Bachelor's thesis

Information and Communications Technology

2023

Michalis Iona

Digital Signature Integration through a CRM platform

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2023 | 29 pages

Michalis Iona

Digital Signature Integration through a CRM platform

Digital signatures have become a new way to validate agreements and an essential feature in improving the sales process through the CRM platform. With this type of signature, a much more verified and authentic signature is possible in the sales process workflow.

This thesis aimed to integrate a digital signature function in the commissioning company's current customer relationship platform, resulting in a much more efficient sales process concerning signing new agreements or renewals. To finalise and complete the thesis, it was necessary to identify and research all digital signature providers who could meet the company's needs of all stakeholder specifications. Each provider was tested to ensure that all specifications gathered from stakeholders meet the requirements.

This thesis introduces all the necessary information regarding integrating the digital signature functionality in the CRM platform in a secure, legal, and knowledgeable manner. It also shows the algorithmic process of a digital signature and a descriptive analysis of the platform itself.

This result provides a working feature in the commissioner sandbox environment of the CRM with all specifications from the stakeholder achieved. The project's main objective was the research, testing and integration of all providers in the commissioner sandbox, with the commissioner production platform integration and user training yet to be completed.

Keywords:

Digital Signatures, Customer Relationship Management, Regulations, Data Protection, Authentication

Contents

Figures

List of abbreviations

AES	Advanced Electronic Signatures
API	Application Programming Interface
CRM	Customer Relationship Management
elDAS	Electronic Identification and Trust Services
GDPR	General Data Protection Regulation
PKI	Public Key Infrastructure
QES	Qualified Electronic Signatures
SES	Simple Electronic Signatures

1 Introduction

Electronic signatures have been introduced since the 2000s as a new and efficient method of signing and validating many agreements. Today the usage of printing and scanning documents is becoming a way of the past. At the same time, electronic signatures enable all people to conduct an efficient transaction when they want to validate and sign a document.

The authentication process of a signed document used to validate a sales process has been an essential factor in ensuring that the signature would be valid if presented in a court of law. Organisations nowadays go through multiple documents daily, requiring a signature placed for a process to be continued, with the signature representing a person's agreement or authentication of the document's contents. A signature is a mark, or a sign made by a person on a physical document to indicate their intention to approve or endorse the document. In legal terms, a signature on a paper is a form of written consent or acknowledgement that the signer understands and agrees to the terms and conditions outlined in the document. It can also serve as evidence of the signer's identity and intention to be bound by the document's contents.

The elDAS regulation (European Commission, 2022) has been introduced in Europe to clarify the authenticity of a document if it is signed electronically. It provides a clear view that when signatures are not hand-written, they are as valid as possible. An electronic signature has different authentication methods to validate that the person signing the document is veracious. Using the Public Key Infrastructure (PKI) technology also provides security measures with detailed importance of how it would be impossible for any unauthorised user to breach.

On its Customer Relationship Management (CRM) platform, the commissioning company needed to integrate a new feature to introduce a unique digital signature system. This would automate all contracts or agreements for a signature to become much more efficient, providing a healthier and more trustworthy relationship between the organisation and its customers. This integration would boost automation with faster and more secure agreements ensuring a better quality of signatures. If needed, the customer and the organisation can have a well-authenticated signature on the document. Therefore, the objectives of this thesis were to accomplish a well-functioning feature that would satisfy the stakeholders' needs, consider future solutions, and manage the agreements.

This thesis is structured as follows: Chapter 2 introduces the whole process of digital signatures, with a detailed analysis of the regulations and the types of signatures available for authenticating a signature on a document. Chapter 3 presents how the algorithmic process works when establishing an authenticated signature. Chapter 4 gives an overall view of the CRM platform and why it would be used in this case. Chapter 5 provides a scope of the project with a detailed analysis of the work carried out to achieve the thesis objectives. Chapter 6 presents the results and what future aspects can be considered when wanting to automate the process as much as possible.

2 Digital Signatures

2.1 Importance of Digital Signatures

A digital signature process, as shown in Figure 1, confirms the legitimacy and integrity of a digital message or document. This unique signature is applied to the paper using encryption, confirming that the document has not been tampered with and ensuring the organisation or person for the signature is required becomes legitimate. PKI technology is used to complete this process with encryption keys, a public key and a private key (Albarqi et al. 2015). The party that signs the document knows the private key and the user who must confirm it uses a public key. The document and signer's identity are mathematically represented, with the signer's private key used to generate the digital signature and the authenticator's public key used to validate the signature.

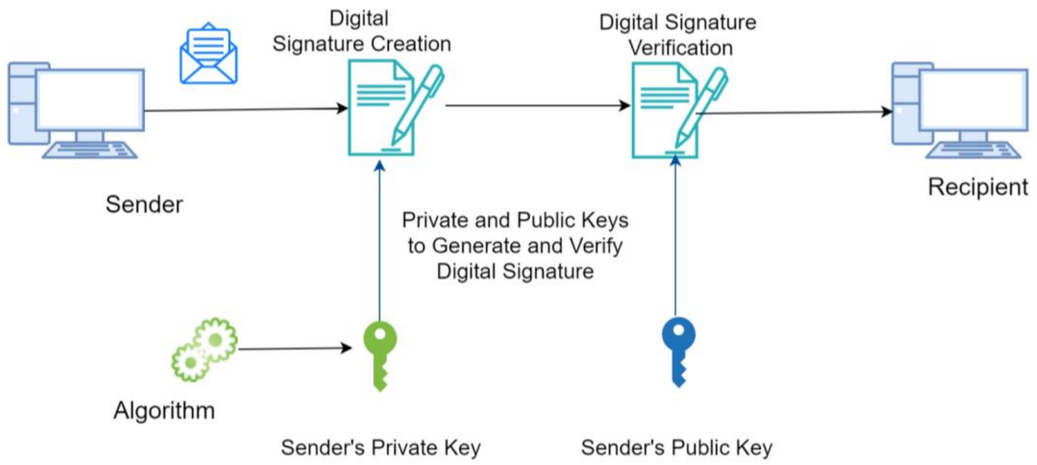

Digital Signature Creation
Digital Signature Verification
Sender
Recipient
Private and Public Keys to Generate and Verify Digital Signature
Algorithm
Sender's Private Key
Sender's Public Key

Figure 1. Digital Signature process. (Bist, 2021)

Compared with the usual paper-based signatures, digital signatures provide several advantages. The sales process in a company becomes much more efficient, with the traditional printing, signing, and scanning parts of the process scrapped. Instead, the documents can be signed electronically. Additionally, the documents used to be signed much more securely due to the encryption used and the temperament of any documents is not possible, as the signature is genuine (Nageotte, 2022). As the requirement of printing or mailing is optional, digital signatures become more affordable than traditional ones. An impenetrable audit trail produced by digital signature systems can be used to follow the procedure and confirm compliance with legal and regulatory signing requirements. Also, automating reminders can be implemented through the electronic signature, completing the process faster. Software development is required for employment to ensure that the software has not been altered and originates from a reliable source.

Companies nowadays tend to change their sales process in modern documentation validation by introducing a secure, affordable and effective CRM system. More importantly, this instrument guarantees the accuracy and veracity of the electronic communication and transaction of the whole signature process for organisations and individuals.

2.2 Regulations and Validation

For digital signature validation to occur, regulations based on location must be concerned and implemented. Relating to the current implementation and area, laws in Europe are to be concerned chiefly, with also an assurance that all countries' business operations take place to follow the proper guidelines.

The eIDAS Regulation is a European Union law (European Commission, 2022) that sets the standards for electronic identification and trust services for electronic transactions in the EU internal market. It aims to create a single demand for electronic identification and trust services, allowing for secure and seamless online interactions between citizens, businesses, and public authorities across the EU. The regulation also establishes a framework for recognising electronic identification schemes used in different EU member states to facilitate cross-border transactions. The eIDAS Regulation came into force on July 1, 2014, and has been applicable since September 1, 2018.

Another validation to consider throughout this project would be the GDPR affecting the storage of documents signed with the bank authentication digital signature. This could provide security but expose the customer's private information with the personal ID being revealed. When completing such a process, no information is disclosed that would tell anyone's confidential information with an assurance that the organisation's CRM platform is not storing any personal GDPR legislated data.

2.3 Authenticating Signatures

Electronic signatures have many different types, depending on your concern about the user's usage. Simple signatures without ID verification don't require such an encrypted and secure data transfer rather than qualified signatures.

2.3.1 Simple electronic signatures

The SES has been the first step in bringing electronic signatures for the possibility of use by many organisations. This type of signature tends to be the least validated due to its lack of authentication and cryptography. It is usually used (Notarize, 2022) for low-risk documents when verifying a recipient's identity as it is not needed upon signing.

2.3.2 Advanced electronic signatures

The AES is the next stage of the SES, and its use is for more unique signatories (Sen, 2022). The process of using this type of signature is to ensure there is control over the key used to sign. If the technique involves and is based on the PKI, it usually qualifies its correct guidelines to be recognised as an AES due to its private and public key usage used for encryption. This method can guarantee integrity and authenticity, but to be ensured of the signer is difficult to tell due to its lack of identity verification.

2.3.3 Qualified electronic signatures

This method is considered the most secure signature available for the most crucial and certain demanding documents. The implementation of QES requires multiple high-security layers (Sen, 2022) taking place for data regarding cryptographic modules when the creation and signature of the paper are stored on reliable and assured devices provided with top-level security standards. Also, a high-security device, such as a cryptographic USB token or hardware security modules (HSMs), must be used to validate this method to ensure a fully secure and authenticated signature.

3 Algorithm Process

3.1 Algorithm Overview

As mentioned in Chapter 2, the document's validity is an essential part of the digital signature process. All parties should ensure their signature is authentic and valid when the verification is complete.

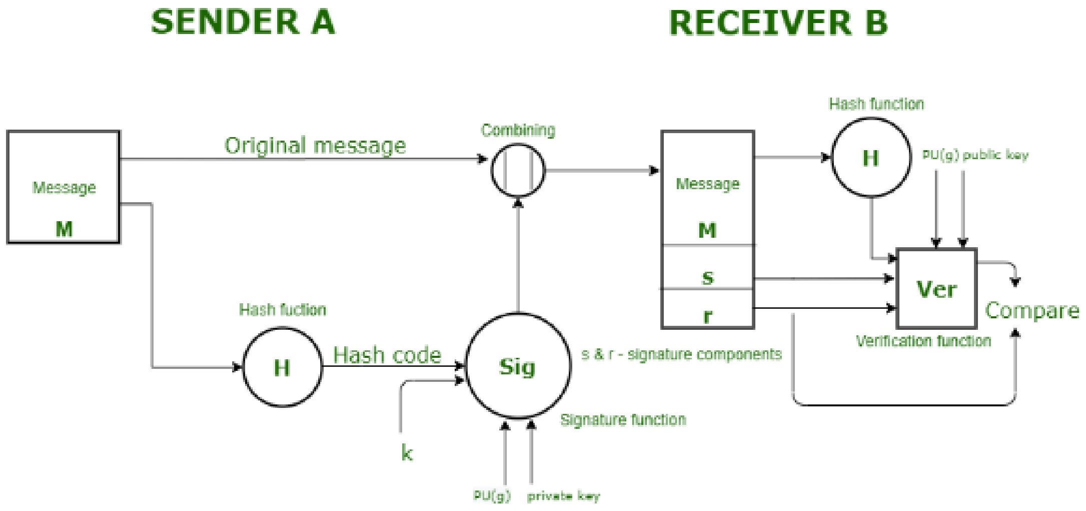


Figure 2. Algorithm in-depth process. (Pekar, 2023)

Figure 2 shows the process involving new cryptographic algorithmic solutions and protocols with a high-level security overview.

To begin with, a signature creation process and signature verification are required for the algorithmic operation to be implemented (Miller, 2020). As the article states, the signer and verifier use a public and private key to complete the process by ensuring the signer generates a signature and thereafter, the verifier verifies it. Both parties have two important keys, with the private key used as a confidential access point for the signature not to be used without the signer's knowledge and the public key to verify the signature.

The next step would be to run the signature process through a hash function, which creates a distinct fixed-length value that serves as the message's representation (Altili, 2021). The hash code is integrated to generate a distinctive digital signature and the sender fuses the private key. The signature identifies the private key and the message being sent. The digital signature has also been decrypted with the verifier obtaining the original hash using the public key. A comparison of the generated hash and the original hash is applied with the same hashing method to the received document. The recipient can be confident that the document has not been altered and that it came from the purported sender if the hashes match.

After a document has been signed, verifying its authenticity and validating its signer are essential for the process. The signer's digital ID certificate status should be authentic and valid to check its validity. There are currently many methods of this validation, with the highest secured one being the QES, along with a need for a trusted certification authority to validate the process. This validation is usually used for legally binding transactions requiring the most robust authentication.

3.2 Public-Key Cryptography

A private and public key pairing can ensure an encrypted transaction when digitally signing a document. Furthermore, these keys are generated using a cryptographic algorithm from multiple mathematical problems described as one-way functions.

One-way functions compute your input through the system but ensure no one can invert your information. This is used for your input cryptographically to provide a secure data transfer from the user's perspective.

$$\Pr[f(F(f(x))) = f(x)] < n^{-c}$$

Figure 3. Equation of one-way function.

Figure 3 signifies the one-way function, with (Rompel, 1990) providing a more detailed understanding of this mathematical process. A one-way functionality was a necessary usage to ensure that a pseudo-random generator took place.

This method ensures confidentiality when digitally transferring a message or a signature; in this case, the only way is using the user's public key to encrypt a message and decrypt it only with the pair of it, the user's private key.

4 Customer Relationship Management Platform

4.1 Platform Capabilities

Throughout history, businesses had a more time-consuming method of maintaining good customer relationships, as the management and storage of information had to be physically stored. Nowadays, most companies use a Customer Relationship Management platform where all data is stored through software, which provides a much more convenient way for salespersons, marketers, or even finance advisers to oversee information of all relationships and interactions with customers related to their day-to-day sales operations.

Moreover, the platform provides practical reasoning for instant access to information, with automation to processes connected with all activities regarding the customer's journey (Wlosik, 2022). This also ensures healthy customer relations regarding loyalty, adapted through an analysis enquiring through their revenue provided and the historical communication exchanges in-between.

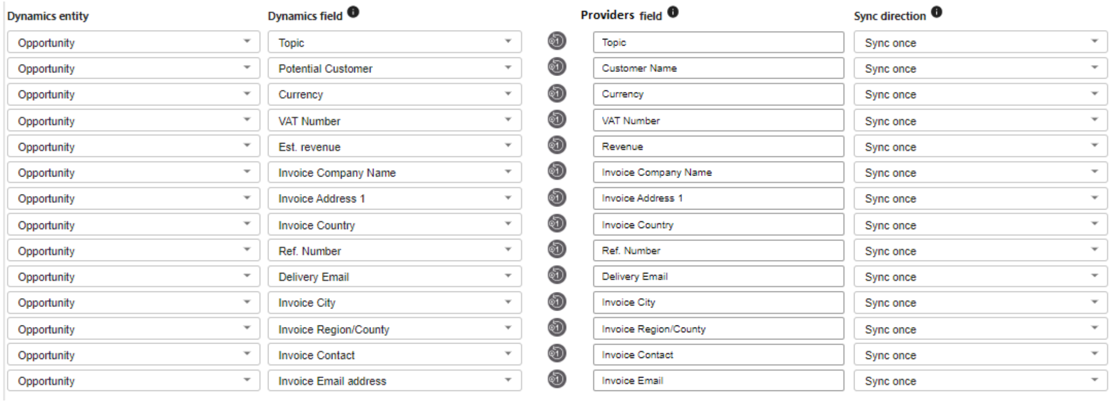
Throughout the platform's usage, setting up automation is a keen interest for all parties. For example, repetitive tasks in the CRM must be managed daily, but with the automation process (Wlosik, 2022), countless hours can be saved from numerous employees with the possibility of exploring a better understanding of the sales pipeline or prospects coming in. Digital signatures, in this case, would be a fundamental matter to be implemented from both the customer and the salesperson, as it provides an enormous difference in timesaving, as well as the authentication verification for contracts to be taken.

4.2 Sales Process

The commissioner has detailed their current sales process through the CRM, analysing all steps taken. First, information based on the customer is all taken into the account entity and transferred to the contact information entity, which can be found through the opportunity form in the CRM platform. All necessary details, such as payment terms, delivery and invoice details, prices, and products, can be found through the opportunity form. When all essential information is met, a quotation document can be generated based on the language used and which business unit the user belongs to. This generated document is used as an agreement to be sent to the customer for a signature to take place. The agreement also includes up-to-date terms and conditions, with the possibility of editing in case of necessary changes. Usually, new customers must sign the delivery agreement with old ones for a renewal to be accepted, which can be verified through an email. When the deal is signed, it is stored in a storage management system, where all business units have unique ways of keeping it.

4.3 Data Mapping

Data storage has played an essential role in developing better relations between a salesperson and a customer by providing all necessary information about a product's sale. Several types of data mapping depend on the CRM system and the integration requirements.



Dynamics entity	Dynamics field	Providers field	Sync direction
Opportunity	Topic	Topic	Sync once
Opportunity	Potential Customer	Customer Name	Sync once
Opportunity	Currency	Currency	Sync once
Opportunity	VAT Number	VAT Number	Sync once
Opportunity	Est. revenue	Revenue	Sync once
Opportunity	Invoice Company Name	Invoice Company Name	Sync once
Opportunity	Invoice Address 1	Invoice Address 1	Sync once
Opportunity	Invoice Country	Invoice Country	Sync once
Opportunity	Ref. Number	Ref. Number	Sync once
Opportunity	Delivery Email	Delivery Email	Sync once
Opportunity	Invoice City	Invoice City	Sync once
Opportunity	Invoice Region/County	Invoice Region/County	Sync once
Opportunity	Invoice Contact	Invoice Contact	Sync once
Opportunity	Invoice Email address	Invoice Email	Sync once

Figure 4. Field mapping.

Effectively as shown in Figure 4, field mapping has been the critical aspect of most data integrations in CRM systems. This involves mapping fields in one system to another, with corresponding fields to ensure that alignment and consistency are crucial for correct data to be shown across separate platforms. The data model for the Dynamics CRM platform has the complexity of how the data mapping is structured. It supports an extensive range of data types, including the standard entities such as contacts, accounts, leads, or even opportunities, with the possibility of customisable entities that developers create for a personalised business process that many different companies would like to include. Microsoft Dynamics 365, in this case, use three different relationship types (Gestisoft, 2021) to define data:

- One to Many: An association from a primary entity to many related entities records due to a field lookup.
- Many to One: The opposite of the one-to-many relationship with a view from the related entity.
- Many to Many: Multiple records of one entity to be associated with multiple records of another.

The above types show different entity relationships that can be established through the platform. The organisation and storage of the data in the system enable all users to analyse and access the data efficiently.

4.4 Data Security

A CRM system contains tons of data that should comply with regulations accordingly and have many security measures. As a business, your main priority is to always satisfy your customers by preventing the exposure of sensitive data and ensuring no data breaches occur, to maintain a trustworthy relationship.

The visibility of data is one of the leading security issues many companies face, as companies usually collect more data than they need (Roy, 2019). Completing the sales process using a CRM, issues are solved, as it assures that companies would contain only the necessary data required and no loss of valuable data will occur. Although the CRM keeps the essential data stored, data privacy is crucial; it should be kept private by giving only the right people within an organisation the right to view and edit such information. While managing the data through a CRM, layers of security are available by default, due to the platform being able to protect the data itself (Roy, 2019). Data governance in the EU should be followed as the commissioner requires accessibility following regulations through GDPR.

5 Project Scope

5.1 Planning

This study utilises the Microsoft Dynamics 365 SANDBOX platform provided by MagiCAD Group Oy. The environment has been used for developing, testing, and validating the eSignature functionality in their platform under the Opportunities form, using digital signature providers suggested within the company. A JIRA ticketing system has been used for progress and task tracking for the completion of the project to conclude.

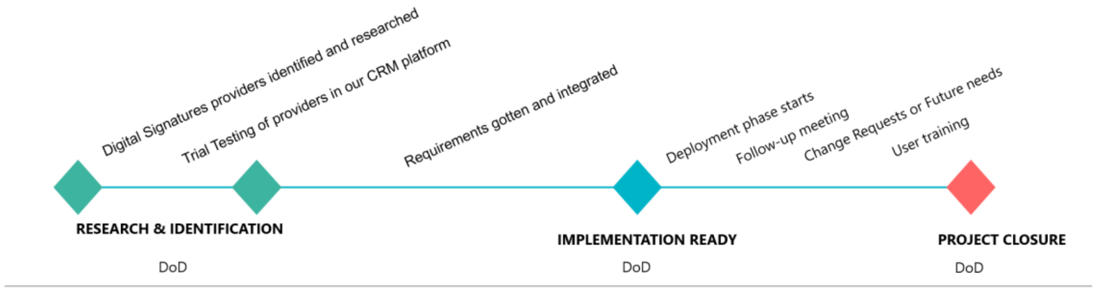

Digital Signatures providers identified and researched
Trial Testing of providers in our CRM platform
Requirements gotten and integrated
Deployment phase starts
Follow-up meeting
Change Requests or Future needs
User training
RESEARCH & IDENTIFICATION
DoD
IMPLEMENTATION READY
DoD
PROJECT CLOSURE
DoD

Figure 5. Project scope.

As presented in Figure 5, a project scope has been created to have a working eSignature functionality that all CRM platform users can adapt and use.

The project has begun with research and identification of all services providing a digital signature capability allowing integration into Microsoft Dynamics 365 and acknowledging the process of digital signature usage. Services have been identified with all specifications reviewed and tested.

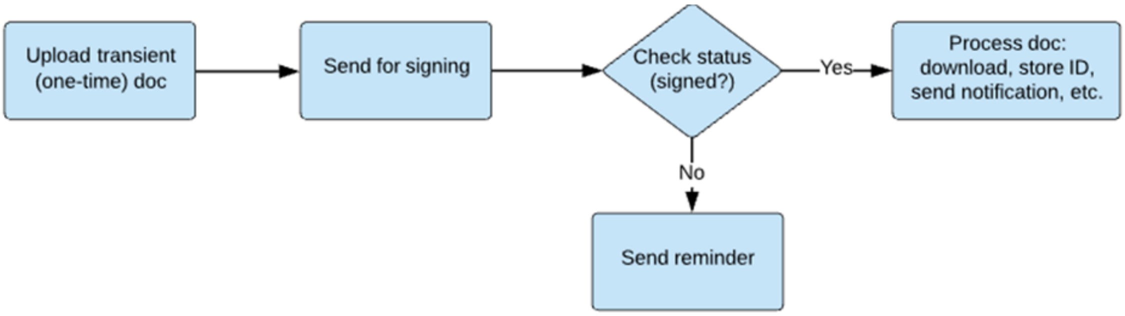
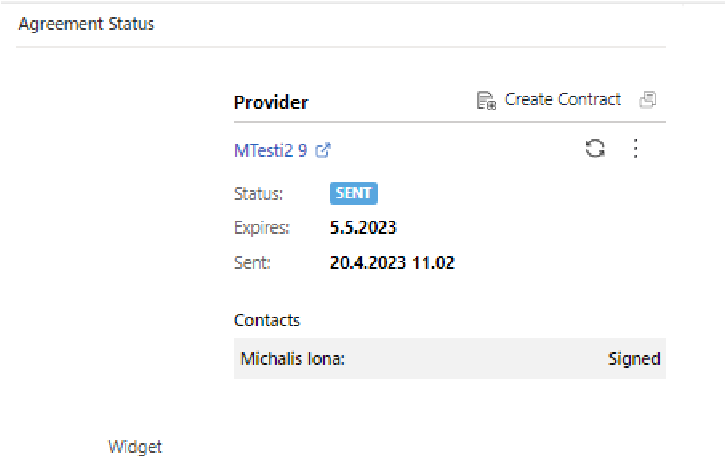

Upload transient (one-time) doc
Send for signing
Check status (signed?)
Yes
Process doc: download, store ID, send notification, etc.
No
Send reminder

Figure 6. eSignature to the current sales process. (Acrobat Sign, 2023)

Figure 6 shows the updated sales process, which would replace the hand-written signature, removing the need for printing and scanning upon signing agreements.

5.2 Testing of Providers

Firstly, digital signature providers used for my study have been integrated and tested throughout the platform for a further review of the company's interests. Research of features and functionality of each provider has been identified, with significant measures taken to conduct an efficient sales process.



Agreement Status

Provider

MTesti2 9

Status: SENT

Expires: 5.5.2023

Sent: 20.4.2023 11.02

Contacts

Michalis Iona: Signed

Figure 7. Integration result of a digital provider in the opportunity form.

Figure 7 displays an example of creating a contract with a certain provider. When contract generation occurs, each provider varies, as some contracts can be generated through the Dynamics 365 platform and others in their own providers' environment. Template creation and syncing between the provider and the CRM platform have been studied and researched, by testing various fields and data structures between them. It involves data fields between the CRM and the providers' system, mapping all data necessary to create a contract. This would ensure a seamless data flow, without any loss of information for the successful integration of both approaches to be aligned with.

However, minimisation of errors and data inconsistencies may appear due to manual or incorrect data entry.

In the course of creating a contract, fields of data can be edited. A reminder automating setup, as well as the role selection of all users involved within the contract, could be adjusted, with the possibility of choosing what type of signature should be required to fulfil your needs.

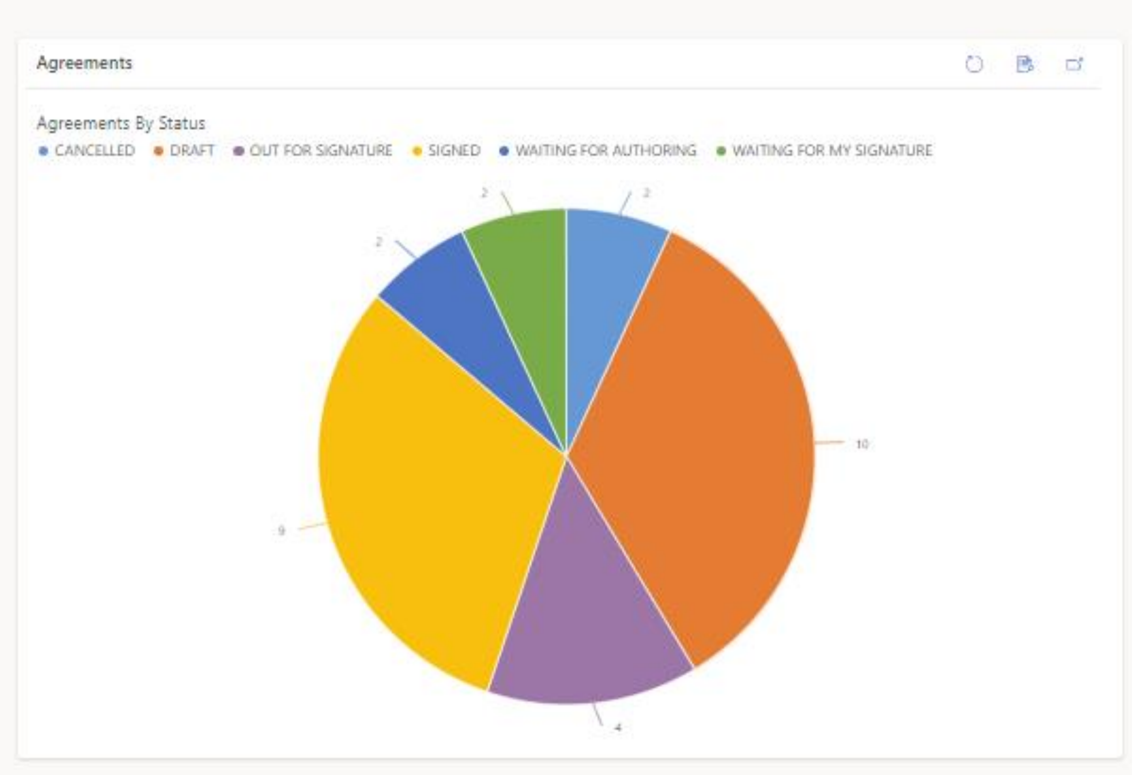


Figure 8. Statistics of all outputs.

Figure 8 shows the statistics of each output possible after a signing process has been completed or drafted. This can provide a more in-depth analysis of how well the system is used and if any pending contracts need to be concerned.

The storage of all contracts has a different approach based on each provider. Some providers can use their platform to store all documents generated and signed, with the possibility of each allocated user group viewing only the agreements they have been involved in. A contract management system is also available through syncing a cloud-based storage management provider through automating a power automate command that would be used to store all completed contracts in their allocated file respectfully.

After identifying and researching all digital providers best suited for the CRM system, a stakeholder demonstration meeting has been held to determine the best solution for improving the current sales process. Technical feedback was gathered with requests for any extra features required.

6 Results

The thesis results showed an implementation of the basic functionality of the e-signature method in the Opportunity form, through the commissioners' company Dynamics 365 Sandbox platform. Integration, testing, validation, and gathering feedback for future ideas and specifications needed, were the main tasks given for the completion of the project. This thesis demonstrates and presents the research and analysis required for a feature to be inputted into the company's current sales process efficiently, saving time when creating new opportunities for new customers or renewals.

Research and identification of digital provider services have been integrated and tested with results demonstrated to stakeholders. Integration of API capabilities and documentation of the process and specifications have been recorded for inner communication decision-making within the organisation.

The implementation of testing through the Dynamics environment exhibited significant results for a functioning feature that would work smoothly within the updated sales process, which was also demonstrated to the stakeholders.

The Sandbox environment was a keen use for data map testing in ensuring all entities can be synced with the provider’s template, resulting in data being transferred from the Opportunity form to the ready-made document. A solution was researched for the one-to-many relationship entities, with a conclusion for the need of 3rd party tools needed or a small self-made project that would be considered later.

7 Conclusion

The objective of this thesis was to research and analyse all information that must be considered about digital signatures, providing an outcome of a satisfactory electronic signature feature in the commissioner CRM platform. The testing was a key part of the functionality in the Sandbox environment, from all research and identification of digital signature providers that would satisfy the commissioner's requirements. An essential successful feature has been integrated into the Dynamics 365 Sandbox platform, but more stakeholder specifications are needed for this solution to be transferred to production. Basic templates were also created, with certain data mapping still being an issue in transferring the data from the CRM to the provider.

The essential integration of the e-signature was the project's main result, with other future concepts that can be considered after the integration has been completed for a more automated experience. The project could have been taken forward by developing, validating, and testing more features on top of it to automate the sales process.

Regarding the future concepts, an automation for storing contracts through storage management would be ideal, to ensure all signed contracts are recorded and found efficiently when searching for a specific one. These contracts can be stored through some of the available digital provider platforms or by syncing and creating an automated command; when a specific user completes a contract, it can be accumulated through cloud-based storage management.

With each product or region of sales, a template can be created and allocated, without having to generate a contract from scratch each time a signature process begins. Template creation with data syncing is currently the main issue when involving a digital provider, as the one-to-many relationship with certain entities is not supported. For example, if a digital signature is applied to a parent record with multiple child records, any changes made to the child records could invalidate the digital signature on the parent record. The digital signature is based on the original data; any changes to related documents could alter the original data. To ensure that the digital signature remains valid, all associated records would need to be updated to maintain the integrity of the data. This can be a complex process, mainly if multiple layers of relationships are involved.

User training and guidance creation for the final phase of the digital signature project are crucial to ensure all CRM users use this new feature smoothly.

References

Acrobat Sign API overview¶ (2023) Acrobat Sign API Overview - Acrobat Sign Developer Guide. Available at: https://opensource.adobe.com/acrobat-sign/developer_guide/index.html (Accessed: April 26, 2023).

Albarqi, A., Alzaid, E., Alghamdi, F., Asiri, S., & Kar, J. (2015). "Public Key Infrastructure: A Survey". Journal of Information Security, 6, 31-37.

Altili, E. (2021) Cryptography, encryption, hash functions and digital signature, Medium. DataDrivenInvestor. Available at: https://medium.datadriveninvestor.com/cryptography-encryption-hash-functions-and-digital-signature-101-298a03eb9462 (Accessed: February 1, 2023).

Bist, M. (2021) Electronic signatures vs Digital Signatures, eSign Genie. Available at: https://www.esigngenie.com/blog/electronic-signatures-vs-digital-signatures/ (Accessed: April 18, 2023).

Eidas regulation (2022) Shaping Europe's digital future. Available at: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (Accessed: January 25, 2023).

Gestisoft (2021) What is field mapping in Dynamics 365?, Gestisoft. Gestisoft. Available at: https://www.gestisoft.com/blog/field-mapping-dynamics-365 (Accessed: April 18, 2023).

Legislation: Data Protection Ombudsman's office Tietosuojavaltuutetun toimisto. Available at: https://tietosuoja.fi/en/legislation (Accessed: April 17, 2023).

Miller, T. (2020) Digital Signature Verification: How to verify a digital signature, @PDFelement. Available at: https://signx.wondershare.com/knowledge/digital-signature-verification.html (Accessed: January 26, 2023).

Nageotte, A. (2022) The benefits of the electronic signature, Oodrive. Available at: https://www.oodrive.com/blog/uncategorized/benefits-electronic-signature/ (Accessed: April 17, 2023).

Notarize (ed.) (2022) 3 different types of digital signatures and when to use them - real estate, Notarize. Available at: https://www.notarize.com/blog/3-different-types-of-digital-signatures-and-when-to-use-them (Accessed: April 19, 2023).

Pekar, R. (2023) Digital Signature Standard (DSS), GeeksforGeeks. GeeksforGeeks. Available at: https://www.geeksforgeeks.org/digital-signature-standard-dss/ (Accessed: April 27, 2023).

Rompel, J. (1990) One-way functions are necessary and sufficient for secure signatures, and One-Way Functions are Necessary and Sufficient for Secure Signatures. Available at: https://www.cs.princeton.edu/courses/archive/spr08/cos598D/Rompel.pdf (Accessed: April 19, 2023).

Roy, S. (2019) Can your CRM help you comply with Data Privacy Regulations?, Tech Wire Asia. Available at: https://techwireasia.com/2019/01/can-your-crm-help-you-comply-with-data-privacy-regulations/ (Accessed: April 18, 2023).

Sen, A.A. (2022) Types of electronic signatures : AES & QES explained: Certinal, E Signature Solution by Certinal. Available at: https://www.certinal.com/blog/electronic-signatures/decoding-aes-and-qes-to-ace-your-e-signature-usage.html (Accessed: April 19, 2023).

Wlosik, M. (2022) What is a CRM and how does it work? - Clearcode blog, Clearcode. Available at: https://clearcode.cc/blog/how-does-crm-work/ (Accessed: January 25, 2023).