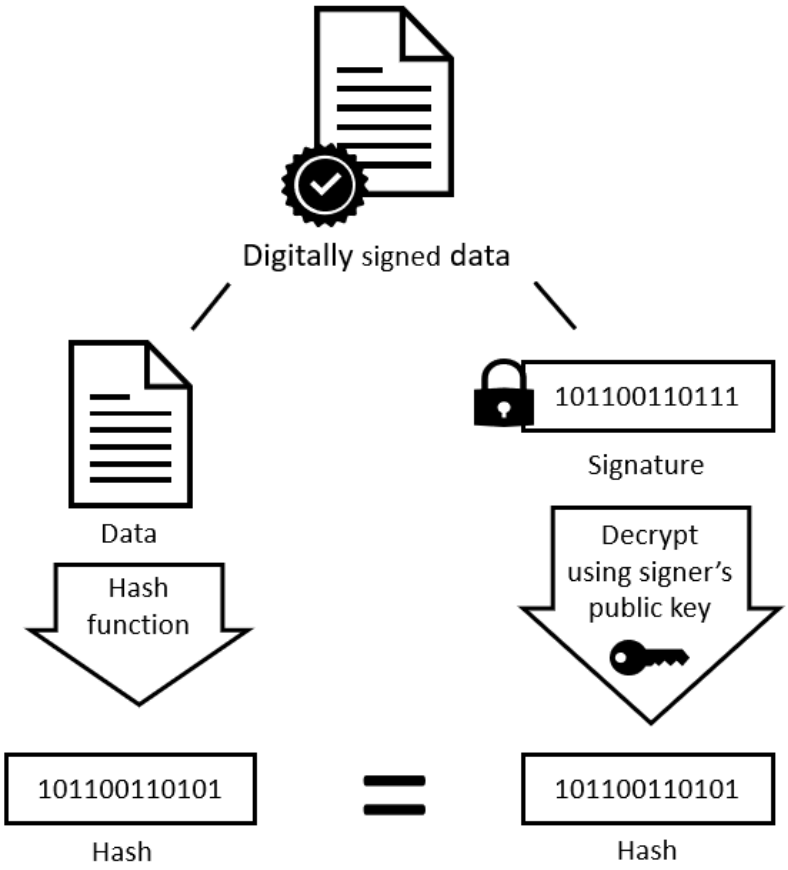

Figure 3. Verification process of digitally signed data. (V Skills Certified, 2022.)

The sanctioned digital signature algorithms are crafted to prevent adversaries lacking knowledge of the signatory's private key from producing an identical signature as the signatory on a different message. In essence, these algorithms are engineered to ensure that signatures cannot be forged. A number of alternative terms are used in this Standard to refer to the signatory or key pair owner. An entity that intends to generate digital signatures in the future may be referred to as the intended signatory. Before confirming the authenticity of a signed message, the individual signing it is denoted as the "claimed signatory" until a satisfactory level of assurance is established regarding their true identity. While the public key doesn't require confidentiality, it must be preserved in terms of integrity. The verification of a properly signed message can be performed by anyone using the public key. (Gallagher, 2009)

3.2. Regulations of Digital Signing

In order to verify a digital signature, the verifier shall obtain the public key of the claimed signatory. Using the appropriate digital signature algorithm, the domain parameters, the public key and the newly computed message digest, the received digital signature is verified in accordance with Digital signatory standard. If the verification process fails, no inference can be made as to whether the data is correct, only that in using the specified public key and the specified signature format, the digital signature cannot be verified for that data. If the verification and assurance processes are successful, the digital signature and signed data shall be considered valid. However, if a verification or assurance process fails, the digital signature should be considered invalid. An organization's policy shall govern the action to be taken for an invalid digital signature. (Gallagher, 2009)

Electronic signature is a legal concept that is defined in the eIDAS regulation. The different levels of electronic signatures are defined in the eIDAS Regulation (EU) No 910/2014. These three levels are shown in the table 2.

Table 2. Three levels of electronic signatures

Electronic signature	Advanced electronic signature	Qualified electronic signature
Used by the signatory for signing	Identity of the signatory	Same features as advanced electronic signatore
Authenticity can not be proved	Modified or forgot information can be detected	Regulated, supervised and assessed
Name at the end of an email	Created with a mobile certificate of online banking codes	eIDAS QSCD

The digital signature utilized by the Digital and Population Data Services Agency is a form of digital information employed by the signatory for the purpose of signing. This type of signature represents the lowest level of digital signature, often known as a simple electronic signature. In its simplest form, it might be akin to the inclusion of a name at the end of an email. However, it is important to note that the lowest level digital signature lacks the ability to be definitively linked to a specific individual and cannot serve as a means of authentication. (DVV, 2022). The lowest level of digital signature has been used by the case company since Covid19 started, which is described with more detail in the chapter 4.2. Current approval process due to exceptional times.

The advanced electronic signature represents the second level of digital signatures. At this level, the signature is intricately connected to the signatory, allowing for unique identification, and the data's authenticity can be verified. The advanced electronic signature employs a private key in its creation, ensuring the security of the document's data, and any alterations can be detected during the verification process, as it is represented in Figure 3. The case company aims to achieve this level with its revised approval process. The creation of an advanced electronic signature is possible through various means, such as a mobile certificate or online banking codes. It's essential to note that an advanced electronic signature can be regarded as a form of digital signature. (DVV, 2022). AdobeSign will meet the level of advanced electronic signature, as it is mentioned in chapter 7. Different solutions for digital signing. As the advanced electronic signature has the same features as qualified electronic signature, as it is stated in the Three levels of electronic signatures table, this will meet the quality level for the case company. The advanced electronic signature meets the eIDAS regulations at the minimum level without the qualified electronic signature creation device (QSCD).

A qualified electronic signature refers to an advanced electronic signature generated using an eIDAS qualified certificate and a creation device, such as a card chip, recognized as an eIDAS qualified electronic signature creation device (QSCD). This type of signature validates both the document's data content and the signatory's identity, akin to the advanced electronic signature previously mentioned. Notably, the devices employed for electronic signature creation undergo more rigorous regulation, supervision, and assessment. (DVV, 2022). The case company would have been able to reach this level, as this is stated enable by Adobe Sign Solutions, as it will be mentioned in later chapters. Although this level of signature is the most accurate, it is considered unsuitable for the case company's needs.

A qualified electronic signature holds legal validity and is unquestionable throughout the entire European Union. According to the eIDAS Regulation, the legal implications of a qualified electronic signature are required to be equivalent to those of a handwritten signature. The devices responsible for generating qualified electronic signatures, referred to as Qualified Electronic Signature Creation Devices (QSCD), boast robust security measures to guard against external threats. (DVV, 2022). This level of electronic signature is used for example in the medical field, and therefore can be seen as an extra secure solution for the case company purposes.

The primary aim of electronic trust services is to guarantee the secure utilization of electronic services. The regulations governing electronic trust services are outlined in the European Union's eIDAS Regulation. The eIDAS Regulation oversees the following trust services:

- certificates, validation and preservation of electronic signatures
- certificates, validation or preservation of electronic seals
- electronic time stamps
- electronic registered delivery services
- certificates for website authentication.

All the later introduced platforms for digital signatures does meet eIDAS regulation. For the case company meeting the eIDAS regulation is crucial, as the business is working in European Union region.

4. Current State Analysis

Before the Covid-19, normal approval process for the case company was to sign every offer document manually. Same process will apply to several other companies. This process is presented in Figure 5, and it can be said that this normal approval chain contains ten steps in total from the client point of view.

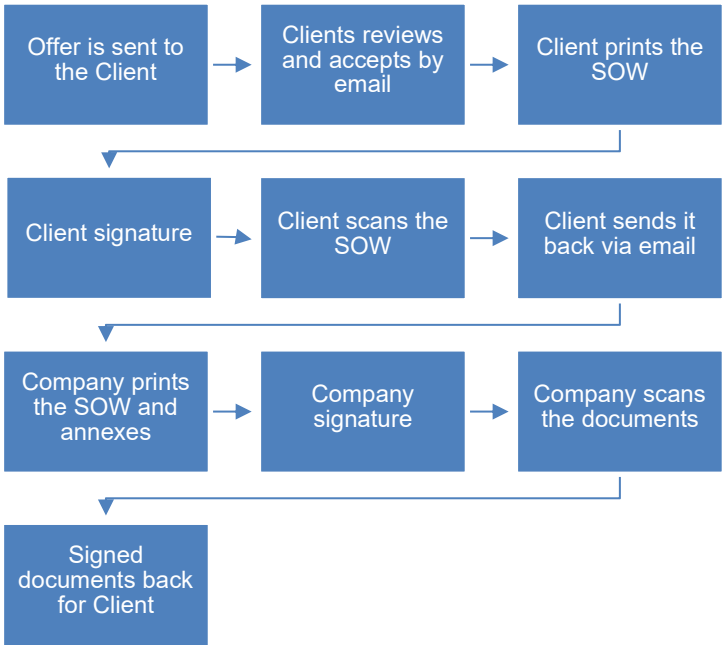

Figure 5. The process to get signed SOW in normal conditions.

The offer is made by the responsible manager, who also sends the offer to the clients. Before the documents are sent to the clients, the signing process took time from three case company representatives. This step can only be done in the office, which requires active and physical presence. In the normal state, offer documents will have two signatures from two responsible managers. Due to busy meeting schedules of the managers, sending the offers to the clients could be delayed one to two days, if the managers were not having any breaks in their days. Third representative was responsible for getting the signatures from the managers.

After the offer is done and sent to the clients, they have been given usually two weeks' time to evaluate and review the offer. In some cases if there is no harmony between the parties, the expiration date can be pushed forward. At this point, if the clients approve the offer and are willing to start it, give notice by email. After this, they should send the

signed contract as an approvement, but it can also take a couple of weeks or so to really get the signed contract. Client may have different ways to internally approve the offers, which can affect their schedules to approve the contract. It has been stated that the work should not start before the actually signed contract but many times the contract may come after the actual start of the Project.

When the client is ready from their part of the signing process, it is the case company's turn to take the same process at their end. When the contract is signed by both parties, a so called Contract package is made by printing all of the documents including annexes related to the offer and all of those documents are scanned again to make an all-including pdf-file. These files will be archived physically and to cloud services.

4.1. Strengths and weaknesses

A hand written signature is known process and can be included as a main strength as listed in Figure 7. SWOT analysis of current state. When the process and protocols are known by everyone involved, mistakes and misunderstandings are less likely to happen. A Hand written signature is also widely recognized as legally binding, providing a robust foundation for the enforceability of agreements. Physically signed agreements offer tangible, clear documentation that is easy to archive and reference.

When the contract and attachments are sent to the client, it is not said that the recipient of the offer email will be the one who is responsible for signing the contract. This can be time-consuming, involving the printing, signing, and scanning of documents, potentially causing delays. In the clients organizations there may be also multiple managers who each have their own responsibility areas and these responsibility areas are not necessarily shared too wide outside of their organizations. This means geographical constraints, as signatories must be physically present or engage in shipping documents, introducing challenges for remote or international approvals. When people are mostly physically in the offices, it can be said that business trips will affect the responsiveness and will slow down the process. The process may contribute to paper waste and environmental concerns, aligning less with sustainable practices. Organizations are also taking a leap to paperless offices as it can lead to cost reductions. Businesses can save money on paper, ink, printing equipment, storage space, and the associated administrative tasks involved in managing physical documents. Efficiency and productivity can be

listed with environmental impact. Digital documents can be accessed, shared, and processed much more efficiently than their physical counterparts. This streamlines workflows, reduces delays, and enhances overall productivity. Going paperless aligns with sustainability goals, as it reduces the need for paper production and lowers the environmental impact associated with printing, transportation, and disposal of paper waste.

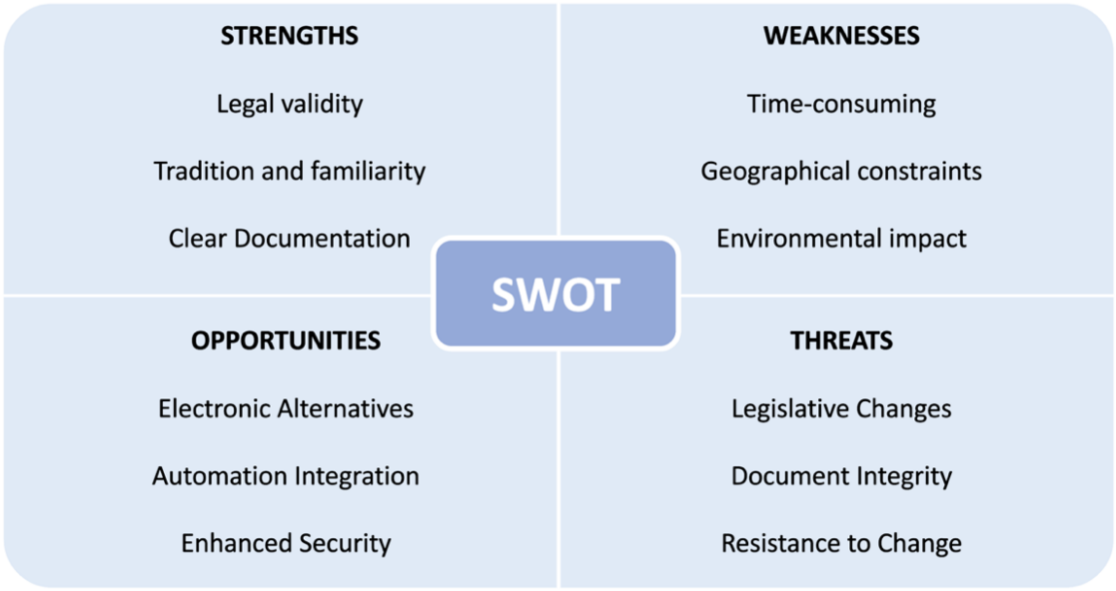

Figure 6. SWOT analysis of current state.

One of the opportunities, also mentioned in Figure 6. SWOT analysis of current state, is that there is electronic alternatives, which are covered in this thesis. Exploring electronic signature solutions can streamline the process, reducing time and environmental impact. Digital documents can be accessed from anywhere with an internet connection, facilitating remote work and collaboration among team members who are working remotely. Integrating automated systems can enhance tracking, reminders, and document management, improving overall efficiency. Automated reminders secure the schedule of the project, as the projects can be started as scheduled if the agreements are processed in the given timeframe.

Digital documents can be easily searched, archived, and retrieved, saving time that would be spent manually searching through physical files. Although the physical archive could be needed in some cases, it is easier to search the signed document from a digital archive. One key benefit is the security of storing in multiple locations. This not only

mitigates the risk of data loss resulting from disasters like fire or flooding but also ensures the availability of critical information when needed.

Moreover, digital document management systems come equipped with features designed to facilitate compliance with regulatory requirements. These features include robust audit trails, version control mechanisms, and advanced security measures. The integration of these functionalities empowers organizations to maintain a meticulous record of document activities, revisions, and access, aligning seamlessly with regulatory standards. As technology continues to advance, the feasibility and efficiency of transitioning to paperless operations become increasingly apparent. These technological advancements not only streamline workflows but also contribute to the overall sustainability and resilience of modern businesses.

While the adoption of digital document management brings numerous advantages, challenges and considerations must be addressed to ensure the integrity and effectiveness of the process. One notable challenge that can happen is instances where clients sign contracts, but the documents fail to reach the organization. This poses a significant threat, particularly during audits or compliance checks. In the absence of the signed contracts, there is no clear reference point, leaving the company vulnerable to disputes and uncertainties.

Evolving regulations on electronic signatures and increasing digitalization may impact the acceptance and validity of manually signed agreements. The lack of a documented path for agreements raises concerns about the potential addition or deletion of clauses in the statement of work. Risks of document tampering or loss exist during the physical transportation of printed agreements can be seen as a threat. Disagreements between parties may arise due to the absence of a trail, impacting the overall credibility and trust in the agreement process. Addressing these challenges requires a combination of technological enhancements, secure delivery methods, regular audits, and legal consultation to ensure a seamless transition to paperless operations while maintaining the integrity of crucial agreements.

4.2. Current approval process due exceptional times

With the global impact of Covid-19 necessitating widespread remote work due to lockdowns, the case company implemented a temporary solution to sustain agreement-related operations. The customary practice of sending offers to clients via email persisted, and if accepted, clients would respond through email. Notably, in a majority of cases, client responses were succinct, often comprising a simple "ok," signaling the acceptance of the offer and providing the green light to commence work. This streamlined approach became a pragmatic workaround during the challenging circumstances imposed by the pandemic.

Recognizing the initial implementation as a temporary solution, the prolonged nature of lockdowns prompted the need for a more sustainable method to sign agreements. Despite the apparent strengths of this approach, as depicted in Figure 7, the increasing visibility of its weaknesses and potential threats necessitated a reevaluation of the process. The case company acknowledged the need for a more robust and enduring solution to address the evolving challenges and uncertainties posed by the ongoing lockdown conditions.

The primary distinction in the usual approval process arises from shifts in working habits, particularly the widespread adoption of remote and home-based working hours. Given that many companies typically do not provide printers and scanners for home use, the traditional method of manual signing becomes nearly impractical for individuals working

outside the office environment. The challenges posed by this change in working dynamics necessitate a reevaluation and adaptation of the approval processes, prompting a closer look at digital alternatives like electronic signatures.

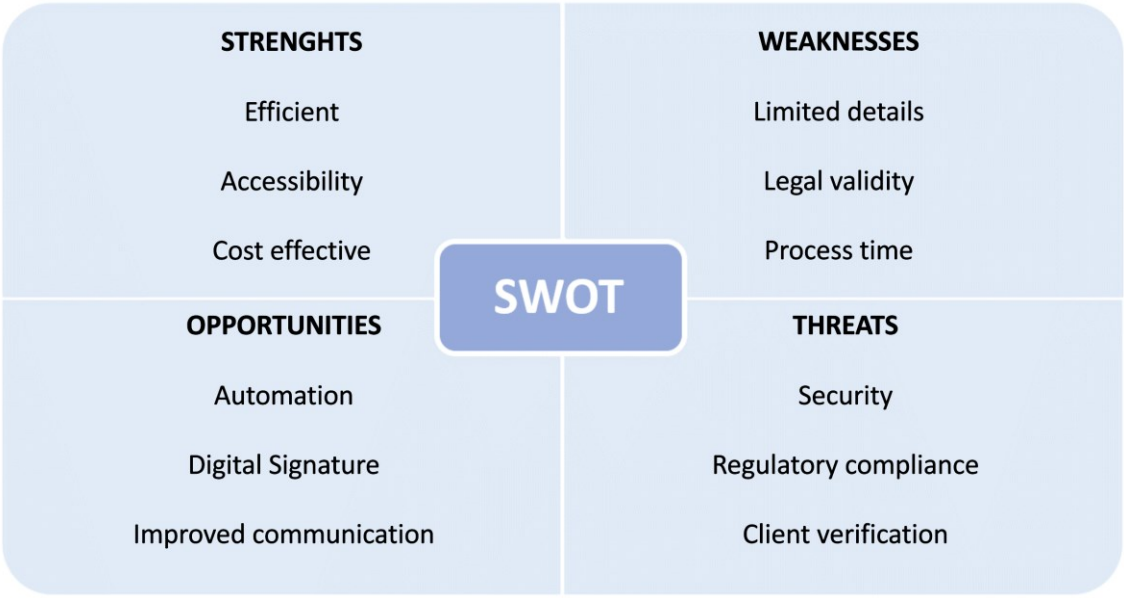

Figure 7. SWOT analysis of approval process due to exceptional times

The positive outcome of working from home is the standard email using and following, because all the work is now happening through the computers. When the employees are constantly available to approve the contract that has been send via email, approvements can be done in a quick schedule. This process requires minimal effort and time from the client. When the email is enough to approve the contract, it can be said that the approving is happening a lot faster than before, when the contract was approved after the signing. The electronic nature of the process reduces the need for physical documentation, lowering associated costs.

The weaknesses of the email signings is the missing documents. The case company's clients do not have to forward the attachments they have approved, and this risk may lead to misunderstandings. Possible risks in these situations are for example modified agreement if it has not followed with approval, and something has not been done due to this misunderstanding. Also there is a risk that the original offer email has been mistyped and does not match the contract number, and due to the approvement and agreement will be connected wrongly. Depending on jurisdiction, an informal "Ok" may lack the legal validity of a formal signature, raising concerns about enforceability.

Integration with automated systems can enhance tracking and documentation, reducing manual intervention. Implementing a more formal digital signature process can enhance legal validity and security. Email can be seen to encourage clients to provide additional comments or questions, fostering clearer communication and reducing potential misunderstandings, but as also mentioned in weaknesses, therefore this can be seen a little bit controversial issue.

Confirming the identity of the client responding with an "Ok" may present challenges, giving rise to concerns regarding unauthorized approvals. There is a potential scenario where an individual from the client's site could respond to the email, indicating approval before the authorized signatory with signature rights has reviewed the offer. This poses a risk to the authenticity of the approval process.

Email-based approvals are vulnerable to security threats, underlining the importance of implementing robust encryption and authentication measures. Without proper safeguards, unauthorized access and responses could compromise the integrity of the approval system. Moreover, the landscape of regulations governing electronic signatures and approvals is evolving. Changes in these regulations may influence the validity and acceptance of informal responses like the "Ok" reply. Organizations relying on such methods should stay abreast of these regulatory shifts to ensure ongoing compliance and the legal standing of their approval processes.

To see the clients' opinion for implementing the new process to sign the agreements, the following questions were asked in the client interview:

- How comfortable are you with the idea of signing contracts digitally?
- Have you signed any contracts digitally in the past? If yes, how was your experience?
- What authentication methods do you find most secure and convenient for digital signing?
- Are you open to using third-party authentication methods, such as banking codes or mobile ID for added security?
- What concerns, if any, do you have about signing contracts digitally?
- Are there any specific aspects of digital signing that make you hesitant or uncertain?
- How important is the accessibility of digital signing platforms to you?

- What features do you consider essential for digital signing platform to be convenient for you?
- Would you be interested in training or informational sessions on how to use a digital signing platform?
- What challenges do you foresee in transitioning from manual signing to digital signing?

Four representatives from the clients side participated in a survey regarding the adoption of the digital signing process. All of these clients have previously utilized digital signing platforms. According to their collective experience, they encountered little to no issues, and any challenges were minor enough not to warrant significant attention.

Despite the unanimous agreement among clients that digital signatures with bank authentication are the most secure, only two customers expressed willingness to use their personal banking details for authentication in work-related scenarios. Notably, clients did not harbor any active concerns regarding the digital signing of contracts. There was a shared enthusiasm among them to embrace digital signing, particularly because the Covid-19 pandemic necessitated remote work for everyone. Given the remote work scenario, all clients emphasized the importance of having access to signing capabilities beyond the corporate network.

5. Updated approval process

The goal of updating the contract approval process is to enhance its efficiency and simplicity. In an ideal scenario, the process would involve only a few steps and be completed within a matter of minutes. As illustrated in Figure 8, the updated process requires significantly fewer steps compared to the manual approval method, aligning with the goal of streamlining and expediting the overall contract approval procedure. The envisioned outcome is a more agile and responsive system that optimizes time and resource.

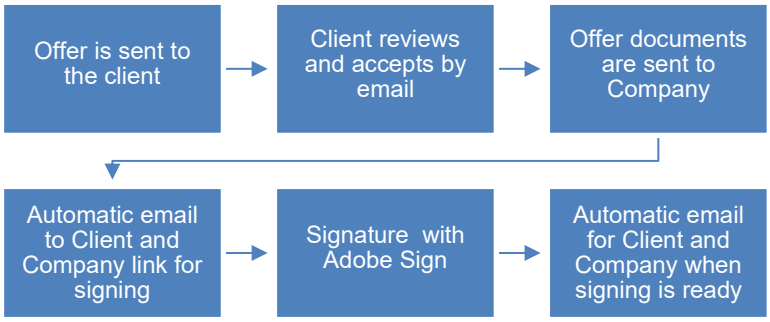

Figure 8. The Signing Process after the update. All the manual printing and scanning can be set aside.

The contract will continue to be presented through email, preserving the familiar method, albeit with a digital signature feature. The offer itself will stipulate the duration within which the client can assess and provide their acceptance. Typically, this timeframe spans around 14 days, though variations may occur, ranging from the following day to over a month. Prior to the conclusion of the offer period, clients have the opportunity to designate the individual responsible for signing the Statement of Work (SOW) if they have given their approval to the offer.

While some clients may consistently assign the same contacts for every contract, there is also the potential for variations. Different contacts may be designated to sign contracts, each with a specific or diverse focus area, such as distinct solution domains, ensuring flexibility and adaptability to the unique requirements of each agreement.

5.1. Strengths and weaknesses of new process

The SWOT analysis of the new process, where the agreements are signed digitally. The analysis delves into the multifaceted aspects of this technology, exploring its impact on

security, efficiency, legal standing, and the broader implications for organizational workflows.

One of the primary strengths of employing digital signatures for agreement confirmation lies in the heightened security and authentication they offer. This method not only ensures the integrity of the agreement but also provides a level of authenticity that is often challenging to achieve with traditional, paper-based signatures. The efficiency gains derived from digital signatures present another notable strength, streamlining the confirmation process and reducing the time traditionally associated with physical signatures. Additionally, the legal recognition of digital signatures in many jurisdictions strengthens their position as a reliable and enforceable means of confirming agreements. Digital signing allows parties to sign documents from anywhere with an internet connection, facilitating remote work and global collaboration, which could be considered as a huge advantage compared to traditional manual signature.

Despite the advantages, digital signatures are not immune to challenges, as it is presented in Figure 9. Some individuals may encounter technological barriers, hindering the seamless adoption of this method. Moreover, there may be initial implementation costs associated with acquiring and implementing the necessary technology and conducting requisite training. Understanding and addressing these weaknesses is crucial for the successful incorporation of digital signatures into the agreement confirmation process.

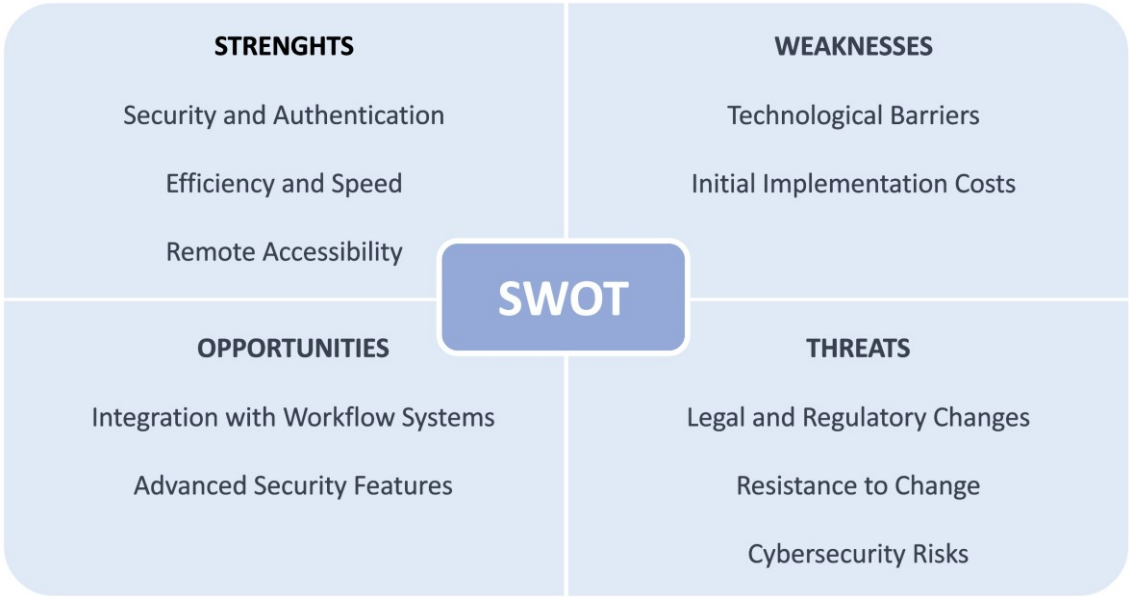

Figure 9. SWOT analysis of updated process

The integration of digital signatures into existing workflow systems presents a significant opportunity to enhance the overall business process automation. Continuous advancements in digital signature technology open avenues for the adoption of enhanced security features, further fortifying agreements against potential threats. The opportunities extend beyond mere confirmation, potentially influencing broader organizational efficiency and technological advancement.

While digital signatures offer a secure and efficient solution, they are not without threats. The dynamic nature of legal and regulatory landscapes poses a threat to the acceptance and validity of digital signatures. Ongoing compliance monitoring is essential to mitigate risks associated with potential legal changes. Resistance to change from stakeholders accustomed to traditional methods and the inherent cybersecurity risks associated with digital platforms also present significant threats that warrant careful consideration.

In the use of digital signing, where direct contact with other parties can be minimized, effective communication becomes more crucial. As mentioned in the earlier chapters, different managers may have different responsibility areas, underscoring the importance of communication, particularly when contracts are send to the clients. This ensures that the documents are directed to the appropriate individuals from the organization. In these cases, miscommunication can have consequential outcomes. Sending contracts to the wrong person might result in the signing request getting lost amidst a barrage of emails. Some clients may be on the alert of opening unfamiliar links, especially if they are not anticipating signing requests. This presents a risk of the contract being overlooked or not reaching the intended signatory.

The internal transmission of information within companies is equally critical. Failure to relay essential details internally may lead to scenarios where contracts remain unapproved, lacking a structured follow-up process. Therefore, establishing clear communication channels, both externally with clients and internally within the organization, is imperative to ensure the seamless progress of the digital signing process and mitigate potential risks associated with misdirected or overlooked contracts.

6. Testing of Updated process with Adobe Sign

Within the operational infrastructure of the case company, digital signing requests are channeled through their proprietary service, referred as Signing solution. This dedicated platform seamlessly integrates with Adobe Sign, serving as the conduit for the actual signing process. To maintain confidentiality and security, the submitted contracts are discreetly labeled as letters X, Y, Z, and Q, guarding against the disclosure of sensitive information.

Upon client approval via email and completion of the submission form, the contract documents are forwarded to the Signing solution team. This team is responsible for uploading the documents to Adobe Sign and initiating the signing requests, which are then distributed to both the client and the case company management. Ideally, this entire process is expected to transpire within a few days.

However, a closer examination of the submissions reveals that the process encounters some challenges that impact its smooth progression. The time span for contracts to be uploaded varies, ranging from one to six days. Uncovering inconsistencies in outcomes despite identical selections in each submission raises concerns and prompts a closer examination of the underlying issues within the digital signing workflow.

6.1. Contract X

While many contract submissions unfolded seamlessly, filled with the requisite information and returned with the necessary signatures, a few anomalies surfaced. These irregularities, seemingly stemming from minor time disparities between the program and real-time events, introduced variations into an otherwise efficient process.

In one instance, an automated notification flagged that a contract still lacked the client's signature. Surprisingly, upon inquiry, the client confirmed that they had signed the document a few hours prior. This discrepancy prompted the Signing solution team to investigate potential technical glitches related to signatures. After a thorough examination, the client's signature eventually registered in the system a few hours later, allowing the con-

tract to proceed to the approval stage within the case company. This incident underscores the importance of promptly addressing and resolving technical issues to ensure the fluidity of the digital signing workflow.

6.2. Contract Y

The processing of Contract Y through the Signing solution service encountered a significant setback. After eight working days, the contract was unexpectedly returned to the sender. The Signing solution team cited the reason that the case company was not recognized.

Despite efforts to clarify the situation with Signing solution, the issue persisted and could not be rectified. Consequently, Contract Y was unable to undergo processing through the service. In response to this hurdle, the contract was archived, accompanied by an email message from the client explicitly expressing the intention to proceed with the work despite the processing challenges encountered. This instance underscores the importance of adaptability and contingency planning to navigate unforeseen obstacles in the digital signing process.

6.3. Contract Z

The submission of Contract Z through the Signing solution service encountered a noteworthy discrepancy. Following the standard procedure, the client received a notification indicating that there was a contract requiring their signature. The client promptly acknowledged signing it as per the agreed terms.

However, automated reminders were triggered, indicating that the client had not signed the agreement. Upon reaching out to the client, they asserted that they had indeed signed the contract through the program. Contrary to the client's confirmation, the signatures failed to register.

This unexpected hiccup highlights the importance of real-time synchronization and communication between different platforms within the digital signing process. Addressing

such anomalies promptly is crucial to ensure the accuracy and reliability of the digital signing workflow.

6.4. Contract Q

Contract Q served as an embodiment of various weaknesses inherent in digital signing processes. The initiation of the contract documents took place at the beginning of the month and was submitted to the Signing solution service. The ensuing timeline revealed a series of challenges:

- Acknowledgment Delays: Seven working days transpired before the Signing solution team confirmed receipt of the submission, leading to an initial delay in the process.
- False Notification: After an additional seven days, the Signing solution team notified that the document had not been signed, despite the client's assertion of completing the signing process.
- Client Confirmation: Seeking clarification, the client confirmed having signed the document, introducing confusion regarding the status of the signing process.
- Delayed Update: A day after client confirmation, Signing solution belatedly updated to reflect that the client had indeed signed the document.
- Unnecessary Follow-up: Subsequently, the system automatically prompted another individual from the same client to sign the document, even though the initial signing had been confirmed.

This intricate case emphasized the need for enhanced communication and streamlined notification processes within digital signing platforms to minimize confusion and ensure a more efficient workflow for all parties involved.

6.5. Feedback, setbacks and problems

After the digital signing process was implemented, feedback from the clients was gathered with another survey. The survey had the following questions:

- How would you describe your overall experience with digitally signing contracts?

- On a scale of 1 to 10, how user-friendly do you find the digital signing process?
- In comparison to the traditional manual signing process, how would you rate the efficiency of digital signing process?
- Have you noticed a difference in the time it takes to complete the signing process digitally?
- Do you find the digital signing platform accessible and convenient for your needs?
- How do you feel about the notifications and reminders sent during the digital signing process?
- Have you needed to seek technical support while using the digital signing platform?
- Are there any features or aspects of digital signing process that you think could be improved?

The overall experience with digital signing was positive for all clients, despite encountering a few issues. The clients expressed enthusiasm for the process and expressed a desire to use it for various types of agreements. The average score for user-friendliness was a robust 8 in the scale 1 to 10. While the signing speed was not perceived as exceptionally fast by the clients, the digital signing process was deemed efficient enough. Notifications were effective in reaching the clients, and the platform was easily accessible via computer. Interestingly, none of the clients attempted to use digital signing via mobile devices.

The implementation of the Digital Signing Process was met with a mix of acceptance and skepticism from clients. One prevalent concern among clients was whether they needed to use their own banking IDs for signing agreements. This apprehension was effectively addressed with Adobe Sign, which facilitated the pointing of agreements to the correct signatory through email links, eliminating the need for banking IDs.

One client inquired whether they could initiate the signing process through their own client-facing system, allowing them to send the signing request rather than a representative from the case company. However, the case company firmly rejected this option, emphasizing the necessity of using the system employed by the parent company. Adopting different signing methods with various clients would have introduced complications and undermined uniformity in the signing process.
Similarly, within the case company, the primary concern mirrored that of clients — ensuring the safety of agreements and appendices when accessed through email links.

7. Different solutions for digital signing

There are multiple suppliers for digital signing. Selecting a digital signing platform involves careful consideration of various factors to ensure that it meets the specific needs and requirements of the organization.

Table 3. Overview of the three solutions that are introduced in this Thesis, pricing from year 2022.

	Adobe Sign	Visma Sign	DocuSign
Price	US$14.99/mo/license Annual commitment	25-55EUR/mo Annual commitment	US$40/mo/license Annual commitment
User qty	License / user	Unlimited	Max. 5 license
Signature qty	Unlimited	240-600pcs/year	Unlimited
Level of Electronic Signature	e-signature, digital signature or combination	Strong or light authentication	Multiple levels
Authentication method	Email or/and password authentication	Banking ID or light authentication with visible trail	Email or/and password authentication
Meets eIDAS regulation	Yes	Yes	Yes

The most important thing to consider regarding digital signing providers, is that the platform adheres to industry-standard security measures. It needs to be verified, if the platform complies with relevant regulations and standards, eIDAS in Europe which is briefly introduced in chapter Regulations of Digital Signing. The systems that are introduced in the following chapters, all meet eIDAS regulation, as mentioned also in the table 3.

As there are different authentication options offered, the selected authentication option needs to meet internal and external requirements, such as multi-factor authentication, to enhance the security of the signing process. The selected platform needs to provide a reliable method to verify the identity of signatories. The platform's capability to generate comprehensive audit trails, documenting the entire signing process, as explained in the chapter Digital Signing in Theory. Assess the platform's record-keeping features, including document storage and retrieval.

It is also good to consider the scalability of the platform to accommodate the organization's growing needs. This means if there can be users added to the platform, or if there are any limitations to how many documents could be signed through a certain price break. New systems also have costs to the companies when implemented and maintained. It is important for the companies' that wants to implement digital signing solution understand the pricing model of the signing platform. Different charging types can be based by any subscription fees, transaction-based charges, combination of these two and other additional costs could be implemented.

7.1. Adobe Sign

Adobe Sign is the program that has been adopted by the case company, but other signature platforms were also discussed before implementing it.

Adobe claims that their approach to digital signatures offers greater flexibility compared to other signature solutions. With Acrobat Sign Solutions, a comprehensive signing processes can be established, incorporating digital signatures, e-signatures, or a blend of both. This flexibility enables the creation of workflows tailored to the company's specific compliance or risk profile. Adobe is compatible with a wide range of secure signature creation devices, including USB tokens, smart cards, and cloud-based digital certificates.

Users have the freedom to collaborate with their preferred certificate authority or timestamp authority, with support for numerous trusted authorities through the European Union Trusted List (EUTL) and the Adobe Approved Trust List (AATL). The Signing solution service department in the case company utilized Adobe Sign as the platform for digital signatures, employing the e-signature method. (Adobe, 2022.)

Acrobat Sign Solutions enables organizations in the European Union to implement signature processes that adhere to the requirements of both Advanced Electronic Signatures (AdES) and Qualified Electronic Signatures (QES) as outlined in the electronic identification and trust services (eIDAS) regulation. (Adobe, 2022.)

7.2. Visma Sign

In the realm of digital signatures, Visma Sign stands out by offering heightened security features, particularly with its emphasis on the creation of a comprehensive audit trail. As highlighted by Visma, the utilization of a digital signature in Visma Sign is considered more secure compared to traditional signatures, primarily due to the incorporation of this digital trace, known as an audit trail.

In Visma Sign the signatures are compounded to the document and each page is stamped with the information of the audit trail as well as the unique document verification code. This code enables verification of the document afterwards. (Visma, 2022.)

With Visma Sign, the collector, the case company, is the one who determines whether the document requires a strong or light authentication. Strong authentication uses a third party, such as banking codes or mobile ID, to confirm the identity. In a sign document, the names, timestamps and information on which country's authentication method were used in the signature event are visible. While Visma Sign advocates for the use of strong authentication, it particularly emphasizes its significance in scenarios where the signer is not personally known or when the signature involves a financial commitment. (Visma, 2022.)

In certain contexts, like internal processes within the case company, the stringent requirements of strong authentication may not be imperative. This is where the light authentication process comes into play, allowing the signer to digitally draw their signature

in the designated field. Light authentication proves advantageous, especially when signatories are situated outside the Nordic region, where the use of Nordic mobile IDs or banking codes may not be feasible (Visma, 2022.)

Even with lightly authenticated signatures, Visma Sign ensures verifiability post-signing. The signed document displays not only the digital signature but also provides visibility into the printed name, email address, and IP address of the signatory, offering a comprehensive overview for subsequent validation. (Visma, 2022)

7.3. DocuSign

DocuSign is also one that was mentioned by the case company, when digital signatures were mentioned first time. According to DocuSign's statistics, 82% of agreements are successfully completed in less than a day, with almost a half of processes taking less than 15 minutes. This not only reflects the speed and efficiency of their platform but also translates to an average savings of $36 per agreement, as DocuSign stated. (DocuSign, 2022.)

DocuSign offers product features that claim to make documents compatible and accessible. DocuSign does not limit support just for a certain type of document, and they are listing to support almost any possible file format. The users of DocuSign can be guided to fill out the specific fields and information by using Tags, that can be standard or customized if needed. In the case of multiple documents, the platform allows to control the visibility of each document, and signatories can be restricted to access individual documents. (DocuSign, 2022.)

DocuSign offers a dynamic range of options for signing documents, providing users with flexibility in the signing process. The documents can be signed using different routing methods, including serial, parallel, and mixed routing. In practical terms, this flexibility allows companies to decide whether a document can be signed all at once or if it requires signatures from each signatory one by one. This adaptability is particularly valuable when dealing with various document signing scenarios. For organizations engaging in high-volume communication with employees and customers, DocuSign introduces its Bulk Send feature. This feature streamlines the process by allowing the importation of a list of signatories. Subsequently, each recipient receives a unique copy of the document

to sign. This approach eliminates the need for a one-by-one signing approach, enhancing efficiency in large-scale document distribution and signing processes. (DocuSign, 2022.). With the case company's needs Bulk Send feature is not seen as necessity, as agreements are issued per clients, but some other organization could benefit from this feature more.

DocuSign's eSignature platform aligns with regulatory standards such as the U.S. ESIGN Act, UETA, and the EU eIDAS Regulation, ensuring a secure and legally recognized digital signing process. DocuSign states that they automatically generate and store an audit trail for every agreement, this serves as a detailed record, providing transparency and accountability throughout the entire signing process. They also offer different kind or authentication methods that can be used to prove the signatory's identity:

- Email authentication, with this method only signatories that are invited via email to sign the document can sign it
- Access code authentication, where sender-generated code is provided in order to open and sign documents
- SMS Authentication, where signatory receives one-time passcode that recipients need to enter in able to access the documents
- Phone Authentication, where signatory makes a phone call where they need to enter their name and access code to review and sign documents
- Third-Party Authentication, requires additional set of third-party account credentials from Salesforce, Google, Yahoo! Or Microsoft
- ID verification, where the photo of signatory's ID is compared and matched against the agreement information

For added transparency and authentication, all signed DocuSign documents come with a certificate of completion. This certificate serves as conclusive proof of the signing process for all parties involved in the transaction. It incorporates essential information extracted from the audit trail, presenting details on who signed, timestamps indicating when and where each signature occurred, and the finalized document itself. This ensures a thorough and verifiable record of the entire signing journey. (DocuSign, 2022.)

8. Conclusions and Summary

The 2019 global pandemic of Covid-19 acted as a catalyst, for most companies to confront their digitalization shortcomings. The following years of Covid-19 have transformed the daily operations of the companies, including the case company. Despite occasional improvements in the global situation, the evident shift towards a more permanent embrace of remote work is unmistakable.

The case company encountered similar challenges to those experienced by many other businesses during the Covid-19 pandemic. Consequently, the thesis served as a foundational resource for a report on the Digital Signing Process tailored to the specific needs of the case company. Decisions were informed by the insights gained from the testing phase of the Digital Signing Process.

The objective of enhancing the contract approval process was to streamline and expedite the entire procedure. In an ideal scenario, the process would involve only a few steps, ensuring quick completion within a matter of minutes. The contract initiation would follow the traditional approach of being offered via email, though with a digital signature. The offer's terms would dictate the evaluation period for the client's acceptance, typically spanning around 14 days, although this timeframe could vary, ranging from the next day to over a month. Prior to the offer's expiration, the client could specify the designated signatory for the Statement of Work. While some clients might consistently use the same contacts for each contract, there exists the possibility of different contacts signing contracts related to specific or diverse solution areas.

As remote work solidifies its position as a standard practice, the challenges associated with tethering individuals to specific times and locations become increasingly apparent. Embracing digital solutions for signing contracts and agreements aligns with the evolving needs of the case company in this modern work landscape. However, the test phase highlighted certain setbacks and additional work introduced by the Signing solution service. While the service demonstrated efficiency when it worked seamlessly, the digital signing process's issues stemmed not from the service provider itself but from external factors.

Clients adopted the Digital Signing Process well, and following a trial period of a few months, they became fluent in digitally signing agreements. Some clients even proactively inquired about the option, demonstrating a high level of enthusiasm. In conclusion, the thesis recommends that the case company should consider implementing the Digital Signing Process.

After introducing three digital signing providers, Adobe, Visma, and DocuSign, it was observed that there are no significant differences among these providers. Notably, in terms of cost-effectiveness, Visma Sign appears to be the most affordable option for the case company, offering an unlimited number of users. With Visma Sign, the collector (the case company) has the authority to determine whether a document requires strong or light authentication. Strong authentication involves a third party, such as banking codes or mobile ID, to confirm the identity.

In a signed document using Visma Sign, the names, timestamps, and information regarding the country's authentication method used in the signature event are visible. While Visma recommends the use of strong authentication, it is noteworthy that light authentication is also possible. This flexibility addresses concerns raised by clients who may be hesitant to use their private banking IDs as an authentication method in a professional setting.

In general, this thesis introduced the concept of Digital Signing for the case company, providing insights that can be applicable to other companies as well.

References

Adobe Sign. 2022. What is a digital signature & how does it work. Available at: <https://www.adobe.com/sign/digital-signatures.html> Accessed 10.2.2022

Digital and Population Data Services Agency. 2022. Available at: <https://dvv.fi/en/electronic-signatures-of-different-levels> Accessed 12.1.2022

DocuSign. 2022. Available at: < https://www.docusign.com/en-us/> Accessed 14.2.2022

European comission. eSignature FAQ. 2022. Available at: <https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature+FAQ#eSignatureFAQ-Anchor2> Accessed: 20.10.2022

Visma Sign. 2022. Available at: <https://vismasign.com/materials/digital-signature-101/> Accessed 10.2.2022

P. Gallagher (2009) FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Digital Signature Standard (DSS< https://staff.fmi.uvt.ro/~stelian.mihalas/cry_sec/download/DSS/fips_186-3.pdf> Accessed 12.3.2022

Pooja, Mrs. Mamta Yadav. 2018. Digital Signature International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Available at: <https://d1wqtxts1xzle7.cloudfront.net/57333083/CSEIT18364-with-cover-page-v2.pdf?Expires=1651326542&Signature=UUlwfnHYNq~14ogIEoE-hzTcqpVODNZ4Lfyp6mmP3NJ6OoGRaZhjp2kO8Go26Wz3wtbGBxs3ywKYC4qHkJe-mvNHPqIJpIeZGvyFw0VnvXn1oAOiFnpSE-x65s5GOi-WeQ3X3BlJpFX0MQwuJyFln8qLpyMmUKq3MexWzJ1tQXh7WW1Fz9MPHLHhpiNE-7512NZ-kSBiXqlgvVn0WMxKuwN0BjxcajfElisVZEeu-Ep~lpJeEVJGnhH8BL2sWCa57GuKpZB1wN85pwY-gbfB1tGNtGqB8bctw9Dj8QUjJreuZydTyJMmBOCXOy-BQKv9Hjea85yWy9lvW4X1jpz6~Feg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA> Accessed 30.4.2022

Secure Key. 2023. Why Digital Signature Audit Trails Are So Important. Available at: < https://www.linkedin.com/pulse/why-digital-signature-audit-trails-so-essential> Accessed 10.8.2023

V skills certified. 2022. Available at: <https://www.vskills.in/certification/tutorial/digital-signatures-and-public-key-infrastructure-3/> Accessed 7.4.2022

Appendix 1:

This appendix is only for use of the case company.

Appendix 2:

This appendix is only for use of the case company.

Appendix 3:

This appendix is only for use of the case company.