TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Erik Kangilaski 232609IVGM

Digitising Governance: A Practical e-Signature Solution for Djibouti's e-Cabinet

Master's thesis

Supervisor:	Ingrid Pappel, PhD
	Associate Prof.
Co-supervisor:	Karin Oolu, MA

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Erik Kangilaski 232609IVGM

Üleminek digivalitsemisele: Digiallkirja lahenduse loomine Djibouti e-kabinetile

Magistritöö

Juhendaja: Ingrid Pappel, PhD
Kaasprofessor
Kaasjuhendaja: Karin Oolu, MA

Tallinn 2025

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Erik Kangilaski

12.05.2025

Abstract

When thinking about a digitally advanced country, digital services are often the first aspect that comes to mind. However, as with most complex systems, the most critical foundations tend to remain invisible. This is especially true in low e-government maturity contexts, where digital transformation begins with the shift from paper-based workflows to digital ones, typically starting with internal correspondence systems such as Electronic Document and Records Management Systems (EDRMS) and e-cabinet solutions. One essential component, however, is often overlooked: the ability to digitally sign documents. Without this, documents must be printed, physically signed, scanned, and archived, reintroducing inefficiencies, increasing workload, and undermining the benefits of digitalisation.

In response to this gap, the present research introduces a practical digital signature solution tailored for environments where full-scale public key infrastructure (PKI) is not yet in place. The solution is tested and validated as an artefact that enables secure and verifiable electronic signing, allowing internal government workflows to become fully digital. A design science methodology was used to develop and validate the artefact. The result is a lightweight, secure, and context-appropriate signing system for low-resource settings, offering a meaningful step forward in improving administrative transparency and efficiency.

Keywords: Digital Signature, Electronic Identity, e-Government, e-Cabinet, Djibouti

This thesis is written in English and is 58 pages long, including 6 chapters, 14 figures and 15 tables.

Annotatsioon

Mõeldes digitaalselt arenenud riigi peale, tulevad kõigepealt meelde e-teenused, kuid nagu enamiku keerukate süsteemide puhul, jäävad kõige olulisemad alustalad tihti märkamata. See kehtib ka madalama digitaliseerituse tasemega riikide digipöördel, kus alustatakse järk-järgult paberdokumentide põhise töökorralduse väljavahetamist elektroonilistega – üldjuhul alustades asutuse siseste dokumentidega ning võttes kasutusele elektroonilise dokumendihaldussüsteemi (EDRMS) ja e-kabineti lahendused. Selle käigus aga on kerge jätta märkamata digiallkirjastamise võimekus. Ilma digiallkirjastamiseta kaovad digitaalse töövoo eelised efektiivsuse osas, sest dokumendid tuleb allkirjastamiseks uuesti välja printida, seejärel kirjalikult allkirjastada, skaneerida, ning paberversioon arhiveerida.

Käesolev uurimustöö leiab lahenduse eelnimetatud probleemile, arendades välja digiallkirjastamise infosüsteemi riikidele, kellel ei ole veel avaliku võtme taristu (PKI) kasutusvalmis. Loodud lahendus võimaldab minimaalselt töötava toote näol turvaliselt ja kontrollitavalt dokumente digiallkirjastada, võimaldades avaliku sektori töövoogude lõplikku digitaliseerimist. Töö koostamisel on kasutatud disainteaduslikku lähenemist artefakti arendamiseks ja valideerimiseks. Uurimistöö tulemusena valmis kergesti kasutatav, turvaline ja praktiline elektroonilise allkirjastamise süsteem, mis sobib just kitsama eelarvega riikidele, pakkudes kaasaegset töövoogude digitaliseerimise lahendust.

Võtmesõnad: Digiallkiri, Elektrooniline identiteet, e-riik, e-kabinet, Djibouti

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 58 leheküljel, 6 peatükki, 14 joonist, 15 tabelit.

List of abbreviations and terms

AdES	Advanced Electronic Signature
AdES/QC	Advanced Electronic Signature Strengthened by a Qualified Certificate
AI	Artificial Intelligence
API	Application Programming Interface
ASiC-E	Associated Signature Container - Extended
DMS	Document Management Systems
DSR	Design Science Research
EDRMS	Electronic Document and Records Management Systems
EGDI	E-Government Development Index
eID	Electronic Identity
eIDAS	Regulation for Electronic Identification and Trust Services
EU	European Union
FURPS+	Categorisation framework
G2G	Government-to-Government
G7	Intergovernmental Forum of Canada, France, Germany, Italy, Japan, the UK, and the USA
ICT	Information and Communications Technology
ID	Identification
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LOA	Level of Assurance
LOSI	Local Online Service Index
MFA	Multi-Factor Authentication
MoSCoW	Prioritisation framework
MVC	Model–View–Controller architectural design pattern
OSI	Online Service Index

PDF	Portable Document Format
PHP	Scripting language for web development
PIN	Personal Identification Number (used to confirm identity or sign digitally)
PKI	Public Key Infrastructure
QES	Qualified Electronic Signature
RMS	Records Management System
SMS	Short Message Service
SSCD	Secure Signature Creation Device
ZIP	Archive file format
TAM	Technology Acceptance Model
TSA	Time Stamping Authority
UN	United Nations
USD	United States dollar
VIIS	Estonian governmental session information system
XAdES	XML Advanced Electronic Signatures

Table of contents

List of figures

List of tables

1 Introduction

In the current era, digital technology is a key enabler [1], as electronic solutions for bureaucratic tasks are often significantly faster and more efficient than traditional paper-based approaches. While Estonia and many Western countries have reached a high level of digital maturity, there are still regions that are only beginning their digital transition. For them, the most visible improvements often come last, while a considerable amount of foundational work must be done first.

This challenge also appears in Djibouti, where the need for digital transformation has been recognised and the implementation of an Electronic Document and Records Management System (EDRMS) for internal processes has already been initiated. However, based on interviews and on-site visits, it became clear that one critical component is still missing: an electronic signature solution. Without it, fully digital workflows are not possible, as documents still require printing and manual signing.

This introductory chapter provides the broader background to this issue and outlines the need for a rapid digital signature solution. It also defines the research questions, objectives, methodology, development approach, and the overall structure of the thesis.

1.1 Country Background: Djibouti

Djibouti is a country in Africa, approximately half the size of Estonia, located next to Ethiopia, Somalia, and Eritrea, and having a sea border with Yemen. Initially governed by Sultanates, in 1862 the French were allowed to establish a colony where mostly Afar and Somali people began to settle. As a result of the third referendum, the population gained independence in 1977, granting nationality to ethnic Somalis and Afar. In 2023, the population was estimated to be nearly one million inhabitants, most of them living in the capital, Djibouti City, which is slightly larger than Tallinn. The official languages are French and Arabic, although many also speak Somali or Afar languages [2].

The World Factbook describes Djibouti as a presidential republic. However, in practice, the political system is characterised by a dominant-party structure, with significant executive influence over the legislative and judicial branches [2], [3].

Most inhabitants of Djibouti are Sunni Muslims, while a little more than one-twentieth, mainly those born outside of Djibouti, adhere to Christianity or other religions [2].

Djibouti is considered one of the hottest locations in the world when evaluating average temperatures. During the cooler periods, daily temperatures remain around 30 °C, even at night, while in warmer periods, they can rise to 50 °C. Near the coast, the climate is humid, but it becomes dry and desert-like inland. Although the warm climate can be enjoyable for short periods, it significantly limits agricultural activity, and almost all food products must be imported [2].

Despite challenges such as poverty, limited literacy, and high unemployment, Djibouti stands out in the region for its relative stability and safety. Compared to several neighbouring countries, it offers a more secure and predictable environment for both residents and visitors. While most buildings are enclosed by fences, the atmosphere in daily life is generally peaceful, and the local population is known for being welcoming and hospitable. It is common to move around safely even after dark. In addition, Djibouti provides shelter to a significant number of refugees, reflecting its role as a stable host in a turbulent region [2].

In addition to political stability, Djibouti benefits from an excellent strategic location. Situated at the Horn of Africa along the Europe to Asia maritime route, it serves as a major connection point for international submarine cables and hosts military bases from the United States, France, China, Italy, and Japan [2], [4].

As a relatively small African country, Djibouti sometimes experiences short electricity outages, even in higher-end buildings. Internet services are available, but they are expensive and not accessible to all residents. Some Estonian mobile carriers do not have roaming agreements in Djibouti.

In its national development agenda "Djibouti 2035," the country describes itself as the lighthouse of the Red Sea. The strategy identifies five key pillars: national peace and unity, good governance, a diversified and competitive economy, consolidation of human capital, and regional integration. In the economic section, it emphasises the expectation that the private sector will serve as the main driver of growth [4].

1.2 Problem Statement

The core problem addressed in this thesis is the absence of a digital signature solution that can be used in Djibouti's EDRMS. In digitally advanced countries, public key infrastructure (PKI), legal frameworks, and trusted digital identity systems are already established, allowing documents to be signed and validated electronically in a seamless, secure, and efficient way. However, in low e-government maturity contexts such as Djibouti, this foundation is missing, and the workflows remain paper-based. Even some European countries like Spain have struggled to fully modernise administrative workflows despite significant investments [5].

One of the main challenges in Djibouti is the outdated nature of internal correspondence workflows between ministries. Although an EDRMS has been technically implemented, its usage is stalled because there is no way to digitally sign documents. Without digital signature support, documents must be printed, physically signed by ministers or senior officials, scanned, and then re-uploaded to the system. This process not only negates the benefits of digitalisation but also introduces inefficiencies, adds workload, and requires the continued use of physical archives and logbooks. As a result, even though a digital system is in place, ministries are still relying on paper workflows for signing, making the digital process incomplete and inefficient.

While the EDRMS could technically operate without digital signatures, the lack of a verifiable signing mechanism makes it impossible to confirm the authenticity of actions such as approvals or rejections. Since all outgoing correspondence still requires a physical signature, implementing digital systems without signing capability creates a trust gap. The situation leads to low adoption rates, as stakeholders do not see the added value of replacing the manual workflow if signing must still be done on paper. Therefore, the absence of digital signature infrastructure has become the primary bottleneck in advancing digital governance in Djibouti.

Djibouti has taken several steps toward digital transformation. In 2018, the World Bank announced a public administration modernisation project [6]. In 2022, Djibouti adopted the X-Road platform for secure data exchange [7], and in recent years, the EDRMS solution WebDesktop has been implemented across ministries. Despite this progress, the lack of a digital signature solution has prevented ministries from using the system in practice. Official documents are still delivered physically across institutions in the capital, taking days to reach their destination and increasing the risk of loss or manipulation.

This thesis is motivated by the author’s direct involvement in four field missions to Djibouti through the GovStack initiative, where the limitations of the system were observed firsthand. The field missions were carried out between April 2024 and April 2025, with three of them one week long and the fourth lasting two weeks. Although the technical infrastructure for digital document management was already in place, it became clear that without a practical signing solution, the entire transformation risked failure. This work proposes a lightweight and rapidly deployable digital signature solution tailored for low-resource environments. The goal is not to replace long-term national PKI infrastructure but to bridge the gap and enable EDRMS adoption while such systems are being developed.

The primary stakeholders who will benefit from this research are the officials within Djibouti’s ministries. With the implementation of the EDRMS and digital signature solution, they can finally start using a streamlined system for both internal and external correspondence, as well as for legislative drafts approval. Together with the signing solution, the entire process will become more efficient, secure, and transparent.

Another important stakeholder, though less visible, is the citizen of Djibouti. While they might not see the changes directly, the faster and more efficient processes enabled by the EDRMS and digital signature solution will ultimately improve their interactions with government services, making their lives easier.

This research also has implications beyond Djibouti. It highlights how similar low-trust-level digital signature solutions could be implemented quickly and effectively in other developing countries, offering a path for their digital transformation. In addition, the findings from this research will be valuable for policymakers who are seeking practical strategies for digitalisation and for researchers globally who are studying e-governance in regions with low digital maturity.

1.3 Research Questions

Based on the semi-structured interviews and document reviews carried out, the biggest issue identified is the lack of an electronic identity system. Therefore, the core objective of this research is to provide a solution of artefact to allow digital signature creation and validation within the ministries, enabling workflows to begin digitalisation. Although the Djiboutian government has shown interest in building a national electronic identity (eID) infrastructure, progress has been slow and fragmented. A smaller scale but high-quality solution could serve as a practical starting point to bridge the current gap.

The ideal outcome of achieving these objectives would be the implementation of this solution within Djibouti’s ministries. However, it is important to note that although the artefact may be technically ready and has received verbal support from government officials, it cannot be deployed in practice until it becomes legally binding. This falls outside the timeframe and scope of this thesis.

Additionally, this artefact is meant only for secure digital signature functionality. While it features some elements of electronic identity, this is not an electronic identity platform in the same way as Estonia’s national eID solution. It is designed for internal governmental use only, and the quality of the identity verification process depends on how the government manages account creation and access rights.

To guide the development and validation of the solution, the following four research questions have been formulated:

RQ1: What are the main challenges and limitations in Djibouti’s internal ministerial workflows that the EDRMS aims to address?

This first research question validates the author’s understanding of the problem and the missing signature solution while enabling the author to find out other important problems that should be addressed during the project of implementing the EDRMS within Djibouti’s ministries.

RQ2: How do stakeholders perceive the current EDRMS implementation, and what gaps remain for achieving fully digital workflows?

This question focuses on gathering feedback from the actual users of the system, public officials, to understand their level of readiness, expectations, and concerns. Their insights reveal both technical and organisational challenges, which guide the design of the digital signature solution.

RQ3: What are the requirements for a digital signature solution that can address these gaps and support efficient and secure document signing within the EDRMS context?

As the digital signature solution is only as good as the technical requirements and features described before development, the requirements need to be analysed and defined carefully before creating the artefact. This ensures that the artefact developed during this research directly addresses the identified concerns and provides a practical solution.

RQ3.1: What levels of trust are required for digital signatures in different types of correspondence and documents in Djibouti's ministries?

In European context, identity validation is strict, as it gives the strength to the signature. Yet multiple levels of trust are defined in eIDAS regulation, and therefore as the Djibouti's context the identification strength might differ on document types, then it is important to find answer for this question as well to understand, if the approval process of new law requires the same identity validation trust level as answer for citizen's incoming document.

1.4 Research Design and Methodology

This study adopts a design science approach in order to deeply analyse the problem and develop a practical digital signature solution as an artefact. This is particularly well-suited for addressing real-world challenges in low-digital-maturity settings like Djibouti, as it enables both a deep contextual understanding of the implementation environment and the iterative development and validation of a technological solution [8], [9], [10], [11].

It includes understanding the current status of the EDRMS implementation project, including the causes for delays, stakeholder perceptions of the project outcomes, and attitudes toward the necessity of such systems. To gain a comprehensive understanding of the situation, six semi-structured interviews were conducted with relevant stakeholders in Djibouti. The interviewees included an IT specialist, cybersecurity officer, ministry official, minister's assistant, department director, and a private IT company CEO, and were focused on existing document workflows, readiness for digitalisation, perceptions of trust in authentication, and anticipated challenges. These interviews were complemented by document and process reviews, carried out during the first three on-site field visits to Djibouti.

Based on insights gathered during the data collection phase, the design science approach was employed to design and refine a digital signature solution tailored to the Djiboutian public administration context. The artefact development followed an iterative and agile-inspired process, where feedback from stakeholders was used to improve the prototype over multiple cycles. This approach aligns with the core principle of design science: solving real-world problems with structured, evidence-based methods [8], [12]. The goal was to create a practical, scalable solution that can support low-maturity e-government environments like Djibouti by improving inter-institutional collaboration, transparency, and trust [13].

Research in such settings is typically exploratory and evolves through ongoing feedback loops, making flexible methods especially valuable [11]. Agile-inspired development processes – such as prototyping, incremental testing, and refinement – reinforce the iterative nature of both design science and case study research [11], [14].

After the artefact was completed, it was presented to stakeholders during a workshop and tested independently by end-users. Their feedback was analysed and used to introduce necessary improvements to the artefact, ensuring its relevance, usability, and technical adequacy for local deployment.

To ensure trustworthiness of the findings, the study applied data triangulation by combining three sources: semi-structured interviews, document and process reviews, and stakeholder feedback sessions. While the interviews provided insight into user needs and expectations, the process documents illustrated actual workflows. Feedback sessions in the final phase were crucial to assessing how the artefact performed against real needs.

In line with design science evaluation practices, artefacts can be assessed through artificial methods (e.g. simulations, lab tests, mathematical analysis) or naturalistic methods (e.g. field-based observation, case studies) [15], [16]. This research adopted a naturalistic, exploratory case study evaluation, which aligned with the real-world environment where the artefact was both built and tested [8], [13], [17]. As design science literature suggests, combining ex-post and naturalistic evaluation provides the most meaningful insights into an artefact's feasibility and utility in a given organisational context [9], [15].

This study employed ex-post evaluation with a fully instantiated artefact and real stakeholders. This summative evaluation method focuses on real users, real problems, and real systems, thereby reducing the risk of biased or theoretical assessment [13], [15].

During the writing process, artificial intelligence (AI)-based tools (ChatGPT) were used for grammar correction, style improvement, and structural suggestions. All content was authored and reviewed.

1.4.1 Design Science

The design science methodology was adopted in this research to develop and iteratively refine a digital signature solution tailored to Djibouti's governmental context. Design science is particularly well-suited for constructing and evaluating IT artefacts in response to identified organisational problems. As a methodology, it emphasises the creation of innovative, useful artefacts through structured and rigorous research processes [8], [10]. In this project, the artefact took the form of a web-based digital signature system aligned with existing workflows and technical capacities.

This research follows Hevner et al.'s well-established three-cycle model of design science [12]. The Relevance Cycle connects real-world needs – gathered during field observations, interviews, and document analysis – with design requirements. The Design Cycle consists of iterative development and evaluation, where stakeholder feedback was used to refine the prototype. The Rigor Cycle ensures that the solution builds upon and contributes to the existing knowledge base of digital signatures, EDRMS, and public-sector ICT frameworks. These cycles guided the design and validation process throughout the project. The process is illustrated in Figure 1, showing how the research bridged practical needs and theoretical foundations through iterative design and contextual evaluation [13].

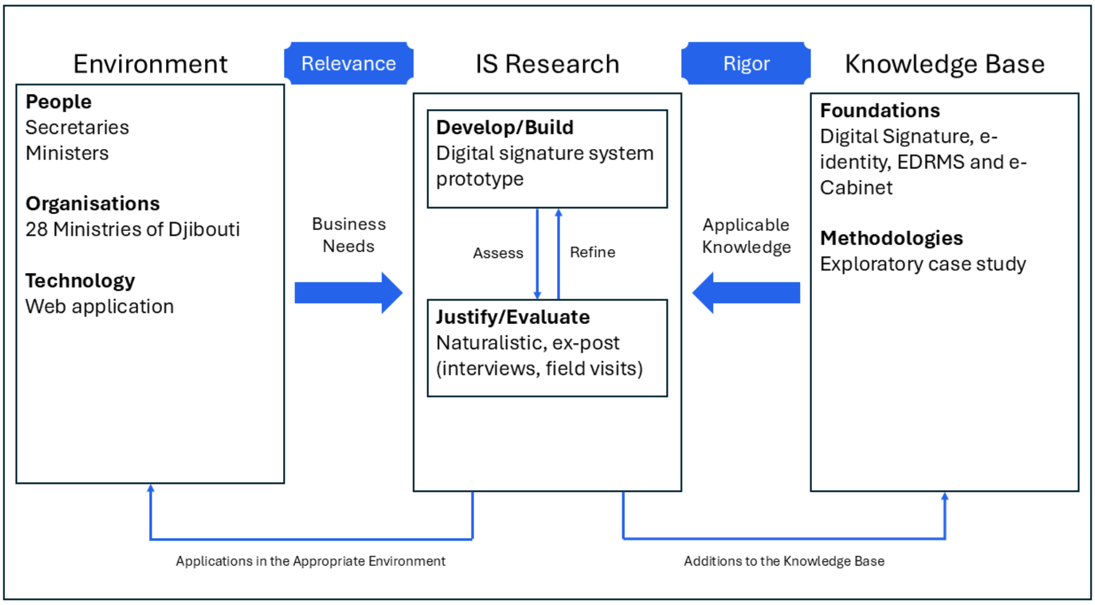


Figure 1. Three-cycle model of this research [8], [13]

In the context of this research, the business needs included the long processing times and lack of transparency in Djibouti’s current inter-ministerial paper-based workflows. Primary stakeholders involved government secretaries and ministers, whose roles in the document approval and signing process shaped the requirements of the system. Technologically, the artefact was designed as a lightweight web application with digital signing and eID functionalities, informed by the eIDAS legal framework and the local institutional landscape. The artefact represents an instantiation, one of the main categories of design science outputs [8], addressing the transition toward more efficient government-to-government (G2G) workflows in a low-digital-maturity setting [13].

The artefact was evaluated through interactive workshops and testing sessions involving stakeholders, including end-users in Djibouti and local technical experts. These sessions allowed participants to interact with the prototype, test its functionality, and provide feedback based on their needs and expectations. Their suggestions were used to make targeted improvements to the system, ensuring that the final version was aligned with actual workflows and user requirements.

The design process also adopted elements of agile development, including iterative prototyping and continuous feedback loops, which mirror the design science research (DSR) build–evaluate cycle [11], [14]. The artefact followed an model-view-controller (MVC) inspired architecture, chosen for its maintainability and suitability for rapid prototyping [18]. These design choices supported a lightweight and adaptable system aligned with the technical and organisational constraints identified during the research process.

1.4.2 Data Collection and Analysis

Data collection was conducted during the first three on-site visits and included interviews with six high-level officials from various ministries and the private sector, as well as document and workflow reviews, with observations documented throughout the process. The interviews were conducted primarily in French with the assistance of an interpreter, and focused on mapping the current situation, assessing trust in digital signatures, and evaluating beliefs about potential efficiency gains. All interviews were recorded, transcribed, and analysed.

Document reviews were carried out to examine existing processes related to document management, inter-ministerial correspondence, and the draft legalisation workflow. Combined with the interview data, these materials provided a detailed picture of the current situation, its bottlenecks, and the overall readiness for digital transformation.

After presenting the artefact, feedback was collected in a workshop format, where participants were able to test the prototype and provide hands-on input regarding usability, functionality, and relevance to their institutional workflows. Their feedback was used to inform further refinements of the solution.

The transcribed interviews were analysed using manual thematic coding, which was chosen due to the small sample size. While software tools like NVivo may offer additional functionality, their cost was not justifiable for a dataset consisting of only six interviews. The coding was guided by the research questions, and the results were compared across responses to identify recurring themes and patterns.

1.4.3 Requirements Engineering

To keep the artefact development both focused and aligned with real-world needs, the FURPS+ and MoSCoW methods were used to categorise and prioritise system requirements. This approach resulted in a scoped artefact aligned with stakeholder needs.

The FURPS+ model, which is widely used in software engineering and requirements analysis, helped categorise the identified requirements into six areas: Functionality, Usability, Reliability, Performance, Supportability, and additional legal or contextual requirements relevant to the public sector. Using this framework provided a clearer overview of what the system needs to achieve and how it must behave in its operating environment [19].

In addition to categorisation, the MoSCoW prioritisation method was applied to distinguish between essential and non-essential requirements. MoSCoW assigns each requirement to one of four levels: Must-have (critical for functionality), Should-have (important but not essential for artefact), Could-have (nice-to-have for future versions), and Won’t-have (excluded from current scope). This prioritisation supported the selection of features for the artefact, while still recognising longer-term goals [19], [20].

1.5 Development Approach

Based on the collected functional requirements, the foundation for the digital signature solution was planned alongside the development process. The system was developed using an agile-inspired approach, with a focus on co-creation and delivering a working solution aligned with the needs of stakeholders in Djibouti [21].

The development process consisted of three phases. First, as described earlier, contextual data was collected, and the situation was analysed. Through interviews and field observations, required features and functional requirements were identified and validated in cooperation with stakeholders.

This was followed by two iterative development cycles, each consisting of planning, implementation, testing, and validation, as illustrated in Figure 2. Given the limited feature set, including only identity management, secure signing, signature validation, and a basic document workflow, two development cycles were considered sufficient. The first cycle focused on translating validated requirements into a functioning prototype. The second cycle addressed stakeholder feedback and included improvements to usability and reliability. Validation sessions were conducted in virtual or on-site workshops, where the artefact was demonstrated and feedback collected. During development, several design decisions were made collaboratively, based on technical constraints, user expectations, and best practices.

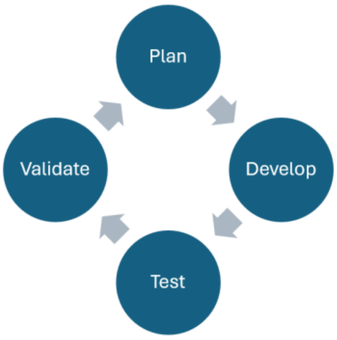


Figure 2. Iterative development cycle

While full-featured frameworks are often used in modern development, a lightweight solution was deliberately chosen for its simplicity, easier setup, lower dependency risk, and better adaptability to local hosting environments. For client-side functionality, two open-source JavaScript libraries were used and one server-side dependency package was included. These were selected for their popularity and community trust, but would require a formal security review before production deployment.

Validation sessions were conducted in virtual or on-site workshops, where the artefact was demonstrated and feedback collected. The feedback from these sessions was systematically documented in a written format to support later analysis and refinement of the prototype.

PHP was used as the server-side scripting language due to its simplicity, popularity, and the author’s prior experience [22]. All business logic and data validation tasks were handled server-side, while privacy-sensitive actions, such as private key generation and digital signing, were carried out in the browser using JavaScript libraries. The server was responsible for secondary validation and storing signed data. For storing the data, MariaDB was selected due to its compatibility with PHP and ease of integration.

The system follows a front controller architecture with an MVC-inspired separation, where the entry point routes requests to a controller [23], [24]. While there is no formal model layer, the business logic is grouped into a shared functions file that handles interactions with the database, as displayed in Figure 3. View templates are used to generate output, maintaining a clear distinction between logic and presentation.

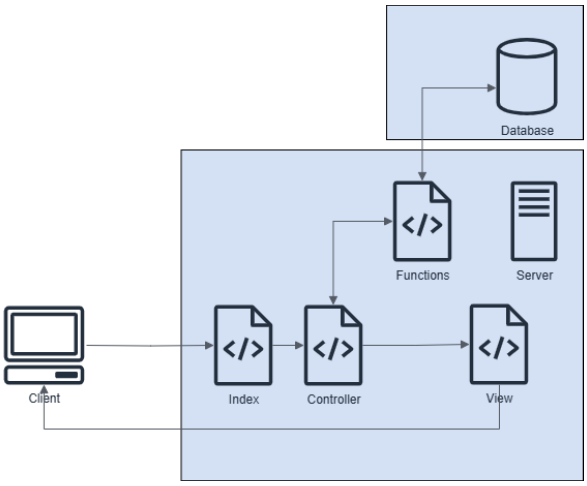


Figure 3. Information system architecture with front controller and MVC-inspired separation

For privacy-sensitive operations, the server sends the required signing libraries to the browser, where operations such as key generation and signing are completed locally. The result is then sent back to the server for verification and storage, as shown in Figure 4.

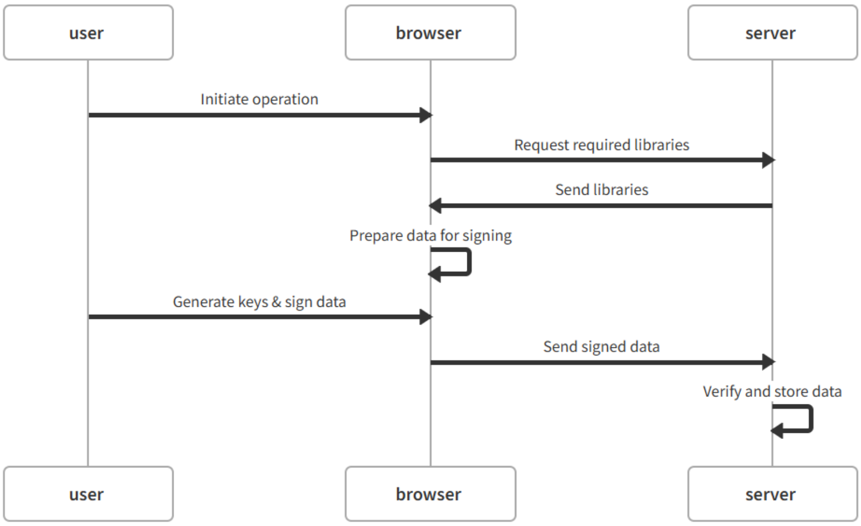


Figure 4. Privacy-Sensitive Operation Flow

During development, the test environment was hosted on a Zone Media virtual server located in the European Union to ensure good data protection, maintain system security, and keep fixed pricing. Zone was selected due to its reliable PHP support and ease of setup compared to other providers.

1.6 Structure of the Thesis

This thesis is structured into six main chapters, each building upon the previous to develop and evaluate a lightweight digital signature solution tailored for Djibouti’s governmental context.

Chapter 1 introduces the broader background of the research, outlining the digital transformation challenges in low e-government maturity settings. It presents the problem statement, research objectives and questions, methodology, development approach, and provides an overview of the thesis structure.

Chapter 2 lays the theoretical and practical foundation for the study. It begins with a literature review on topics such as e-government, EDRMS, e-cabinet systems, digital identity, and digital transformation. It then introduces the key theoretical background and concludes with a review of legal frameworks and technical standards relevant to digital signature systems.

Chapter 3 presents the case context of Djibouti’s ministries and their current level of digitalisation. Based on field observations, stakeholder interviews, and workflow analysis, it outlines the existing processes, main challenges, and derives the functional requirements for a digital signature solution in this context.

Chapter 4 describes the developed prototype system, designed to meet the identified requirements in low-resource settings. It covers the technical architecture, user workflows, security measures, and outlines the validation results gathered through stakeholder feedback.

Chapter 5 discusses the broader findings and contributions of the research. It reflects on the artefact’s practical relevance, the trade-offs made during development, and the conditions necessary for its adoption.

Finally, Chapter 6 concludes the thesis by summarising the key results, outlining legal and organisational preconditions for implementation, and suggesting future improvements to strengthen alignment with long-term digital signature standards.

2 State of the Art

This chapter lays the theoretical and practical foundation for the research, beginning with a literature review on EDRMS, digital identity, and digital signatures, and continuing with relevant theoretical models. In the final section, existing legal frameworks and technical standards relevant to digital signatures are described.

2.1 Literature Review

E-governance has been a focus for decades. As early as 1995, the G7 nations and the European Commission met in Brussels and launched eleven projects aimed at developing the information society. One of these, "Government Online," aimed to digitalise public services. Since then, electronic governance has rapidly gained popularity as a smart and efficient way to manage state functions [25].

Digitalisation in the public sector is increasingly seen as a way to improve how governments deliver services. By using information and communication technologies, public administrations can make processes faster, more transparent, and easier to access. This approach helps increase efficiency, reduce paperwork, and improve accountability, making government operations more responsive and citizen-friendly [26], [27], [28], [29], [30].

2.1.1 E-Government

E-government is a popular topic with many definitions; however, its main goal remains improving efficiency and offering better services to citizens [31]. It is often described as the effective use of information and communication technologies [32], [33], with particular attention to areas like e-parliament, which bring benefits such as increased transparency, accessibility, and accountability [32]. While e-government focuses more on external interactions (government to citizens, businesses, or other governments), e-governance is broader, encompassing internal management and political participation as well [34].

E-government is also recommended as an anti-corruption tool [35]; however, for it to function successfully, the existing governmental structures must already operate relatively well [36].

Alongside technology adoption, effective information governance remains crucial. This involves implementing systems and procedures that safeguard public information, supporting the effectiveness and knowledge preservation that are vital for successful e-governance [37], [38].

The European Union (EU) has estimated potential savings of 50 billion euros through the shift towards e-administration, while Denmark’s move to electronic billing for taxpayers was expected to save 200 million euros annually [25].

To understand global progress, the United Nations conducts a bi-yearly e-Government Survey, initiated in 2001, assessing all UN member states using indicators such as the E-Government Development Index (EGDI) and the Online Service Index (OSI). While Europe remains the global leader, Africa is steadily showing progress [39].

There are many stakeholders involved in e-government development [31], [40], [41], making consensus-building around upgrades more difficult. Additionally, challenges often arise related to legal frameworks, funding, and infrastructure [36]. Successful transitions to e-government require not only political will and resource availability but also strong legal frameworks, citizen awareness, and reliable digital identity systems [33].

Implementation of an EDRMS is a strong beginning toward building e-government [42].

2.1.2 Electronic Document and Records Management Systems

EDRMSs are not new and are nowadays widely available, as the amount of digital information has grown significantly. However, managing it properly still requires thoughtful planning [37]. Already in 2005, the United States required their companies, and those having trading arrangements with the U.S., to implement records management systems [43], [44]. In Estonia, EDRMS has been made mandatory for all public sector agencies [36]. Although initially perceived as a bureaucratic requirement, their benefits as a foundation for improving organisational efficiency have been acknowledged, as demonstrated by a study conducted in Switzerland [43]. EDRMS has been recognised as the most popular service in e-government initiatives and the most effective enterprisewide solution within the public sector [45], [46], [47]. Many countries embarking on their digitalisation journeys choose to start with EDRMS implementation, as it brings the most immediate impact on intergovernmental processes [36], [48], [49].

EDRMS evolved from Records Management Systems (RMS) and Document Management Systems (DMS) in the 1990s. RMS primarily stored information about document locations, while DMS stored only the document files themselves. EDRMS combined both functionalities, enhancing overall efficiency [50]. While early systems were monolithic, modern solutions are more advanced, offering integration with office applications and support for the entire document lifecycle.

The main goal of EDRMS is to structure captured information from both electronic and paper formats. ISO 15489 defines the essence of a records system as the capturing, managing, and providing access to records [50], supporting effective and economically efficient management [51], [52]. In the public sector, EDRMSs also serve to improve document reliability and authenticity, as they support structured document workflows [36], [37]. A 2006 study revealed that disorganised email management by nine employees resulted in a loss of 1.3 billion pounds weekly for companies in the United Kingdom [50].

There are five types of related systems: Electronic Document and Records Management (EDRM), Electronic Document Management (EDM), Electronic Records Management (ERM), Enterprise Content Management (ECM), and Enterprise Knowledge Management (EKM), distinguished by the nature and storage of information [37].

Janne Yläjääski identified seven basic and nine supporting functions common to EDRMS. Basic functions include document manipulation, document archiving, search functionality, user rights management, virtual folders, version management, and change management. Supporting functions include viewing and printing documents, establishing relations or comparisons, document numbering, integrating external applications, workflow management, multilingual interfaces, and red-lining for inspection and correction purposes. These are considered essential for a functional EDRMS. Modern, higher-end systems also offer integration with email services, document scanners, and text editors [50].

According to Nguyen et al., a major advantage of EDRMS is the significantly lower risk of data loss. Numerous cases have shown organisations losing all their documents to fires, whereas electronic documents, if structured properly, offer far better resilience [43].

In Estonia, the move towards digital EDRMS was supported by making their use mandatory for local governments and developing specific solutions for them between 2009 and 2011. By the end of that period, at least 85% of local governments, as well as all ministries and their subdivisions, were using EDRMS. To facilitate this transformation, the e-LocGov model was developed to help local governments better manage their processes and workflows. During this period, Estonia's digital identification infrastructure was already operational, enabling secure identification of government officials in electronic environments [36]. Although the need for EDRMS was not fully understood initially, its value, especially the reduced time spent searching for documents, is now recognised, and the Estonian approach has been praised in a European context [37], [53].

At least seven EDRMS solutions are in full or partial use in Estonia today: Delta, Amphora, Alfresco, WebDesktop, FolderIt, DocLogix, and Postipoiss [54].

When implementing an EDRMS, it is important to consider that data may be distributed across multiple locations, and not all documents should be accessible to everyone. Different levels of access are required for personal, team, organisational, and external stakeholder documents. Furthermore, the system's cost and the organisation's willingness to embrace change are often underestimated [53].

A defining characteristic separating EDRMS from simpler systems is the use of metadata. Metadata is crucial for searchability and auditing purposes, as simply storing documents without contextual information is insufficient [53]. Typically, a classification scheme is employed to categorise documents or records based on functions and series [55].

Finally, in Estonia and other European countries, the archiving of data plays an important role. Although the need to access certain documents diminishes over time, legal requirements often mandate that they be retained for a specific period. During this archival period, documents become view-only, with editing rights restricted to specific user groups. Once the retention period ends, documents may be permanently deleted unless they have archival value, in which case they are transferred digitally to national archives. The best EDRMS systems support this integration [56].

2.1.3 E-Cabinet Systems

One step more specific than EDRMS is the e-cabinet system, which improves the efficiency and speed of digital document exchange. In Estonian context, one of many developments in the beginning of digital transformation journey was e-cabinet system [57] that was launched in 2000. While EDRMS is broader, the first e-cabinet system in Estonia, VIIS (republic's government's session information system), was only meant for preparing the sessions, agendas and memos. Implementation of that system included training workshops for the ministers, one stakeholder group for that system. While before the system, 17 000 pages of paper was printed out weekly, the system replaced most of that [58], [59].

While in the beginning there was no digital signing, and approvals and rejections were simply done by button click, the growing need for stronger authentication led to the development and integration of digital identity solutions as they evolved. Nowadays, technologies including ID-card, Mobile-ID, and Smart-ID allow secure authentication and digital signing, making fully paperless workflows possible. It should no longer be necessary to print out a document, sign it by hand, and scan it back again [57].

2.1.4 Digital Identity

Digital identity and its management systems are essential components of any e-governance ecosystem. They enable the secure display of personal information and ensure that communications and service requests genuinely originate from the individuals or officials they claim to represent. Electronic identification and authentication form the foundation for both intra-governmental workflows and citizen-facing services [60], [61].

Electronic or digital identity allows users to prove their identity in e-services in much the same way passports or identity cards function in the physical world. It is a key element for building an efficient country and municipality, allowing easy identification without the need for physical offices and long queues. Moreover, the introduction of electronic signatures further boosts efficiency by enabling the implementation of fully digital workflows [25], [62], [63].

Globally, there is no unified standard for electronic identification – not even across the United States [61]. Different countries have developed their own solutions based on their needs. In Canada, the Directive on Identity Management defines identity handling requirements for federal departments. Japan’s DS-500 Guidelines focus on risk-based online identity verification for administrative procedures, with new standards under development to address emerging digital needs. The United Kingdom’s efforts are centred around the GOV.UK One Login service and a broader framework to ensure secure, inclusive digital identities across the economy. Meanwhile, in the United States, National Institute of Standards and Technology’s Digital Identity Guidelines (SP-800-63-3) provide best practices for identity proofing, authentication, and federation, with a new revision expected to better address accessibility needs and technologies such as mobile wallets and verifiable credentials [62]. Research on implementing digital identity and signature solutions for e-cabinet systems in low-maturity e-government contexts remains limited [13].

In EU, Regulation (EU) No 910/2014 (eIDAS) created a trusted framework for electronic identification and trust services across member states, requiring mutual recognition of national electronic identities [64]. This regulation also set common standards for electronic signatures, seals, and timestamps, enabling secure cross-border digital transactions. In 2024, Regulation (EU) 2024/1183 updated eIDAS by introducing the European Digital Identity Wallets, aiming for full rollout by 2026–2027 to further enhance interoperability and user trust [62].

Within authentication frameworks, three levels of identity assurance have been specified: low, substantial, and high. Similarly, levels for digital signatures exist and are discussed in later chapters [64].

Estonia is considered highly advanced in digital identity, having implemented a PKI-based identity system over twenty years ago and requiring public authorities to accept digital signatures. By 2019, 98% of the population had an ID-card equipped with an electronic identity token. Over 500 million digital signatures have been created using ID-card, Mobile-ID, or Smart-ID services. Earlier stages of development included the use of PIN-calculators and Bank-ID for authentication [57], [60], [65], [66].

Digital identity is designed to solve many problems of the paper-based world by providing a gateway to digital services. Electronic signatures, which can be legally equated to handwritten signatures in some cases, bring additional benefits [25], [39]. Unlike physically signed documents, digitally signed documents can be copied endlessly without losing their authenticity, require no paper or printing, and eliminate the need for physical delivery. Digital signatures are tamper-proof, offering an important advantage over traditional signatures [57].

Recognising the importance of electronic authentication and digital signatures, Estonia treats these services as part of its state-critical infrastructure. Elsewhere, similar benefits have been observed; in Germany, it was reported that companies could save up to 100 USD per document by switching to digital signatures [30], [61], [67].

However, with the use of digital identities and signatures, considerations for archival and long-term accessibility become critical. While software platforms typically have a lifecycle of about five years, every new generation must still maintain support for older systems.

Finally, advancing computing power, tenfolding every decade, and the emergence of quantum computing raise new challenges. Traditional cryptographic algorithms such as RSA and DHKE are already becoming vulnerable [68], [69], [70].

2.1.5 Transparency and Accountability

With the rise of e-government services, digital transparency tends to increase, although achieving it remains a challenge [71]. Citizens can now be more directly included in decision-making processes, and smaller services are no longer concentrated under the authority of a single official. These developments contribute to increasing citizen trust in public officials, which is critical in a time when many governments face declining public trust. Trust remains one of the foundational pillars of a functioning democracy [36], [57], [72], [73].

For e-services such as EDRMS, digital identity, and electronic signatures to succeed, trust is both a prerequisite and a goal. Transparency, usability, security, and verifiability are key factors influencing trust in digital services [35], [72], [73]. Once operational and reliable, these services further enhance public trust in government institutions.

Corruption, while appearing beneficial to participants, ultimately damages governmental credibility. Surveys show that nearly half of citizens believe that high-level officials may exchange political favours for lucrative private sector positions [35], [74], [75]. Transparency is recognised as a critical mechanism for reducing such opportunities and rebuilding public trust.

Corruption is often more prevalent in services controlled by a small number of officials, where new problems can be artificially created to solicit bribes. The introduction of e-government services reduces these risks by making processes more transparent and activities more easily traceable, both in theory and in practice [26], [35], [66].

In parallel with transparency, respecting citizens’ privacy is essential. Strong privacy protections enhance trust in digital services, whereas incidents of data breaches or misuse can significantly damage public confidence [76].

2.1.6 Digital Transformation

At the end of traditional workflows and the beginning of the new era, transformation towards digital processes must not be done hastily, but carefully prepared and planned. While most attention is typically directed towards technology, ultimate success depends on whether officials begin to adopt and effectively use the upgraded methods. An information system can be as advanced as possible, yet if no one knows how or wants to use it, the transformation will fail, often causing reputation damage. It is noted that EDRMS implementation projects typically require at least four years to reach broad adoption [36], [45], [47], [68].

Before development or contracting begins, it is crucial to fully understand the processes, user needs, and required functionalities, prioritising them realistically according to available financial resources and project timelines. However, organisations at any technology maturity level can implement digital systems; for example, in digital procurement, returns on investment can be seen within weeks rather than years. Even after implementation, processes must be regularly analysed to identify inefficiencies and eliminate unnecessary tasks [77], [78], [79], [80].

Beyond the system upgrade itself, a mindset and organisational culture shift is necessary. Common reasons for transformation failures include lack of IT literacy, poor e-readiness, weak IT infrastructure, insufficient management support, inadequate training, missing IT policies, and a rigid culture resistant to change [32], [51], [81], [82].

It is important to recognise that when digital environments are introduced for the first time, human error remains a major vulnerability; a lack of IT literacy can lead to cybersecurity incidents or misuse of information systems. Therefore, the quality of the digital experience and careful planning are critical [83], [84].

Finally, before any new system, especially those involving digital identity or digital signatures replacing handwritten signatures, is adopted, the legal framework must be adjusted accordingly. Legal permission is essential for fully recognising digital decisions and ensuring successful transformation [33].

Taken together, these elements form the critical backbone for any meaningful digital transformation, where legal readiness, technological robustness, and human capacity must evolve in unison to ensure secure, efficient, and trusted digital governance.

2.2 Theoretical Background

Technology adoption is analysed exhaustively, and there are several theories and models as the understanding why users embrace some changes and others not. Most common are Theory of Planned Behaviour and Theory of Reasoned Action. Also, there are the Technology Acceptance Model (TAM), the Unified Theory of Acceptance and Use of Technology, and the Diffusion of Innovation. TAM has emerged as the most influential [45], [68], [85], [86].

Technology adoption studies often refer to the Theory of Planned Behaviour, where the important aspects are training, perceived usefulness, perceived ease of use, and compatibility. Yet the more popular one is the TAM, published in 1986, an adaptation of the Theory of Reasoned Action [47].

TAM's goal is to explain computer acceptance and user behaviour, and to provide a basis for tracing the impact of external factors on internal beliefs, attitudes, and intentions. It defines two key beliefs: perceived usefulness and perceived ease of use. Perceived usefulness is meant as the user's understanding that using the system will make tasks easier and improve performance, while perceived ease of use draws attention to the user's expectation that the system will be simple and not problematic [68].

TAM is used because of its clarity, ease for applying, and validated approach, giving not only the facts but also the background and context to help addressing the problems easier [85].

2.3 Standardisation and Requirements

When considering electronic identity and signatures in the European context, many technical and procedural requirements are established to ensure a standardised approach with minimal vulnerabilities. The eIDAS and Single Digital Gateway regulations are two of the key frameworks within the EU's Trust and Safety section, directly applicable in all EU member states, and holding higher priority over national regulations. eIDAS and its concept of qualified services form the foundation for current electronic signature practices. In Estonia, additional national regulations also apply separately [36], [87], [88].

There is a separate category for trust services related to electronic identity and its management. In the EU, trust services include the management and issuance of personal certificates, timestamp services, creation, verification and storage of electronic signatures, electronic data exchange services, and issuance of web server certificates [64].

2.3.1 Levels of Assurance

eIDAS defines levels of assurance (LOAs) for electronic authentication to grade the trustworthiness of different authentication methods. Authentication levels are determined by several factors, with the most notable being the enrolment process (how the identity is issued to the user), the system setup, the login methods enabled, and how authentication is performed. Three levels are defined: low, substantial, and high. While a range of levels is used in many countries, all Estonian authentication methods operate at the high level [62], [64], [89], [90], [91].

The low level of assurance is relatively easy to achieve, as self-registration and verification through email and password are acceptable. This provides weak identification, where the user is not properly verified, but if the provided information appears credible, it is assumed that the same person continues to use the account [89], [90], [91].

The substantial level adds stronger assurances. An identity check must be performed during enrolment, and multi-factor authentication is required. At this level, identity can be confirmed with a reasonable degree of trust, as authentication would not succeed without the user's active participation [89], [90], [91].

The high level introduces even stricter requirements. Enrolment must include a comprehensive identity verification, and authentication must be performed using a smartcard or another method fully controlled by the user. The cryptographic material must be securely stored and remain inaccessible to third parties [89], [90], [91].

2.3.2 Digital Signatures

In case authentication is not enough, digital signatures are used to link the identity of the signer with the document through a separate file container. Once the document is signed, any further modifications can be detected. According to the eIDAS regulation, applicable across all EU member states, electronic signatures are legal and have evidential value, even if they are not classified as qualified electronic signatures [66], [88].

eIDAS defines an electronic signature as “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” [92].

There are three levels of electronic signatures legally recognised across the European Union; however, only the highest level is equated to handwritten signatures and is therefore mostly used in governmental processes. Member states are allowed to accept lower-level signatures if the value or importance of the signature is not high [64], [93].

PKI is the system used to manage digital certificates and cryptographic keys to support electronic signatures. PKI ensures that signatures can be trusted by verifying the signer’s identity and protecting the data from tampering. In environments without existing PKI, implementing higher level signatures becomes more complicated, as the core trust services are missing and need to be set up or replaced with alternative solutions.

The highest level of trust is provided by a qualified electronic signature (QES), which must be supported by a qualified certificate. The signature must be created using a secure signature creation device (SSCD) that ensures the signature creation data is safely stored, cannot be forged, and creates unique signatures. The signature creation data must remain within the device and must not be shared externally [88].

The second level is the advanced electronic signature (AdES), which can optionally be strengthened by a qualified certificate (AdES/QC). In AdES/QC, the signature creation data may be stored externally, such as on the user's computer, although storing it in a chip-based device is also possible. [94] For regular AdES, requirements include the signature's relation solely to the signer, inclusion of the signer’s identification data, detectability of any manipulation, and secure storage of the signature creation data [64].

The third level covers other electronic signatures that do not meet the requirements for AdES or QES, including basic PDF signing solutions or hand-drawn signatures stored as images. While these are considered electronic signatures, their legal strength is lower [64], [94].

While QES provides the highest legal assurance, in many cases AdES or even basic electronic signature is legally sufficient, depending on the regulatory and business requirements.

Signatures must be always verifiable. In Estonia, the software DigiDoc validates signed containers, checks the signature certificates and their level, and performs additional verifications. In Estonia, the ASiC-E file format is used for signed containers [64].

3 Foundations and Requirements for Digital Transformation

This chapter provides an overview of the digitalisation level in Djibouti's ministries and outlines the need for a digital signature solution. It describes the current workflows, key problems, and expected improvements. The content is based on field observations, stakeholder interviews, and analysis of existing procedures. The chapter also identifies the main challenges affecting implementation and presents the system requirements. Finally, it discusses the importance of training, user readiness, and management support for successful adoption.

3.1 Current State of Digital Capacity in Djibouti

To understand the challenges better, it is useful to first look at the current level of digitalisation in Djibouti. From its perspective, there is significant room for advancement. The United Nations (UN) ranks Djibouti in the lower half of countries in its e-Government Survey. In the Local Online Service Index (LOSI), Djibouti is placed 152nd, and in the EGDI, 174th, out of 193 UN member states [39], [95].

It is estimated that approximately every second person has access to either a mobile phone or a fixed line. Djibouti Telecom holds a monopoly over telecom services, which usually leads to relatively high prices. Nevertheless, improvements have been made, such as the introduction of D-Money, a mobile payment service [2], [96].

Based on Layne and Lee's e-Government maturity model, which includes the stages of cataloguing, transaction, vertical integration, and horizontal integration, Djibouti would currently be placed at the second phase. Over 40 services have been catalogued, and information is provided via the website egouv.dj, but in most cases, it only offers information rather than fully functional e-services [97], [98], [99].

An exception to this is the country's online e-visa system, which supports online payments and simplifies the process of entering Djibouti, although the English localisation of the service has some deficiencies [100].

Djibouti has made steady efforts to develop its Digital Code regulations over the past several years, although these have not yet been officially adopted as law. At the same time, new digitalisation projects have been launched with international support. The International Telecommunication Union (ITU), a United Nations agency, has been involved in several initiatives aimed at expanding the country's e-services. These include the development of an online construction permit system for Djibouti City and an e-cabinet system intended for use by government ministries. The objective of the e-cabinet project was to establish digital workflows for correspondence across all 28 ministries [101], [102], [103], [104], [105].

3.2 AS-IS Governmental Processes

As part of the ITU and GovStack initiative, field visits were carried out to support the implementation of the e-cabinet system. The initiative was initially planned to begin with a pilot phase focused on digitalising correspondence processes within three ministries. Although referred to as *correspondence*, these should more accurately be categorised as cross-organisational workflow management or inter-agency data exchange processes.

At the time of the fieldwork, all such workflows were still paper-based. The existing process involved receiving documents from a courier, registering them in the internal registry, and in some cases scanning them for easier handling. The document would then be forwarded to the minister, who decided whether a response was necessary and which senior employee would be responsible. Documents intended for higher-level staff were always routed through their secretaries.

Once a response letter was drafted by the assigned official, the document was sent back to the minister through the same hierarchical path, for review, approval, and handwritten signature. The signed letter was then physically returned to the originating institution using a courier.

It is important to note that the employees responsible for drafting response letters are often located in different buildings or even ministries. This means documents must be physically transported across organisations. According to interviewees, this delivery process can take multiple days and, in some cases, documents are lost in transit. One interviewee mentioned that sometimes she had to call another ministry to confirm whether a document had been received and to ask for its status. Although incidents of corruption or tampering were not directly mentioned, the possibility of intentional document loss or manipulation cannot be ruled out.

Computers are used in most offices, primarily for drafting text and unofficial internal communication. However, all official documents are still printed, physically signed, and stored in physical archives when necessary.

As part of the project, the Estonian EDRMS WebDesktop was selected during the procurement process to support Djibouti’s document management needs. The planned digitalised procedure would involve scanning the document upon receipt, after which all tasks would proceed in digital form using semi-automated workflows. As in Estonia, it was expected that not all documents would require digital signatures; in some cases, simple approval or rejection through action buttons would suffice.

Field observations and interviews confirmed a strong need for digital signature capability. Most respondents agreed that a *substantial* level of authentication would be sufficient for internal correspondence and response letters. Based on these insights, the implementation of a digital signature solution offering substantial-level authentication appears to be well-aligned with local needs and expectations.

3.3 Insights from Interviews

The interviews carried out with stakeholders of the EDRMS system revealed strong enthusiasm for its implementation and a general readiness for digital transformation. As described in Table 1, all interviewees stated that the implementation of EDRMS would be beneficial both for their individual work and for the government as a whole.

Expectations for efficiency gains ranged from 50% to 90%. Most participants were confident that processes could become nearly twice as fast, primarily due to the elimination of delays caused by traditional postal deliveries. While nearly all ministries currently rely on paper-based workflows, a few have started using partial digital processes, which may explain their slightly lower estimated improvements.

Regarding correspondence workflows, most interviewees considered a substantial level of authentication sufficient for digital signatures. One respondent suggested that a high assurance level might be required, while another preferred a simpler approach. The differing opinions on expected efficiency gains appear to be linked to the interviewees' familiarity with digital technologies. While a 60–70% improvement seems feasible, doubling the speed would likely require substantial changes to organisational culture and internal procedures. Notably, all participants emphasised the need for legal regulation before digital signatures can be officially adopted.

Table 1. Stakeholder beliefs on EDRMS benefits, efficiency gains, and assurance levels

Interviewee	**Believing in EDRMS**	**Efficiency gain**	**Paper use**	**Required LOA**
A	Yes	70%	100%	Substantial
B	Yes	70%	100%	Substantial
C	Yes	50%	90%	Substantial
D	Yes	70%	100%	Substantial
E	Yes	90%	100%	High
F	Yes	75%	100%	Low/Substantial

When asked about the use of AI in the EDRMS for routine tasks, opinions were mixed. One interviewee expressed optimism, while others voiced concerns related to data privacy and the lack of transparency in AI decision-making. Interestingly, the more technically knowledgeable respondents appeared more cautious about adopting AI, suggesting a direct correlation between digital literacy and scepticism.

Perceptions of implementation speed varied, seemingly based on age and experience in the public sector. Younger or less tenured officials believed EDRMS could be implemented within a few months. In contrast, more experienced staff estimated a timeframe of 6 to 12 months, with some recommending a phased approach, starting with a pilot project before rolling it out across all ministries. The summarised expectations are shown in Figure 5.

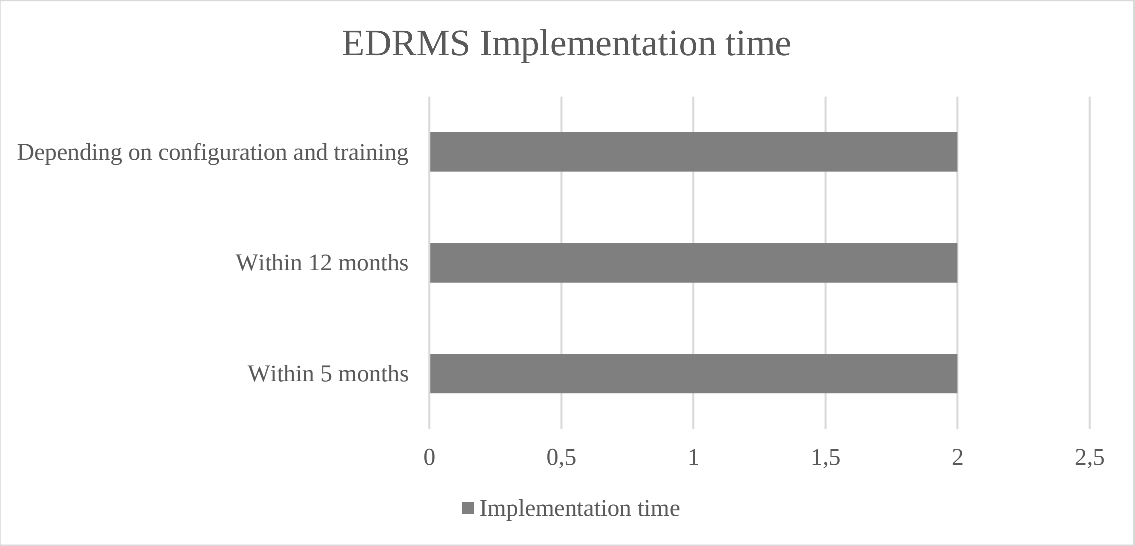


Figure 5. Estimated implementation timeframes for EDRMS adoption

To better assess the effectiveness of EDRMS, the following key performance indicators (KPIs) were suggested and are grouped into operational, performance, process quality, and user engagement categories for clarity, as shown in Table 2.

Table 2. Suggested KPIs for measuring EDRMS efficiency

Group	**KPI description**	**Purpose**
Operational	Volume of daily email or correspondence	Monitor overall communication activity
Performance	Response time between ministries	Measure inter-ministerial communication speed
	Response time to citizen requests	Assess external service responsiveness
	Document processing duration	Benchmark internal process efficiency
Process quality	Confirmation rate (sent vs received)	Audit reliability of message delivery
	Frequency of lost documents	Identify transparency and accountability gaps
User engagement	System usage frequency per user or ministry	Monitor adoption and active usage
	Time required for user onboarding	Assess training needs and support effort

In conclusion, the interviews confirmed a strong optimism toward the implementation of EDRMS, with a shared belief in its potential to significantly increase administrative efficiency. Additionally, most interviewees agreed that for correspondence workflows, a substantial level of assurance would be sufficient for digital signature authentication.

The full list of interview questions is provided in Annex 2 for reference.

3.4 Challenges in Digitalisation

Based on the interviews, observations, and field insights, eight main challenges can be identified that will affect the implementation of the WebDesktop system. Without addressing these challenges, the implementation is unlikely to succeed, even though the system can technically be configured with the correct privacy permissions, document categorisation, and workflows.

Lack of legal framework

The first and most critical challenge is the absence of a legal framework to support digital transformation. Although the Digital Code is under development, it has not yet been approved or enforced. Until that happens, no electronic identity method can be legally binding. As understood from observations, many documents require official signatures, and in such cases, a full digital process is not possible. The documents must still be printed and signed manually.

Lack of foundational systems

While birth, marriage, and death registrations are formally required, they are not centralised. This means there is no complete national overview, and in Estonian terms, no functioning population registry [106]. Without both the legal base and a population register, it is difficult to build a functioning public key infrastructure (PKI), which is necessary for issuing digital identities and enabling secure signatures.

No means for digital signatures

As there is no electronic identity system available, there is also no way to create digital signatures. While WebDesktop is suitable as an EDRMS, it cannot serve as an identity provider. If a national eID and digital signature system were introduced, it would likely be managed separately, and integrating it with WebDesktop through Application Programming Interfaces (API) would require extra development and time.

Digital literacy

Digital literacy is another issue. Even in Estonia, not every person fully understands basic computer usage. For example, not everyone knows how to use a navigation bar or navigate efficiently online. Considering Djibouti's lower literacy rate, it is essential that officials who will use the system also understand basic digital processes, logic, and internet-related risks.

Trust gap

The gap in trust can be partially attributed to the challenges discussed above, as ministries are generally cautious about adopting digital systems. Ministries are expected to be cautious about digital systems. While they may not be fully familiar with digital tools, they do understand the importance of document integrity and signatures, meaning their concerns about tampering or misuse are valid. This challenge can only be addressed through proper training and gradual familiarisation.

Infrastructure instability

There are occasional power outages and internet problems. In a fully digital environment, this can bring work to a stop, either because the office has no electricity, the server is unreachable, or the connection is down. While this is not a daily issue, it must still be considered during planning.

Paper-based mindset

A further challenge is the prevailing mindset: many officials have worked their entire careers using paper, and imagining digital alternatives is difficult. Two specific issues come from this. First, existing processes are often unoptimised, and when digitalised, they are simply copied into a digital format without improvement. Second, there is a very hierarchical structure: secretaries cannot send documents outside the ministry, only ministers can. In standard cases, this causes unnecessary delays and offers only a small gain in control. As this represents a major shift in working culture, it will not be easy to change.

3.5 Functional Requirements for Digital Signature Solution

As discovered and discussed previously in chapter 3.3, although the EDRMS system could technically be implemented, it would not be used in practice due to the lack of digital signing capability. To solve this issue, the goal of this thesis was to develop a lightweight solution that enables rapid implementation until a full-scale PKI can be established.

Based on interviews and observations, the digital signature solution should include identity management, secure signing, signature validation and basic document workflows in order to allow ministers to sign without needing multiple systems. In terms of authentication, based on interview results described in chapter 3.3, eIDAS *substantial* level is considered sufficient, and for signature containers, the solution should follow the requirements of AdES. While eIDAS provides a widely accepted best practice framework, this thesis adopts only its general principles. A full technical and legal implementation analysis falls outside the scope of this research project, which focuses on developing and evaluating a lightweight solution suitable for rapid deployment.

Functional and non-functional requirements have been defined based on the identified features. These are categorised using the FURPS+ model and prioritised using the MoSCoW method. A total of 44 requirements were identified and are presented in the following tables, grouped by FURPS+. As this is a master’s thesis, only general-level requirements are presented; detailed technical specifications, especially those relating to full eIDAS compliance, are left for future work. Lower-priority requirements (below *Must* in MoSCoW) are also excluded from the implementation scope but are documented here for completeness.

In Table 3, 14 functionality requirements are defined and assigned a priority. Only two advanced functionality requirements are included, both marked as *Should have*, meaning they are considered valuable but will not be developed within this thesis.

Table 3. Functionality requirements

Requirement	**MoSCoW priority**
User authentication with username, password and one-time PIN	Must have
Role and ministry (or unit) based access (signing or initiating or viewing)	Must have
Documents remain visible only for initiator or signer or inside the ministry	Must have
Secure key generation using OpenPGP JavaScript library	Must have
Public key storage on server, private key kept by user	Must have
Ability to revoke and regenerate signing keys	Must have
Digital signing of documents in browser with private key	Must have
Sequential signing workflow for signatures	Must have
Parallel signing workflow for signatures	Could have
Email notifications related to new documents waiting for signing or completed or revoked workflow	Should have
EDRMS document id included in signing system	Must have
Validation of signatures before completing the signing process	Must have
All document types can be included in signable container	Must have
Container validation accessible for everyone who has the container file	Must have

Table 4 continues the requirements by introducing usability-specific criteria. These are important for ensuring a positive user experience and are directly aligned with the TAM, which emphasises the role of perceived ease of use in adoption.

Table 4. Usability requirements

Requirement	**MoSCoW priority**
User-friendly interface	Must have
Mobile-friendly interface	Must have
Simple and straightforward UX	Must have
Clear error messages and guidance for users	Must have
Low text mode or icon based support	Could have

Table 5 appends technical requirements for reliability and system uptime. These ensure that the system remains stable and operational under expected usage conditions, even in environments with infrastructural limitations.

Table 5. Reliability requirements

Requirement	**MoSCoW priority**
Audit logs for all signing actions	Must have
Regular backups of public keys, signed containers meta-data	Must have
System yearly uptime minimum 99% (allowing daily 14 minutes downtime)	Must have

Once reliability is ensured, performance becomes equally critical. Table 6 outlines requirements that help the system remain responsive and efficient, particularly in scenarios involving higher user loads or broader institutional adoption.

Table 6. Performance requirements

Requirement	**MoSCoW priority**
Signing should be processed in under 5 seconds	Must have
150 concurrent signing operations without performance degradation	Should have
System should be scalable to support large-scale signing operations	Could have

Table 7 points out the supportability requirements. Although some of them are external to the system itself, they remain important for maintaining usability and user satisfaction over time.

Table 7. Supportability requirements

Requirement	**MoSCoW priority**
Error handling with detailed logging	Must have
Helpdesk support	Should have
Multi-language support	Could have
Admin panel tools for easier maintenance	Could have

As the last category, Table 8 includes additional requirements that were not categorised earlier. In order to keep the system safe and secure, 13 security-related requirements are defined.

Table 8. Additional requirements: Security

Requirement	**MoSCoW priority**
All communication only over HTTPS	Must have
Use of HTTP-only and Secure cookies	Must have
Consists of open-source frameworks where possible	Must have
Clear and enforced processes for user validation when creating the accounts	Must have
Rate limiting on login and key operations	Should have
Support for additional authentication means	Could have
Encryption for private keys	Must have
Timestamping of digital signatures	Should have
Support for external signature verification tools	Should have
Automatic email alerts for failed login attempts	Should have
Automatic logout after inactivity	Must have
No user private key should be stored on the server-side	Must have
Regular security audits	Should have

Finally, legal requirements are defined in Table 9. These ensure that the system complies with regulatory expectations and that digitally signed documents carry legal validity.

Table 9. Additional requirements: Legal

Requirement	**MoSCoW priority**
Legal framework for digital signatures in the country (not a technical system requirement, but essential for legal recognition)	Must have
Audit logs should be tamper-proof	Could have

3.6 Implementation Challenges

Although structural and technical barriers have been addressed above, organisational and human factors remain equally critical to the successful implementation of the information system.

According to the TAM, successful adoption of a new system depends on how users perceive its usefulness and ease of use. These perceptions shape their attitude toward the system and ultimately their willingness to use it. Even if the technical solution functions as intended, user resistance or lack of understanding can result in project failure.

As stated earlier, even a well-designed information system cannot solve problems in isolation and requires active cooperation and acceptance from users. Support from higher management is particularly important.

Throughout the full implementation process, management must remain proactive and visibly supportive. This includes understanding the system’s role, adhering to timelines and commitments, and maintaining consistent messaging. Limited situation awareness, contradicting decisions or even slightly neutral attitude will be quickly picked up by the staff, increasing the chance for project’s failure significantly.

Capacity building is also essential. While officials are fluent in paper-based workflows, many, including ministers, may lack practical skills in using computers, web browsers, or maintaining device security. Training programs must therefore be designed not only to introduce system features, but also to build basic digital competence and trust in the new workflow, following examples such as the early training provided in Estonia [59].

Training must be tailored to the specific roles and responsibilities of different user groups. While general sessions on digital workflows and cybersecurity would benefit all staff, more targeted instruction is also necessary. For ministers, high-level briefings should clarify the principles of secure digital signing, including the creation and safe storage of private keys. For secretaries, practical training is needed on how to initiate signing workflows and link documents between the EDRMS and the signing platform.

Overall, the success of the information system depends not only on its technical implementation, but also on user empowerment, training, and sustained support for adoption.

4 Digital Signature Solution Prototype

This chapter presents the developed artefact – a lightweight digital signature system designed to operate in low-resource, transitional environments. Built using open-source tools and aligned with stakeholder requirements, the system offers a secure and production-ready solution for creating digital identities and handling signing workflows. The chapter covers its key features, technical design, security architecture, integration approach, and validation results gathered through stakeholder workshops.

4.1 Overview

To address the identified problem, a design science artefact was developed for a digital signature solution in terms of core functionality and security features, but not audited or deployed in production at the time of writing. This information system is intended to provide a temporary, secure electronic identity mechanism for government officials during the transition period before a full-scale national PKI is implemented and enforced. The system is designed to be easy to set up, simple to use, and deployable in resource-constrained environments.

The digital signature solution is not currently integrated with existing EDRMS, primarily due to concerns that the authentication mechanisms in those systems may not meet the assurance level required for secure digital signing. However, the system is designed to operate alongside EDRMS, with each document entered into the digital signature platform optionally including an EDRMS document ID to facilitate cross-system traceability and search.

The system uses one server-side dependency and two client-side libraries. On the server side, the Dompdf 3.1 library is used for generating PDF documents during the creation of validation sheets. The package, last updated in January 2025, has over 130 million installs and currently has no known critical security advisories [107], [108].

On the client side, the JSZip library is used to create the ZIP-based signature container, which stores the documents and their associated metadata. This library also supports reversible operations for managing container content. Although its last major release was in August 2022, it remains widely used and has no known vulnerabilities [109], [110].

The system uses the OpenPGP.js library for all cryptographic operations, including key generation, digital signing, and signature validation. Originally developed in 1997 for secure email communication, it continues to be updated and is considered a stable, trusted solution. No vulnerabilities have been reported in its latest versions [111], [112], [113].

For styling and usability enhancements, the system also integrates Flowbite and Orest Bida's CookieConsent libraries. As outlined in Chapter 3.5, the system follows a lightweight front-controller architecture with procedural logic grouped into a shared functions file for clarity and maintainability.

Five core features were developed based on the requirements gathered during stakeholder engagement. These are summarised in Table 10.

Table 10. Core System Features

Feature	**Description**
Enrolment and authentication	Creation of a secure digital identity through user account creation and login.
Key operations	Generation and revocation of public/private key pairs.
Container generation and workflow initiation	Preparing a signable document container and initiating the signing workflow.
Document signing	Receiving signing tasks and applying the digital signature.
Container validation	Verifying the container's integrity and signatures, and generating a validation sheet if needed.

To enhance usability, two additional features were implemented, as shown in Table 11.

Table 11. Usability enhancements

Feature	**Description**
Permission levels	Allows assignment of specific roles, including signing, workflow initiation, and administration.
Ministries groups	Enables filtering of signers by ministry for easier task assignment.

Since the system is used to establish digital identities and aims to operate securely within an intra-governmental context, security considerations have been comprehensively addressed. These are summarised in Table 12.

Table 12. Implemented security measures

Security measure	**Description**
Strict user enrolment	Account creation requires in-person verification using official documents such as a passport or ID.
Multi-factor authentication	Access requires a username, password, and one-time PIN sent via email (to be replaced with SMS or app-based codes in production).
Safe private key handling	Key pairs are generated in the browser; only the public key is sent to the server. The private key is downloaded and never stored server-side.
Short session time	Sessions expire after a period of inactivity, requiring reauthentication.

The principles of the project management triangle [114] are also applicable to this system. As a rapid-response solution designed to bridge the gap until a national PKI is fully deployed, certain technical trade-offs were necessary; however, these have been addressed through deliberate design decisions, as summarised in Table 13.

Table 13. System Limitations and Mitigation Strategies

Weakness	**Mitigation measure**
PHP and MariaDB are not designed for high-assurance systems	Regular source code hash verification, external audit log storage, and hardened access controls.
Private keys are stored on the user's device	While permitted under AdES, signing requires full authentication. Offline signing is not possible, minimising the risk of unauthorised use.

In addition to these general safeguards, specific threat scenarios were analysed and addressed. These scenarios represent realistic risks in the system's operational context and are mitigated through design choices, as shown in Table 14.

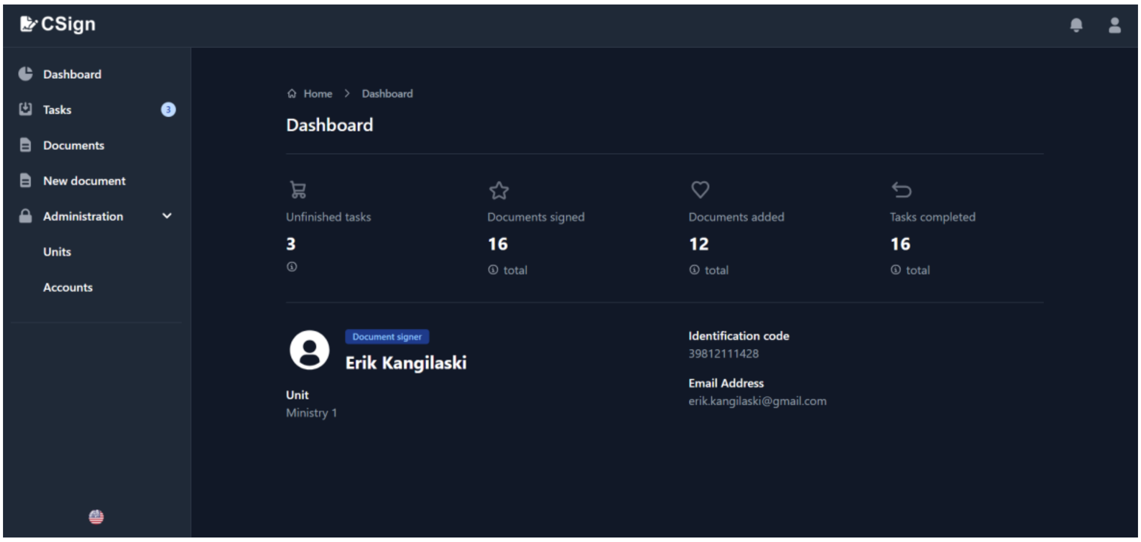
Table 14. Threat scenarios mitigations

Threat scenario	**Mitigation measure**
Lost private key	The key can be revoked and a new key generated without affecting system access. Only the key itself needs to be replaced.
Stolen private key	Signing requires successful authentication. The private key alone is insufficient to sign on behalf of another user.
Insider misuse	All critical actions are logged externally. Misuse can be traced, although strong internal audit policies are also recommended.
Replay attacks	Sessions expire quickly. Even if account access is compromised, the attacker would still need the user's local private key.
Signed container manipulation	The signature container is hashed, and the value is stored in both the internal database and the container itself. Any changes are detected during validation.
Weak password or email compromise	Multi-factor authentication is enforced. Planned updates include app-based or SMS code delivery to strengthen identity verification.

4.1.1 System Overview

The system has been developed with two primary user groups in mind: secretaries, who are responsible for preparing documents for signing, and ministers, who review and sign them. Additionally, administrators oversee system usage, manage user enrolment, and handle account deactivations. Although the user groups are well-defined, permissions are not strictly role-based; instead, the system uses a granular permission model. For example, ministers may be granted permissions to both initiate and sign documents, depending on the administrative configuration.

As illustrated in Figure 6, the user interface is designed to be simple and intuitive. Navigation elements are positioned on the side, and the interface maintains a clean layout to minimise distractions. The dashboard view displays an overview of unfinished tasks and other relevant statistics. The system is fully mobile-responsive and supports use across laptops, desktops, tablets, and smartphones. Additionally, user guidance is built in: whenever an error occurs, the system provides contextual explanations and suggests corrective actions.



Dashboard

Unfinished tasks 3

Documents signed 16 total

Documents added 12 total

Tasks completed 16 total

Erik Kangilaski

Unit
Ministry 1

Identification code
39812111428

Email Address
erik.kangilaski@gmail.com

Figure 6. User interface design

Signed documents are stored in a custom ZIP-based archive format with a system-specific file extension. Each container includes a metadata.json file, which contains the document container ID, hashes of the stored files, and signature metadata (including key ID, public key, and signature file name). The signature files themselves are located in a signatures/ folder, while the document files are compressed into a *files/* folder. To avoid unnecessary hash mismatches caused by changes to file timestamps, the modification dates of all included files and the archive are normalised to zero.

The system relies on a relational database schema to manage key entities such as user accounts, key pairs, tasks, and containers. Each document container is associated with a unique document ID, which is used during validation to cross-check metadata and ensure consistency. The schema is designed to support secure access control, digital signature verification, and administrative operations. Table 15 summarises the main database tables and their roles within the system.

Table 15. Key database tables and their roles in the digital signature system

Table name	**Description**
accounts	Stores user info such as ministers, secretaries, and admins.
account_keys	Contains public keys for digital signatures, with validity periods.
accounts_logins	Stores login attempts for each account (success/failure + IP).
accounts_logincodes	Manages one-time codes used for login or 2FA.
accounts_pinchanges	Tracks password reset requests and their state.
documents	Holds signable documents, unsigned/signed files, and metadata.
logs	Tracks system events and errors for audit and debugging.
rate_limiter	Prevents abuse by limiting how often an action can be done per IP.
tasks	Assigns and tracks document-related tasks between users.
units	Organises users into departments or organisational units.

4.1.2 User Workflows

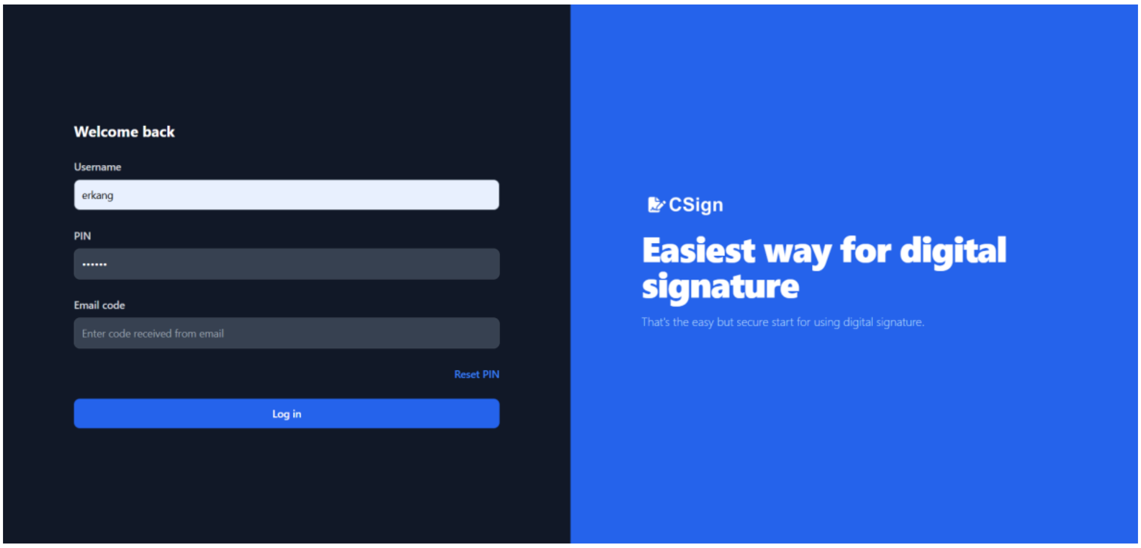
This section provides a detailed overview of the five core features of the system, focusing on how users interact with it in practice.

Enrolment and authentication

To gain access to the system, officials must first undergo an organisational identity verification process. This process involves presenting a valid government-issued document (such as a passport or national ID-card), which is verified by an administrator. This enrolment step is critical, as it establishes the user’s digital identity within the system.

Once verification is completed, the administrator creates a new user account by entering the official's username, full name, email address, assigned permissions, and affiliated ministry or organisational unit. After account creation, the official is provided with their username and can initiate the login process by requesting a password setup link.

To log in, the user navigates to the login page (shown in Figure 7), enters their username and password, and completes multi-factor authentication (MFA) by entering a one-time code sent to their registered email address. In case of repeated failed login attempts, the account is temporarily locked and must be manually reactivated by an administrator.


Welcome back

Username: erkang

PIN: ••••••

Email code: Enter code received from email

CSign

Easiest way for digital signature

That's the easy but secure start for using digital signature.

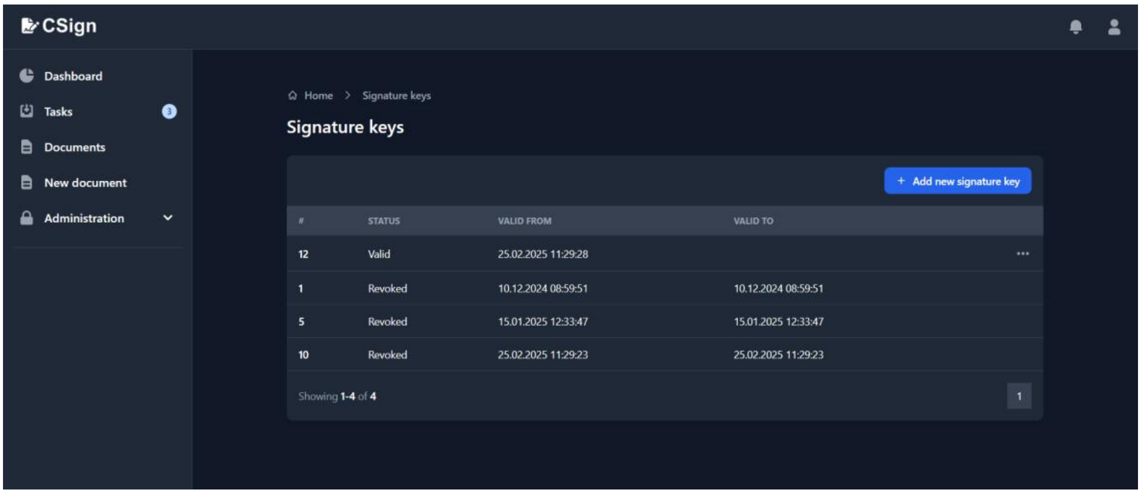
Figure 7. Log-in page

Key operations

After successfully logging in, users who need to digitally sign documents must generate a public–private key pair. As shown in Figure 8, this process is user-friendly: the user clicks a *Generate Key* button, chooses a secret PIN code to protect the private key, and downloads the private key file to their device.

Only one active key pair can be associated with an account at a time. However, users may revoke an existing key and generate a new one if needed. Key generation takes place entirely in the browser using OpenPGP.js and the Ed25519 elliptic curve, a cryptographic algorithm widely recommended for digital signatures [111].

While downloading a private key to a personal device is not ideal in high-assurance environments, the system mitigates this risk by requiring secure login and PIN entry before any signing operation. This approach balances ease of use with reasonable security for an interim solution in a low-PKI environment.



Signature keys

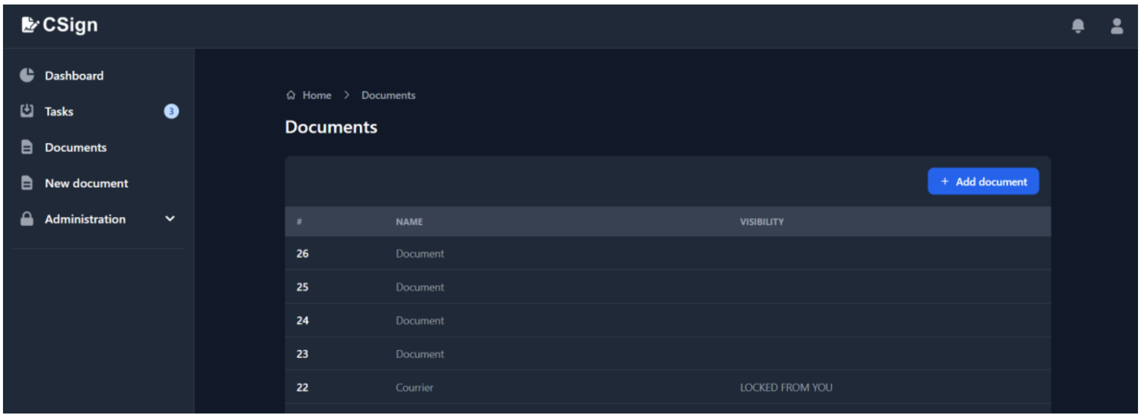
#	STATUS	VALID FROM	VALID TO
12	Valid	25.02.2025 11:29:28	
1	Revoked	10.12.2024 08:59:51	10.12.2024 08:59:51
5	Revoked	15.01.2025 12:33:47	15.01.2025 12:33:47
10	Revoked	25.02.2025 11:29:23	25.02.2025 11:29:23

Showing 1-4 of 4

Figure 8. Signature key page

Container generation and workflow initiation

Users can access the document list page, which displays all documents created within the digital signature system, as illustrated in Figure 9. While the list is visible to all authenticated users, detailed access is restricted to the document's creator and assigned signers. This ensures both transparency and privacy, while maintaining trust and access control.



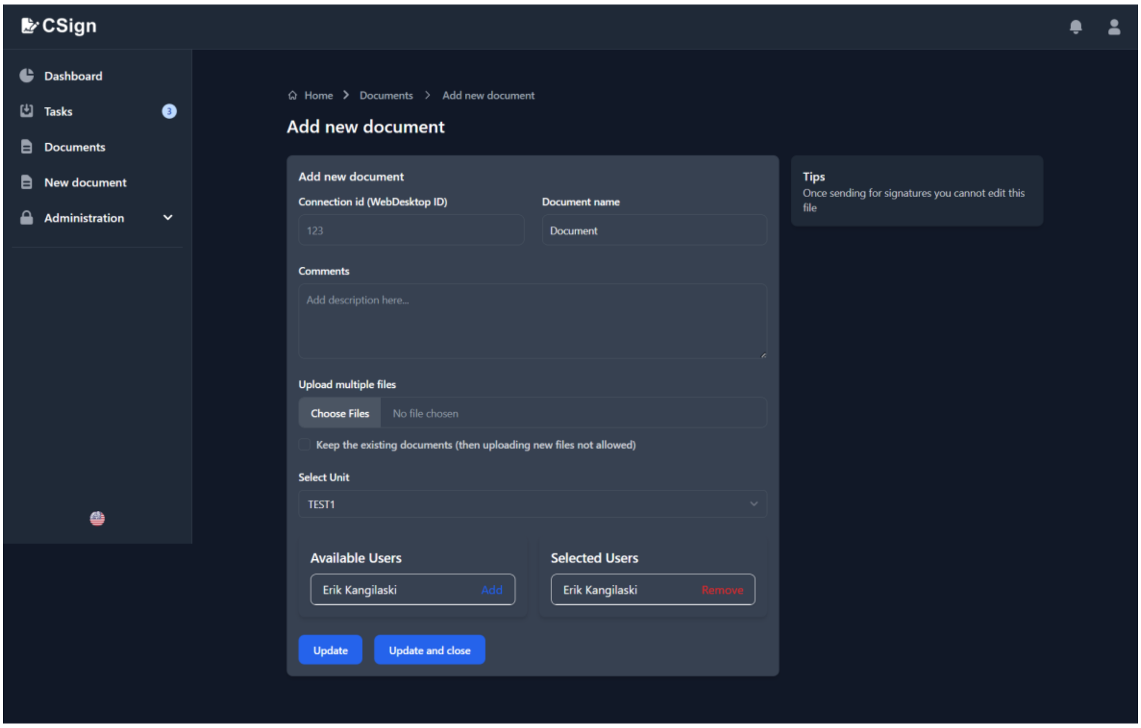
Documents

#	NAME	VISIBILITY
26	Document	
25	Document	
24	Document	
23	Document	
22	Courrier	LOCKED FROM YOU

Figure 9. Document list page

To initiate a new signing workflow, users can create a new document record. The form requires a connection ID (e.g., from an EDRMS) and at least one uploaded file. Document name and comments are optional but encouraged. This enables a streamlined process where users can export a document from the EDRMS, upload it to the signing system, and simply specify the required signers.

As shown in Figure 10, the signer selection interface supports filtering by ministry or organisational unit. Once the form is submitted and signing users are assigned, a dedicated button appears to initiate the signing workflow.



Add new document

Add new document

Connection id (WebDesktop ID): 123

Document name: Document

Comments: Add description here...

Upload multiple files: Choose Files No file chosen

□ Keep the existing documents (then uploading new files not allowed)

Select Unit: TEST1

Available Users: Erik Kangilaski Add

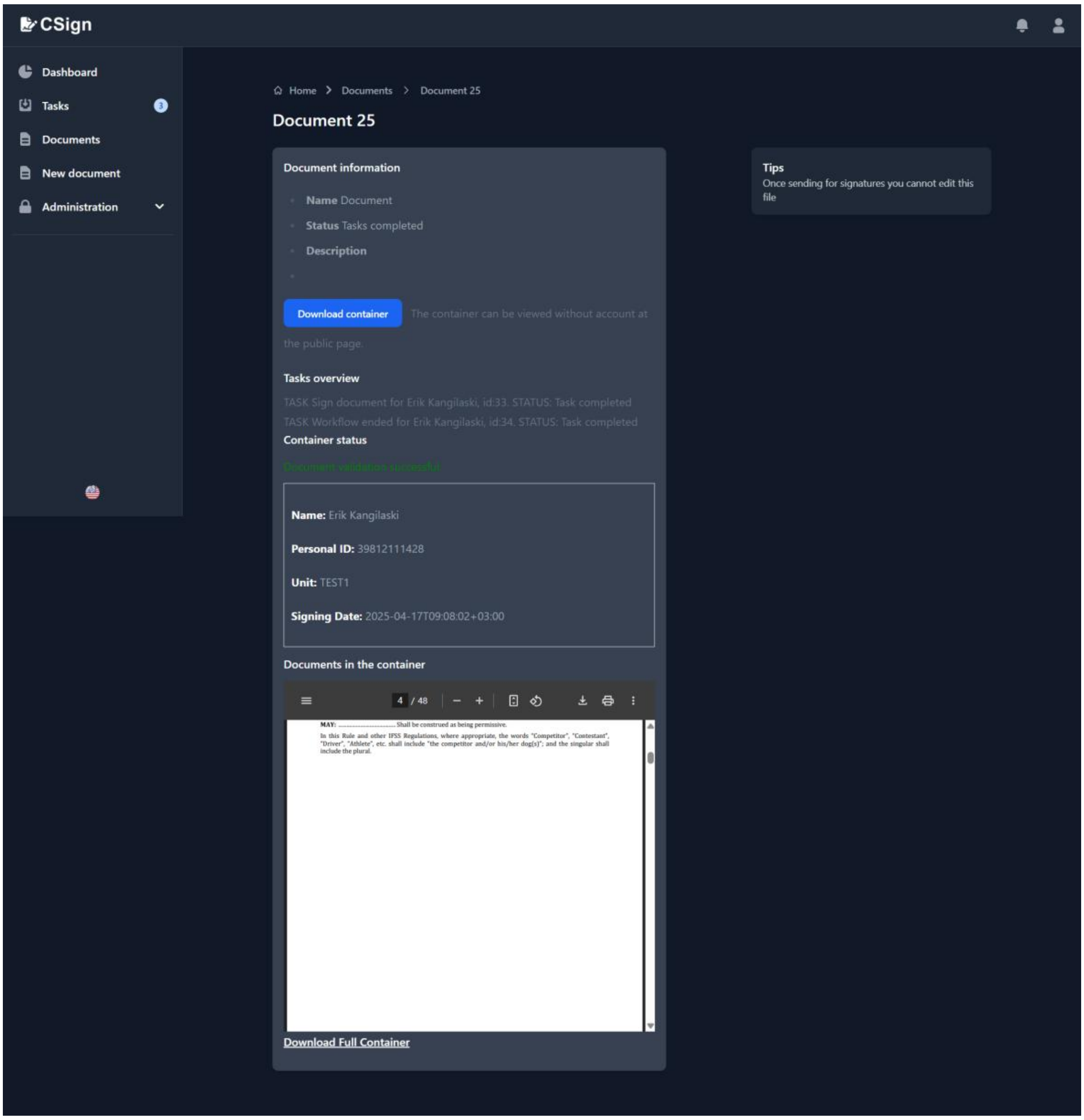
Selected Users: Erik Kangilaski Remove

Tips

Once sending for signatures you cannot edit this file

Figure 10. New document creation page

Each saved document can be viewed by those with access rights. Figure 11 shows the document view page, which displays basic metadata, the current workflow status, and, if signatures have been added, a list of signatures. If only one PDF is present, it is previewed in an embedded frame; if multiple files exist, they are presented in a downloadable list. A container validation check is also automatically performed on this page.



Document 25

Document information

- Name Document
- Status Tasks completed
- Description

Download container The container can be viewed without account at the public page.

Tasks overview

TASK Sign document for Erik Kangilaski, id:33. STATUS: Task completed
TASK Workflow ended for Erik Kangilaski, id:34. STATUS: Task completed

Container status

Document validation successful

Name: Erik Kangilaski

Personal ID: 39812111428

Unit: TEST1

Signing Date: 2025-04-17T09:08:02+03:00

Documents in the container

MAY: .... Shall be construed as being permissive.
In this Rule and other IFSS Regulations, where appropriate, the words "Competitor", "Contestant", "Driver", "Athlete", etc. shall include "the competitor and/or his/her dog(s)"; and the singular shall include the plural.

Download Full Container

Tips
Once sending for signatures you cannot edit this file

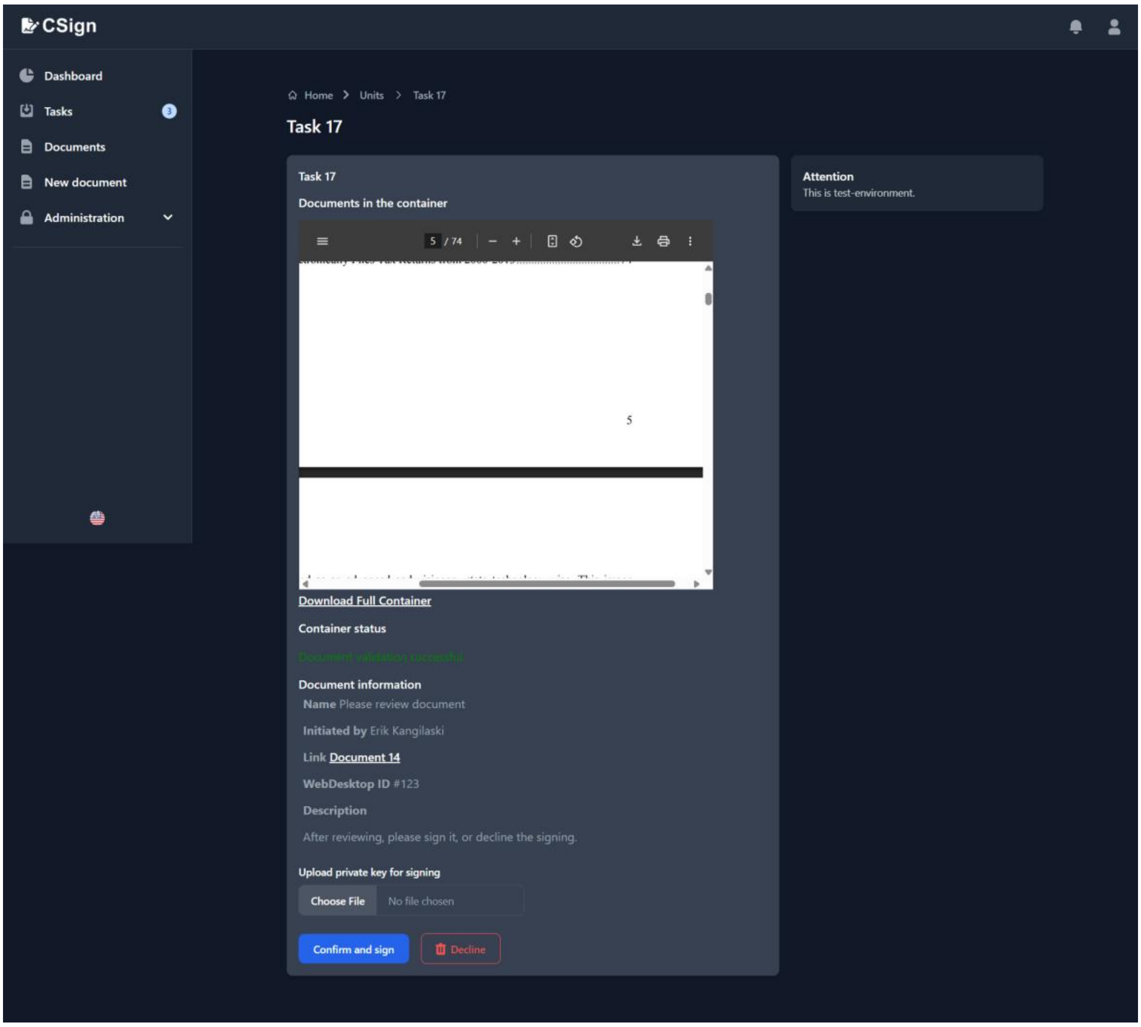
Figure 11. Document overview page

Document signing

After a signing workflow is initiated, designated signers are notified via email, but only if they have no prior incomplete signing tasks. This approach prevents redundant notifications and reduces the risk of spamming users with repeated emails.

As shown in Figure 12, the signer is presented with the document's primary metadata and a link to the full document view. At the bottom of the interface, a file upload form allows the signer to submit their private key file. To complete the signing process, the user enters the PIN associated with their private key in a secure prompt. The system then performs an initial validation of the container, and only if the validation is successful, the digital signature is generated and appended to the container.

When all required signatures have been collected, the system generates a final task for the workflow initiator, informing them that the document is ready for upload back to the EDRMS. The same process is followed if any signer declines to sign, ensuring the initiator is notified regardless of outcome.



Task 17

Task 17

Documents in the container

Attention
This is test-environment.

Container status

Document validation successful

Document information

Name Please review document

Initiated by Erik Kangilaski

Link Document 14

WebDesktop ID #123

Description

After reviewing, please sign it, or decline the signing.

Upload private key for signing

No file chosen

Figure 12. Document signing page

Container validation

Both unsigned and signed containers can be downloaded from the system and shared with external parties, including citizens or institutions not registered in the system. Validation functionality is available on the document view, document signing, and public validation pages, as shown in Figure 13.

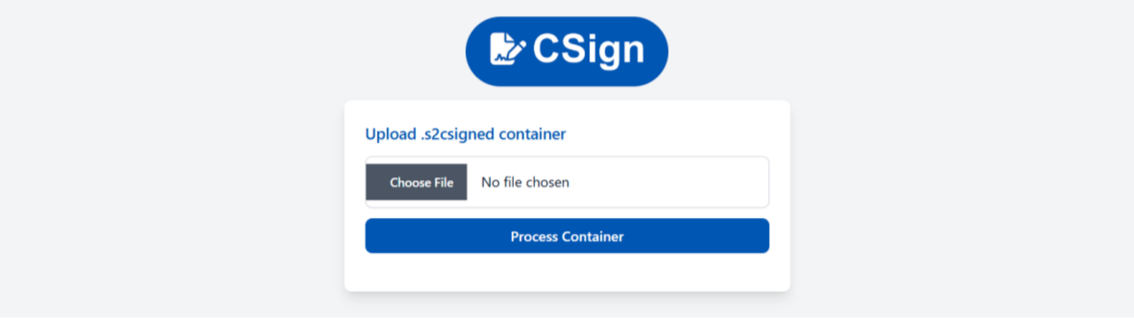


Figure 13. Container validation page

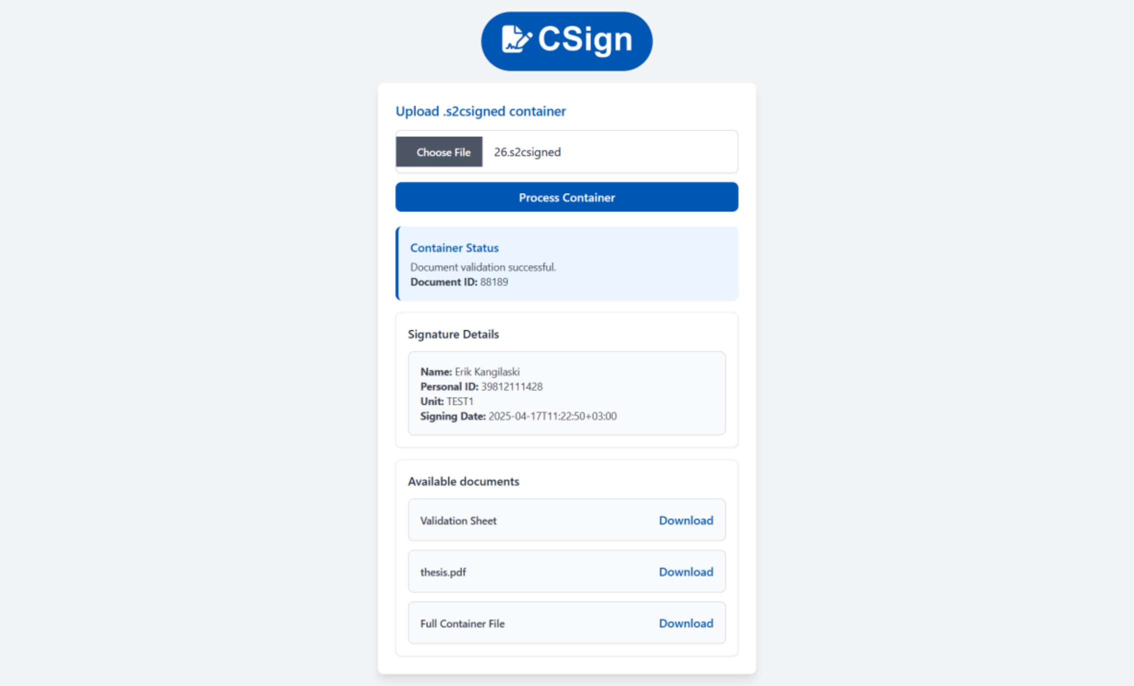
To begin validation, the user selects the container file and clicks the *Process Container* button. Validation is performed in two stages: client-side and server-side.

On the client side, the structure of the container is checked using JSZip and OpenPGP. Required files (e.g., metadata, signature folders) must be present. Then, the SHA-256 hashes of the signed files are computed and compared to the values in the *metadata.json*. For each signature, the system verifies that the public key matches the expected hash.

After client-side checks, the container is sent to the server, which retrieves the corresponding document from the database based on the document ID in the metadata. Hash values from three sources, the database, client-side computation, and metadata, are compared for consistency.

Next, the system validates each signature using the stored public key. It checks whether the key was valid and not revoked at the time the signature was applied. The files are then rehashed server-side for verification. File sizes are also recorded.

Finally, a PDF validation sheet is generated using Dompdf. This sheet includes the overall validation status, the document's connection ID (to facilitate cross-referencing in the EDRMS), and a list of all signatures along with their verification status, and a summary of the signed files. Additionally, individual download links are provided for each file included in the container. Once the validation process is complete, the server returns this data as a structured JSON object, which is then rendered in the user interface as illustrated in Figure 14.



Upload .s2csigned container

26.s2csigned

Container Status

Document validation successful.
Document ID: 88189

Signature Details

Name: Erik Kangilaski
Personal ID: 39812111428
Unit: TEST1
Signing Date: 2025-04-17T11:22:50+03:00

Available documents

Validation Sheet

thesis.pdf

Full Container File

Figure 14. Document validation page with validated container information

4.1.3 Planned Improvements

While the system is technically secure and functionally complete, several enhancements are planned to qualify for full eIDAS AdES compliance and to improve usability and permission control.

From a user experience perspective, future work includes support for parallel signing, which would streamline document workflows involving multiple signers. Additionally, permission granularity should be improved by introducing read-only roles, allowing users to view documents without being assigned signing tasks. This aligns with the principle of least privilege and supports better document governance.

On the security side, smartcard-based key storage is recommended for production environments. This would ensure that private keys are generated and used entirely within a secure hardware environment, eliminating the residual possibility of key leakage, which is already mitigated in the current system through client-side key generation and multi-factor authentication, but could be further reduced with hardware-based signing.

To meet AdES technical requirements, the current custom container format must be replaced with a standardised format such as ASiC-E. The signature metadata must be structured using XAdES (XML Advanced Electronic Signatures), and include signer identity attributes, signature references, and document hashes. Additionally, the system must support trusted timestamps from a Time Stamping Authority (TSA), and implement an immutable, append-only audit trail to ensure tamper-evident tracking of signing events.

4.2 Validation of the Artefact

As described in the Methodology chapter, the digital signature artefact was validated in two workshops with stakeholders in Djibouti: first after the initial version was completed, and second after the first improvements had been implemented.

Both workshops were constructive, and the feedback was generally positive. The participants agreed that the artefact could solve the missing digital signing capability in the workflows currently being implemented within their EDRMS. The system was considered relevant, functional, and secure enough to meet their expectations.

During the first workshop, a concern was raised that when a digitally signed document needs to be shared with a citizen who does not use digital tools, there should be a way to generate a PDF confirmation that proves the document has been signed. This feature was added before the second workshop, and no further missing features were pointed out.

Participants expressed a preference for having digital identity integrated directly into the EDRMS rather than using two separate systems. This is not currently possible, as the EDRMS does not provide strong enough authentication and is not meant to serve as an identity provider. It would be technically possible to integrate the signing system into the EDRMS for user authentication and document signing, but this would require additional development work on the EDRMS side. The current approach avoids the need for integration, which makes it faster to implement, but also brings some disadvantages.

Since the system includes basic workflows alongside the signing functionality, using it together with an EDRMS may feel complicated for higher-level officials. While these users are experts in their fields, they may have less experience with digital systems. Even using one digital system can already require effort and training, and having two separate ones can make this more difficult.

In terms of perceived usefulness, stakeholders recognised the benefits of the system compared to the existing paper-based or hybrid workflows, where EDRMS is used but signatures are still done on paper. As mentioned earlier, digital transformation should happen in smaller steps so that everyone can get used to the changes gradually. Regarding perceived ease of use, participants did not raise concerns about the system's security, the level of assurance, or the way signature containers are handled.

Some stakeholders suggested that the workflows inside the signing system could be made even simpler, to help users with lower digital skills manage their tasks more easily. They also noted that the main obstacle to using the system in practice is that digital signatures are not yet legally recognised. Without legal enforceability, there is no real benefit to switching from handwritten signatures to digital ones.

5 Contributions and Discussions

Building on the implementation presented in the previous chapter, this section reflects on the broader findings and implications of the developed solution. It evaluates the artefact's practical relevance, identifies remaining limitations, and discusses the social, legal, and technical conditions required for successful adoption. It also explains the design choices made during development, assesses their trade-offs, and outlines how the artefact contributes to the broader goals of digital transformation in the public sector.

5.1 Findings and Contributions

Traditional paper-based workflows are increasingly inefficient compared to the capabilities of modern digital systems. This also applies to governmental workflows in Djibouti, where the implementation of an EDRMS is intended to address inefficiencies caused by slow postal delivery, difficulties in archiving and retrieving documents, and the lack of traceability. It also aims to initiate a gradual digital transformation in administrative thinking by shifting away from a paper-based mindset and towards more efficient processes. Although the EDRMS can accelerate certain tasks, it may also complicate workflows if not paired with fully digital processes.

While this reflects the focus of research question 1 defined in Section 1.3, it is also important to note that Djibouti is still in the process of developing legislation related to digital identity and electronic signatures. At the time of writing, electronic signatures are not considered legally binding.

All interviewees agreed that the introduction of EDRMS improves the efficiency of internal correspondence and document handling, answering the research question 2. However, several challenges were identified. These include missing laws, hierarchical processes that limit flexibility, and lower digital skills, especially among higher-level officials. These issues contribute to mistrust and create difficulties in adopting new tools. Furthermore, implementation success depends heavily on active and visible support from management. Without such involvement, the project is unlikely to succeed.

To answer Research question 3 and 3.1, 44 functional and non-functional requirements were defined in Chapter 3. The required level of authentication assurance was identified as *substantial* according to the eIDAS framework. Within the scope of this thesis, only the highest-priority requirements, as defined by the MoSCoW method, were implemented.

As a result of the research, a digital signature artefact was developed and validated by stakeholders. Only the most critical features were included. The minimum viable product supports five essential functions: user enrolment and authentication, public and private key operations, document container generation and workflow initiation, document signing, and container validation. These are sufficient for the rapid deployment of a governmental digital identity system while a full-scale public key infrastructure is being developed.

5.2 Discussion

Despite successful validation, several unresolved tensions remain that influence whether the developed solution can be adopted in practice. While the artefact was successfully built and received positive feedback, the final outcome depends on the people and institutions in Djibouti. Even though the system is designed to be secure, digital signatures and user authentication cannot have legal status unless local legislation supports them. As Djibouti does not yet legally recognise electronic signatures, the system can only be prepared technically and kept ready for use once the legislation is updated.

Based on interviews and observations, it can be concluded that technology alone cannot solve the problem. Digital transformation is not only a technical challenge but also a human and political one. Even if the legal status were established, much work would still be needed to train users to use the system safely and effectively. This is especially important for high-level officials, who often have lower levels of digital literacy. Since they have decision-making power, any mistake or vulnerability, such as falling victim to manipulation or security risks, can have greater consequences than for regular staff.

The role of leadership cannot be ignored in this kind of project. In cases where management is supportive and involved, problems tend to be solved quickly, or at least within the agreed timeline. This helps to build trust in the project and keep it on track.

However, if management lacks experience or shows limited interest, projects like this can face delays. Even when problems are clearly defined, a lack of follow-up and clear actions from leadership can cause the implementation to stall. While technical quality is essential, real success in digital transformation depends on committed and capable leadership.

The developed artefact, a digital signature solution, follows the general requirements of AdES. It includes secure enrolment, two-factor authentication, safe generation and storage of private keys, validation of signed containers, and detection of tampering. While timestamping is not yet included, it should be added in future versions to improve legal recognition. Still, the current implementation demonstrates that even in a low-resource context, a substantial level of assurance and mid-level signature quality can be achieved if the solution is designed carefully.

Although the artefact is technically production-ready, the responsibility for its adoption now lies with the local authorities in Djibouti. Final implementation depends on the development and approval of national legislation that recognises digital identity and electronic signatures.

The development process followed the logic of DSR. The artefact was built in response to a real need, and stakeholder feedback was used to improve it further. The result was a working system, validated by actual users in a real context. Evaluation was conducted in a natural setting, consistent with DSR methodology, where practical solutions are developed, applied, and assessed in real environments. This confirms that functioning digital signature systems can be created and evaluated even when legal and institutional frameworks are still developing.

During development, a simple and independent solution was preferred over full integration. The digital signature system was built to function separately from existing EDRMS platforms. While this means that users must work across two systems, it allowed the solution to be developed quickly without needing to request or build API integrations or plugins, particularly important considering that some EDRMS platforms are privately owned and extending them is costly. This design also improves identity security, as authentication is fully handled within the signing system. This makes it possible for the EDRMS to operate with lower authentication levels without compromising the overall assurance level of the signing process.

A second trade-off involved the balance between assurance level and ease of implementation. The system currently generates private keys in the user's browser and stores them locally. This enables a lightweight and simple setup, but introduces certain vulnerabilities. As discussed earlier, these are mitigated by two-factor authentication and controlled access. While smartcards or hardware security modules could provide stronger guarantees, they would significantly increase complexity and delay implementation. Split-key cryptography is another option, but it introduces its own development and usability challenges. Given the current context, the selected approach provides a reasonable compromise between assurance and practicality.

The third consideration is related to advanced features. The solution is a production-ready artefact but does not yet include timestamping, detailed signer metadata, or tamper-proof audit logs. These features are not strictly required for AdES-level compliance but are important for improving long-term security, legal robustness, and accountability. They should be considered in future iterations, especially if the system is to be scaled or used for more critical decision-making.

Overall, the developed digital signature solution is well-suited for low digital maturity environments that require a fast and reliable way to introduce electronic signatures. It is based on open-source tools, has minimal infrastructure requirements, and can be deployed without major external dependencies. However, legal recognition is critical. Without proper legislation that accepts digital signatures as equivalent to handwritten ones, systems like this cannot offer their full benefits. Legal readiness, institutional support, and basic user training must go hand-in-hand with technical development to ensure real impact.

6 Conclusion

To start digital transformation in low e-government maturity contexts, it is reasonable to begin with internal correspondence systems such as EDRMS and e-cabinet solutions. In order to fully digitalise existing workflows, the ability to sign documents electronically is essential, yet often overlooked. The aim of this thesis was to address that gap in Djibouti, identified through field visits, interviews, and document analysis, and to provide a digital signature solution that can be set up rapidly while the country prepares for full-scale PKI implementation.

The need for such a solution was confirmed during four on-site visits and six interviews with key public sector stakeholders in Djibouti. Based on the findings, the required assurance level for digital signatures was defined. A total of 44 functional requirements were collected, structured using the FURPS+ model, and prioritised using the MoSCoW method. A production-ready minimum viable product was developed using a design science research approach, covering the *Must have* requirements. The system is designed for low-resource environments where PKI is not yet available, and supports electronic authentication and digital signatures aligned with eIDAS substantial assurance and the advanced electronic signature level. The artefact was validated in two workshops with public sector stakeholders in Djibouti.

Technically, the system follows eIDAS principles. It uses Ed25519 cryptography, client-side key generation with OpenPGP, and open-source JavaScript libraries. Private keys are not stored server-side, two-factor authentication is enforced, and session handling is secured. The solution is independent and does not require EDRMS integration, which speeds up implementation and keeps identity management self-contained. At the same time, users must work in two systems, which adds some complexity. Identified vulnerabilities and user experience issues were mitigated with design improvements.

While the artefact is ready for production use, legal recognition is necessary before it can be fully adopted. Digital signatures must be accepted as equal to handwritten ones. Training is also important, especially for officials with limited digital literacy. They must understand both how to use the system and how to avoid risks in the digital environment. Full implementation is outside the scope of this thesis, since legislative processes require time and political decision-making.

The solution developed is not only suitable for Djibouti. It can be used as a temporary signing system in other countries with similar limitations. It works as a bridge until a national PKI is in place, and helps governments make early progress in digitalisation.

In future development, the system can be improved to better meet eIDAS and long-term validation requirements. Possible improvements include stronger private key storage, support for timestamping, and switching to the XAdES container format.

This thesis provides both a working system and a practical path for moving forward with digital signing in low-resource conditions. It shows that digital signatures do not need to wait for full infrastructure and legal readiness. With a focused approach and institutional support, countries like Djibouti can already take meaningful steps toward digital governance.

References

[1] United Nations: Department of Economic and Social Affairs, *United Nations e-Government Survey 2022: The Future of Digital Government*. in United Nations e-Government Survey Series. New York: United Nations Publications, 2022.

[2] ‘Djibouti - The World Factbook’, Central Intelligence Agency. Accessed: May 11, 2025. [Online]. Available: https://www.cia.gov/the-world-factbook/about/archives/2023/countries/djibouti/

[3] ‘Djibouti: Country Profile’, Freedom House. Accessed: May 11, 2025. [Online]. Available: https://freedomhouse.org/country/djibouti

[4] Republic of Djibouti, ‘Vision Djibouti 2035’. Accessed: May 11, 2025. [Online]. Available: https://djiboutiembassykuwait.net/assets/files/djibouti-2035-en.pdf

[5] A. Muñoz-Cañavate and P. Hípola, ‘Electronic administration in Spain: From its beginnings to the present’, *Gov. Inf. Q.*, vol. 28, no. 1, pp. 74–90, 2011.

[6] ‘Djibouti Launches Digital Transformation to Improve Services to Citizens’, World Bank. Accessed: May 11, 2025. [Online]. Available: https://www.worldbank.org/en/news/press-release/2018/04/25/djibouti-launches-digital-transformation-to-improve-services-to-citizens

[7] ‘Podcast & blog : Making interoperability a reality in Djibouti’, E-riigi Akadeemia. Accessed: May 08, 2025. [Online]. Available: https://ega.ee/interoperability-djibouti/

[8] A. R. Hevner, S. T. March, J. Park, and S. Ram, ‘Design science in information systems research’, *MIS Q.*, pp. 75–105, 2004.

[9] L. Carter, V. Yoon, and D. Liu, ‘Analyzing e-government design science artifacts: A systematic literature review’, *Int. J. Inf. Manag.*, vol. 62, p. 102430, 2022.

[10] L. Õunapuu, *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes*. Tartu : Tartu Ülikool, 2014. Accessed: May 11, 2025. [Online]. Available: http://hdl.handle.net/10062/36419

[11] A. Abel, ‘Agile software development in the public sector-the case of digital learning resources portal e-Koolikott’, 2016, Accessed: May 11, 2025. [Online]. Available: https://www.academia.edu/download/64283155/786e298f645140f78d67ab0f412e7208.pdf

[12] A. R. Hevner, ‘A three cycle view of design science research’, *Scand. J. Inf. Syst.*, vol. 19, no. 2, p. 4, 2007.

[13] E. Kangilaski, E. B. Jackson, Y. Martinez Mancilla, and I. Pappel, ‘Enabling Digital Governance: Developing a Digital Signature Solution for Djibouti’s E-Cabinet’, presented

at the Tenth International Conference on eDemocracy & eGovernment - ICEDEG 2025, Bern, Switzerland, 2025.

[14] W. Van Casteren, *The Waterfall Model and the Agile Methodologies : A comparison by project characteristics*. 2017. doi: 10.13140/RG.2.2.36825.72805.

[15] J. Venable, Pries-Heje ,Jan, and R. and Baskerville, ‘FEDS: a Framework for Evaluation in Design Science Research’, *Eur. J. Inf. Syst.*, vol. 25, no. 1, pp. 77–89, Jan. 2016, doi: 10.1057/ejis.2014.36.

[16] J. Venable, ‘A framework for design science research activities’, in *Emerging Trends and Challenges in Information Technology Management: Proceedings of the 2006 Information Resource Management Association Conference*, Idea Group Publishing, 2006, pp. 184–187.

[17] J. Venable, J. Pries-Heje, and R. Baskerville, ‘A Comprehensive Framework for Evaluation in Design Science Research’, in *Design Science Research in Information Systems. Advances in Theory and Practice*, K. Peffers, M. Rothenberger, and B. Kuechler, Eds., Berlin, Heidelberg: Springer, 2012, pp. 423–438. doi: 10.1007/978-3-642-29863-9_31.

[18] D.-P. Pop and A. Altar, ‘Designing an MVC model for rapid web application development’, *Procedia Eng.*, vol. 69, pp. 1172–1179, 2014.

[19] E. Rashid and N. E. Mastorakis, ‘A Novel Complexity Scoring Model for Non-Functional Requirements in Request for Proposal in Housing Industry Using FURPS Quality and Moscow Priority Model’, *Int. J. Hous. Sci. Its Appl.*, vol. 45, no. 4, pp. 30–40, Dec. 2024, doi: 10.70517/ijhsa4543.

[20] J. Hristoforov, ‘Tegevusriskide juhtimise parendamine Enefit Power AS-i näitel’, May 2022, Accessed: May 11, 2025. [Online]. Available: https://digikogu.taltech.ee/et/item/d9c063f3-527a-4ccf-93e2-45c136ad61a9

[21] J. Tepandi, ‘Tarkvara protsessid ja kvaliteet - osaline lühiülevaade’. Jan. 15, 2024. Accessed: May 11, 2025. [Online]. Available: https://tepandi.ee/tks-loeng.pdf

[22] A. Roosleht, ‘Klienditeavituste rakenduse juurutamine Zone Media OÜ näitel’, Master’s Thesis, 2023. Accessed: May 11, 2025. [Online]. Available: https://digikogu.taltech.ee/et/item/5399ff77-e244-42dd-80b0-96ced557bd70

[23] J. Deacon, ‘Model-View-Controller (MVC) Architecture’, 2009. Accessed: May 11, 2025. [Online]. Available: https://www.academia.edu/download/50526307/MVC.pdf

[24] R. Lelumees, ‘Spordialaliidu infosüsteem’, Bachelor’s Thesis, 2014. Accessed: May 11, 2025. [Online]. Available: https://digikogu.taltech.ee/et/item/b7dd6d4a-d57b-4888-a8b8-56c93f426668

[25] A. Muñoz-Cañavate and P. Hípola, ‘Electronic administration in Spain: From its beginnings to the present’, *Gov. Inf. Q.*, vol. 28, no. 1, pp. 74–90, Jan. 2011, doi: 10.1016/j.giq.2010.05.008.

[26] A. Cordella and F. Iannacci, ‘Information systems in the public sector: The e-Government enactment framework’, *J. Strateg. Inf. Syst.*, vol. 19, no. 1, pp. 52–66, Mar. 2010, doi: 10.1016/j.jsis.2010.01.001.

[27] P. Dunleavy, H. Margetts, S. Bastow, and J. Tinkler, ‘New public management is dead—long live digital-era governance’, *J. Public Adm. Res. Theory*, vol. 16, no. 3, pp. 467–494, 2006.

[28] B. Gupta, S. Dasgupta, and A. Gupta, ‘Adoption of ICT in a government organization in a developing country: An empirical study’, *J. Strateg. Inf. Syst.*, vol. 17, no. 2, pp. 140–154, Jun. 2008, doi: 10.1016/j.jsis.2007.12.004.

[29] R. Heeks, ‘Reinventing government in the information age’, in *Reinventing Government in the Information Age*, Routledge, 1999.

[30] S. Lips, V. Tsap, N. Bharosa, R. Krimmer, T. Tammet, and D. Draheim, ‘Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership: Learning from the Case of Estonia’, *Inf. Syst. Front.*, vol. 25, no. 6, pp. 2439–2456, Dec. 2023, doi: 10.1007/s10796-022-10363-5.

[31] K. Axelsson, U. Melin, and I. Lindgren, ‘Public e-services for agency efficiency and citizen benefit — Findings from a stakeholder centered analysis’, *Gov. Inf. Q.*, vol. 30, no. 1, pp. 10–22, Jan. 2013, doi: 10.1016/j.giq.2012.08.002.

[32] A. Mustafa and M. Sharifov, ‘The Challenges of e-Parliament Adoption and its Mitigation’, vol. 5, p. 87, Jun. 2018.

[33] R. K. Ahmed *et al.*, ‘A Legal Framework for Digital Transformation: A Proposal Based on a Comparative Case Study’, in *Electronic Government and the Information Systems Perspective*, A. Kö, E. Francesconi, G. Kotsis, A. M. Tjoa, and I. Khalil, Eds., Cham: Springer International Publishing, 2021, pp. 115–128. doi: 10.1007/978-3-030-86611-2_9.

[34] S. C. J. Palvia and S. S. Sharma, ‘E-government and e-governance: definitions/domain framework and status around the world’, in *International Conference on E-governance*, 2007, pp. 1–12. Accessed: May 11, 2025. [Online]. Available: https://csi-sigegov.org.in/1/1_369.pdf

[35] V. Kalesnikaite, M. I. Neshkova, and S. Ganapati, ‘Parsing the impact of E-government on bureaucratic corruption’, *Governance*, vol. 36, no. 3, pp. 827–842, 2023, doi: 10.1111/gove.12707.

[36] I. Pappel, V. Tsap, and D. Draheim, ‘The e-LocGov model for introducing e-Governance into local governments: an Estonian case study’, *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 2, pp. 597–611, 2019.

[37] I. Pappel, I. Pappel, and M. Saarmann, ‘Digital records keeping to information governance in Estonian local governments’, in *International Conference on Information Society (i-Society 2012)*, IEEE, 2012, pp. 199–204. Accessed: May 11, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6285076/

[38] T. Kangilaski, I. Pappel, M. Sihvonen, and M. Weck, ‘Cross-Border Communication and Service Provision within Silver Economy Domain: How to Sustain a Collaborative Platform for Seniors Services’, in *Human Factors, Business Management and Society*, AHFE Open Acces, 2022. doi: 10.54941/ahfe1002275.

[39] UNITED NATIONS DEPARTMENT FOR ECONOMIC AND SOCIAL AFFAIRS, *UNITED NATIONS E-GOVERNMENT SURVEY 2024*. S.l.: UNITED NATIONS, 2024.

[40] R. Traunmuller and M. Wimmer, ‘Processes-collaboration-norms-knowledge: signposts for administrative application development’, in *Proceedings 11th International Workshop on Database and Expert Systems Applications*, IEEE, 2000, pp. 1141–1145. Accessed: May 11, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/875170/?casa_token=qyln9wygQHwAAAAA:5ykuo5eGffu4WnSJh9JyNzPMBG89V1qI-2TWO7tzEyQZF6YYIQRlq9M1x3T3j0Z-k8ZFDs7_

[41] L. S. Flak, M. K. Sein, and Ø. Sæbø, ‘Towards a Cumulative Tradition in E-Government Research: Going Beyond the Gs and Cs’, in *Electronic Government*, vol. 4656, M. A. Wimmer, J. Scholl, and Å. Grönlund, Eds., in Lecture Notes in Computer Science, vol. 4656. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 13–22. doi: 10.1007/978-3-540-74444-3_2.

[42] M. Rebuglio, P. E. De Magistris, A. Carlin, and A. De Marco, ‘Implementing EDRMS in public procurement: a retrofit approach’, *Procedia Comput. Sci.*, vol. 239, pp. 541–546, 2024.

[43] L. Nguyen, P. Swatman, and B. Fraunholz, *EDMS, ERMS,ECMS or EDRMS : fighting through the acronyms towards a strategy for effective corporate records management*. Deakin University, 2007. Accessed: May 11, 2025. [Online]. Available: https://dro.deakin.edu.au/articles/conference_contribution/EDMS_ERMS_ECMS_or_EDRMS_fighting_through_the_acronyms_towards_a_strategy_for_effective_corporate_records_management/20556384/1

[44] D. O. Stephens, ‘The Sarbanes-Oxley act: records management implications’, *Rec. Manag. J.*, vol. 15, no. 2, pp. 98–103, 2005.

[45] A. A. Aziz, Z. M. Yusof, U. A. Mokhtar, and D. I. Jambari, ‘The determinant factors of electronic document and records management system (EDRMS) adoption in public sector: A UTAUT-based conceptual model’, in *2017 6th International Conference on Electrical Engineering and Informatics (ICEEI)*, Nov. 2017, pp. 1–6. doi: 10.1109/ICEEI.2017.8312413.

[46] A. Ab Aziz, Z. M. Yusof, U. A. Mokhtar, and D. I. Jambari, ‘The determinant factors of Electronic Document and Records Management System (EDRMS) adoption in public sector: a UTAUT-based conceptual model’, in *2017 6th International Conference on Electrical Engineering and Informatics (ICEEI)*, IEEE, 2017, pp. 1–6. Accessed: May 11, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8312413/?casa_token=OkkwWqOtK8cAAAAA:LyyoMVFiEBt9PuygwCFhlVligapF4bRrBk6G8hDBrLNzKBQ9JctVDSDuF-Gp4FeU6NMWt-mg

[47] S.-Y. Hung, K.-Z. Tang, C.-M. Chang, and C.-D. Ke, ‘User acceptance of intergovernmental services: An example of electronic document management system’, *Gov. Inf. Q.*, vol. 26, no. 2, pp. 387–397, 2009.

[48] S.-Y. Hung, K.-Z. Tang, C.-M. Chang, and C.-D. Ke, ‘User acceptance of intergovernmental services: An example of electronic document management system’, *Gov. Inf. Q.*, vol. 26, no. 2, pp. 387–397, 2009.

[49] K. Welch, ‘Implementing an EDRMS through a new records manager’s eyes’, *IQ RIMPA Q. Mag.*, vol. 32, no. 1, pp. 18–24, 2016.

[50] P. Joseph, ‘EDRMS 101: The basics’, *Inf. Rec. Manag. Annu. IRMA*, vol. 25, pp. 9–26, 2008.

[51] S. Butt, I. Pappel, and K. Oolu, ‘Implementation of Electronic Records Management Systems: Potential and Challenges a Case Study of the Water and Power Development Authority (WAPDA) in Pakistan’, 2021, pp. 629–639. doi: 10.1007/978-981-15-8354-4_63.

[52] C. J. Mutimba, ‘Implementation of electronic document and records management system in the public sector: a case study of the Ministry of Higher Education Science and Technology’, Master’s Thesis, University of Nairobi, 2014. Accessed: May 11, 2025. [Online]. Available: https://erepository.uonbi.ac.ke/handle/11295/76120

[53] J. Yläjääski, ‘DOCUMENT MANAGEMENT AS A PART OF PRODUCT LIFECYCLE MANAGEMENT’, Master’s Thesis, 2003.

[54] A. Meženin, ‘Dokumendihalduse lahendus korteriühistutele’, Master’s Thesis, 2021. Accessed: May 11, 2025. [Online]. Available: https://digikogu.taltech.ee/et/item/80b2fc56-fdc7-409a-b2a8-3410b68c2b50

[55] A. Karu, ‘Lõputööde haldamise süsteemi projekteerimine, realisatsioon ja juurutamine Tallinna Tehnikaülikooli informaatikainstituudis DHS Amphora baasil’, Master’s Thesis, 2015. Accessed: May 11, 2025. [Online]. Available: https://digikogu.taltech.ee/et/item/be4ba776-7ca2-46c6-834b-26710b591db7

[56] I. Pappel, K. Oolu, K. Saarevet, M. Lauk, and D. Draheim, ‘The Digital Archiving Process in Estonia – Assessment and Future Perspectives’, in *Future Data and Security Engineering*, T. K. Dang, R. Wagner, J. Küng, N. Thoai, M. Takizawa, and E. J. Neuhold, Eds., Cham: Springer International Publishing, 2017, pp. 472–481. doi: 10.1007/978-3-319-70004-5_34.

[57] S. Felt, I. Pappel, and I. Pappel, ‘An Overview of Digital Signing and the Influencing Factors in Estonian Local Governments’, in *Future Data and Security Engineering*, T. K. Dang, R. Wagner, J. Küng, N. Thoai, M. Takizawa, and E. Neuhold, Eds., Cham: Springer International Publishing, 2016, pp. 371–384. doi: 10.1007/978-3-319-48057-2_26.

[58] A. Rahno, ‘Vabariigi valitsuse töökorraldus ja infosüsteemid’, Accessed: May 11, 2025. [Online]. Available: https://www.tlu.ee/sites/default/files/Eestikeelne_esitlus_14102022.pdf

[59] R. Einberg, ‘Valitsuse Istungite InfoSüsteem Info system of Government meetings VIIS’. Accessed: May 11, 2025. [Online]. Available: https://slideplayer.com/slide/4654599/

[60] S. Lips, K. Aas, I. Pappel, and D. Draheim, ‘Designing an Effective Long-Term Identity Management Strategy for a Mature e-State’, in *Electronic Government and the Information Systems Perspective*, A. Kő, E. Francesconi, G. Anderst-Kotsis, A. M. Tjoa, and I. Khalil, Eds., Cham: Springer International Publishing, 2019, pp. 221–234. doi: 10.1007/978-3-030-27523-5_16.

[61] J. Pruša, ‘E-identity: Basic building block of e-Government’, in *2015 IST-Africa Conference*, IEEE, 2015, pp. 1–10. Accessed: May 11, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7190586/

[62] OECD, *G7 Mapping Exercise of Digital Identity Approaches*. OECD Publishing, 2024. doi: 10.1787/56fd4e94-en.

[63] V. Tsap, I. Pappel, and D. Draheim, ‘Factors Affecting e-ID Public Acceptance: A Literature Review’, in *Electronic Government and the Information Systems Perspective,* A. Kő, E. Francesconi, G. Anderst-Kotsis, A. M. Tjoa, and I. Khalil, Eds., Cham: Springer International Publishing, 2019, pp. 176–188. doi: 10.1007/978-3-030-27523-5_13.

[64] Information System Authority, ‘Usaldusteenused ja koostöö’. Accessed: May 11, 2025. [Online]. Available: https://www.ria.ee/riigi-infosusteem/elektrooniline-identiteet-ja-usaldusteenused/usaldusteenused-ja-koostoo

[65] V. Tsap, S. Lips, and D. Draheim, ‘Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia’, in *Electronic Government and the Information Systems Perspective*, A. Kő, E. Francesconi, G. Kotsis, A. M. Tjoa, and I. Khalil, Eds., Cham: Springer International Publishing, 2020, pp. 159–173. doi: 10.1007/978-3-030-58957-8_12.

[66] I. Pappel, I. Pappel, J. Tepandi, and D. Draheim, ‘Systematic Digital Signing in Estonian e-Government Processes’, in *Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVI: Special Issue on Data and Security Engineering*, A. Hameurlain, J. Küng, R. Wagner, T. K. Dang, and N. Thoai, Eds., Berlin, Heidelberg: Springer, 2017, pp. 31–51. doi: 10.1007/978-3-662-56266-6_2.

[67] V. Tsap, S. Lips, and D. Draheim, ‘eID Public Acceptance in Estonia: towards Understanding the Citizen’, in *Proceedings of the 21st Annual International Conference on Digital Government Research*, in dg.o ’20. New York, NY, USA: Association for Computing Machinery, juuni 2020, pp. 340–341. doi: 10.1145/3396956.3397009.

[68] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, ‘User Acceptance of Computer Technology: A Comparison of Two Theoretical Models’, *Manag. Sci.*, vol. 35, no. 8, pp. 982–1003, 1989.

[69] A. Peled, ‘The next computer revolution’, *Sci. Am.*, vol. 257, no. 4, pp. 56–64, 1987.

[70] I. Kong, M. Janssen, and N. Bharosa, ‘Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions’, *Gov. Inf. Q.*, vol. 41, no. 1, p. 101884, Mar. 2024, doi: 10.1016/j.giq.2023.101884.

[71] R. Matheus, R. Faber, E. Ismagilova, and M. Janssen, ‘Digital transparency and the usefulness for open government’, *Int. J. Inf. Manag.*, vol. 73, p. 102690, Dec. 2023, doi: 10.1016/j.ijinfomgt.2023.102690.

[72] M. Janssen, N. P. Rana, E. L. Slade, and Y. K. Dwivedi, ‘Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modelling’, *Public Manag. Rev.*, vol. 20, no. 5, pp. 647–671, May 2018, doi: 10.1080/14719037.2017.1305689.

[73] D. Duenas-Cid, T. Janowski, and R. Krimmer, ‘Trust and Distrust in e-Democracy’, in *Proceedings of the 23rd Annual International Conference on Digital Government Research*, in dg.o ’22. New York, NY, USA: Association for Computing Machinery, Sep. 2022, pp. 486–488. doi: 10.1145/3543434.3543637.

[74] R. Matheus, M. Janssen, and T. Janowski, ‘Design principles for creating digital transparency in government’, *Gov. Inf. Q.*, vol. 38, no. 1, p. 101550, Jan. 2021, doi: 10.1016/j.giq.2020.101550.

[75] ‘Anti-corruption and integrity’, OECD. Accessed: May 11, 2025. [Online]. Available: https://www.oecd.org/en/topics/anti-corruption-and-integrity.html

[76] S. Prabowo *et al.*, ‘Privacy-Preserving Tools and Technologies: Government Adoption and Challenges’, *IEEE Access*, vol. 13, pp. 33904–33934, 2025, doi: 10.1109/ACCESS.2025.3540878.

[77] S. Felt, ‘Amphora iseteenindusportaali eelanalüüs’, Master’s Thesis, 2020. Accessed: May 11, 2025. [Online]. Available: https://digikogu.taltech.ee/et/item/e88c2b6e-0bfd-4fe4-b576-327a8c82c551

[78] Deloitte Development LLC, ‘Procurement’s Path to Digitization’, WSJ. Accessed: May 11, 2025. [Online]. Available: http://deloitte.wsj.com/cio/procurements-path-to-digitization-1502337730

[79] N. Tšudakova, ‘Äriprotsesside modelleerimine ARIS tarkvaras ja juurutamine ettevõttes Enefit Power Varahalduse üksuses’, Master’s Thesis, 2021. Accessed: May 11, 2025. [Online]. Available: https://digikogu.taltech.ee/et/item/629f74e7-06c2-417c-abe6-e5ea63852c3a

[80] K. Mahmood, T. Kangilaski, and E. Shevtshenko, ‘Usage of Process Models for Quality Management System: A Case Study of Energy Company’, *Evol. Mech. Eng.*, vol. 1, Aug. 2018, doi: 10.31031/EME.2018.01.000510.

[81] V. Tsap, I. Pappel, and D. Draheim, ‘Key Success Factors in Introducing National e-Identification Systems’, in *Future Data and Security Engineering*, T. K. Dang, R. Wagner, J. Küng, N. Thoai, M. Takizawa, and E. J. Neuhold, Eds., Cham: Springer International Publishing, 2017, pp. 455–471. doi: 10.1007/978-3-319-70004-5_33.

[82] V. Weerakkody, M. Janssen, and R. El-Haddadeh, ‘The resurgence of business process re-engineering in public sector transformation efforts: exploring the systemic challenges and

unintended consequences', *Inf. Syst. E-Bus. Manag.*, vol. 19, no. 3, pp. 993–1014, Sep. 2021, doi: 10.1007/s10257-021-00527-2.

[83] M. Kaur, M. van Eeten, M. Janssen, K. Borgolte, and T. Fiebig, 'Human Factors in Security Research: Lessons Learned from 2008-2018', Mar. 24, 2021, *arXiv*: arXiv:2103.13287. doi: 10.48550/arXiv.2103.13287.

[84] E. Kangilaski, 'Digital Experience Design coursework', Haaga-Helia University of Applied Sciences, 2021.

[85] I. Benbasat and H. Barki, 'Quo vadis TAM?', *J. Assoc. Inf. Syst.*, vol. 8, no. 4, p. 7, 2007.

[86] S. Hong, J. Y. L. Thong, and K. Y. Tam, 'Understanding continued information technology usage behavior: A comparison of three models in the context of mobile internet', *Decis. Support Syst.*, vol. 42, no. 3, pp. 1819–1834, Dec. 2006, doi: 10.1016/j.dss.2006.03.009.

[87] J. S. Marcus, K. Sekut, and K. Zenner, 'A dataset on EU legislation for the digital world', Bruegel | The Brussels-based economic think tank. Accessed: May 11, 2025. [Online]. Available: https://www.bruegel.org/dataset/dataset-eu-legislation-digital-world

[88] M. Kutyłowski and P. Błaśkiewicz, 'Advanced Electronic Signatures and eIDAS – Analysis of the Concept', *Comput. Stand. Interfaces*, vol. 83, p. 103644, Jan. 2023, doi: 10.1016/j.csi.2022.103644.

[89] European Commission, 'eIDAS Levels of Assurance', European Comission. Accessed: May 11, 2025. [Online]. Available: https://ec.europa.eu/digital-building-blocks/sites/digital-building-blocks/sites/display/DIGITAL/eIDAS+Levels+of+Assurance

[90] Information System Authority, 'eIDAS-autentimistasemed'. Accessed: May 11, 2025. [Online]. Available: https://www.ria.ee/sites/default/files/documents/2022-11/eIDAS-autentimistasemed.pdf

[91] Information System Authority, 'EESTI VABARIIGI INFOSÜSTEEMIS AUTENTIMISLAHENDUSTELE KEHTIVAD NÕUDED'. Nov. 2022.

[92] European Union, 'Regulation - 910/2014 - EN - e-IDAS', EUR-Lex. Accessed: May 11, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng

[93] R. K. Ahmed, S. Lips, and D. Draheim, 'Signature in eCourt Systems', in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, Jul. 2020, pp. 352–356. doi: 10.1109/WorldS450073.2020.9210309.

[94] M. Erlich, 'e-Allkirjad Euroopas ja nende käsitlemine Eestis'. Jun. 2016.

[95] United Nations, 'About Us', United Nations. Accessed: May 11, 2025. [Online]. Available: https://www.un.org/en/about-us

[96] 'D-Money – Digital Mobile Money'. Accessed: May 11, 2025. [Online]. Available: https://d-money.dj/

[97] A. Fath-Allah, L. Cheikhi, R. E. Al-Qutaish, and A. Idri, ‘E-government maturity models: A comparative study’, *Int. J. Softw. Eng. Appl.*, vol. 5, no. 3, pp. 71–91, 2014.

[98] K. Layne and J. Lee, ‘Developing fully functional E-government: A four stage model’, *Gov. Inf. Q.*, vol. 18, no. 2, pp. 122–136, Jun. 2001, doi: 10.1016/S0740-624X(01)00066-1.

[99] ‘E-Gouvernement’. Accessed: May 11, 2025. [Online]. Available: https://www.egouv.dj/

[100] ‘Djibouti electronic visa platform’. Accessed: May 11, 2025. [Online]. Available: https://www.evisa.gouv.dj/applicant-api/#/

[101] S. D. Bejide, ‘Digimuutuste juhtimine e-Parlamendi juurutamisel: Djibouti juhtumiuuring’, 2023. Accessed: May 11, 2025. [Online]. Available: https://digikogu.taltech.ee/et/item/77709a70-aba2-4059-b116-cf6756d3c5d3

[102] Ansie, ‘Code du numérique’, Ansie. Accessed: May 11, 2025. [Online]. Available: https://www.ansie.dj/Pages/detailRubriquePages/54

[103] ‘About ITU’, ITU. Accessed: May 11, 2025. [Online]. Available: https://www.itu.int:443/en/about/Pages/default.aspx

[104] A. C. Quenum, ‘Djibouti Launches Pilot Phase of E-Permit for Construction Projects’. Accessed: May 11, 2025. [Online]. Available: https://www.wearetech.africa/en/fils-uk/news/djibouti-launches-pilot-phase-of-e-permit-for-construction-projects

[105] S. Njoya, ‘Djibouti Unveils e-Government Services to Streamline Governance and Permitting’. Accessed: May 11, 2025. [Online]. Available: https://www.wearetech.africa/en/fils-uk/news/tech/djibouti-unveils-e-government-services-to-streamline-governance-and-permitting

[106] UNICEF, ‘CRVS - Birth, Marriage and Death Registration in Djibouti’, UNICEF DATA. Accessed: May 11, 2025. [Online]. Available: https://data.unicef.org/crvs/djibouti/

[107] ‘dompdf/dompdf - Packagist’. Accessed: May 11, 2025. [Online]. Available: https://packagist.org/packages/dompdf/dompdf

[108] ‘Security Advisories - dompdf/dompdf - Packagist’. Accessed: May 11, 2025. [Online]. Available: https://packagist.org/packages/dompdf/dompdf/advisories

[109] Snyk, ‘jszip vulnerabilities’, Find detailed information and remediation guidance for vulnerabilities and misconfigurations. Accessed: May 11, 2025. [Online]. Available: https://security.snyk.io/

[110] S. Knightley, ‘Stuk/jszip’. Accessed: May 11, 2025. [Online]. Available: https://github.com/Stuk/jszip

[111] Snyk, ‘openpgp vulnerabilities’, Find detailed information and remediation guidance for vulnerabilities and misconfigurations. Accessed: May 11, 2025. [Online]. Available: https://security.snyk.io/

[112] 'openpgp', npm. Accessed: May 11, 2025. [Online]. Available: https://www.npmjs.com/package/openpgp

[113] OpenPGP, 'About', OpenPGP. Accessed: May 11, 2025. [Online]. Available: https://www.openpgp.org/about/

[114] J. Smith and F. Magnusson, 'The Project Management Triangle: a hidden framework? A qualitative study of ERP implementations in Sweden', Oct. 2015, Accessed: May 12, 2025. [Online]. Available: https://gupea.ub.gu.se/handle/2077/40815

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Erik Kangilaski

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Digitising Governance: A Practical e-Signature Solution for Djibouti's e-Cabinet”, supervised by Ingrid Pappel and Karin Oolu
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

12.05.2025

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Interview questions

Where do you work and what is your role?

How much would WebDesktop make your daily tasks easier and faster?

What would be the increase of efficiency in percentages?

How much does implementing WebDesktop requires changing processes and daily tasks? How much changes must be done?

Do you think AI could do the tasks you will continue to do in WebDesktop instead of you (correspondence)? Do you think that it would be possible?

With WebDesktop it should be easy to get statistics. What do you think what would be the best KPIs or statistics to get?

How much time it would take for that system to be used smoothly? How long to get it fully implemented?

How much of the daily tasks are currently paper-based and not digital?

Do you think, WebDesktop makes communication between units easier? How and why?

In case of simple correspondence what level of trust concerning eIDAS is needed (eIDAS scheme). Low, substantial, or high?

One solution would be solution using identification by certified email. In your opinion, would it be sufficient for simple correspondence? If no, why this is not sufficient?

There are additional document types needing signing as well. What of these can be low, substantial, high level trust needed?