Usability of Token-based and Remote Electronic Signatures: A User Experience Study

Ömer Ege, Mustafa Çağal, Kemal Bıçakcı

April 2025

Abstract

As electronic signatures (e-signatures) become increasingly integral to secure digital transactions, understanding their usability and security perception from an end-user perspective has become crucial. This study empirically evaluates and compares two major e-signature systems—token-based and remote signatures—through a controlled user experience study with 20 participants. Participants completed tasks involving acquisition, installation, and document signing using both methods, followed by structured surveys and qualitative feedback. Statistical analyses revealed that remote e-signatures were perceived as significantly more usable than token-based ones ($p < 0.001$), due to their minimal setup and platform-independent accessibility. In contrast, token-based signatures were rated as significantly more secure ($p < 0.01$), highlighting users' trust in hardware-based protection. Although more participants preferred remote e-signatures for document signing, the preference did not reach statistical significance ($p = 0.058$), indicating a trend toward favoring convenience in real-world scenarios. These findings underline the fundamental trade-off between usability and perceived security in digital signing systems. By bridging the gap between theoretical frameworks and real user experience, this study contributes valuable insights to the design and policy-making of qualified electronic signature solutions.

Keywords: Electronic signature, token-based authentication, remote signature, usability, perceived security, user experience, digital identity, multi-factor authentication

1 Introduction

The rapid advancement of digital technologies has transformed many sectors, and electronic signatures (e-signatures) have become a crucial element in digital identity verification, document authentication, and online transactions. E-signatures allow individuals and organizations to authenticate documents remotely, reducing the need for physical paperwork and enabling more efficient and cost-effective business practices. Qualified electronic signatures (QES) are

necessary for the safe authentication of individuals in a number of transactional e-government services [1]. Although the adoption of electronic signatures has increased significantly in various industries such as finance, e-commerce, and e-government, the usability of these systems remains a significant concern [7], [8]. Despite their security and legal validity, many users struggle with the complexity of the processes involved in acquiring, installing, and using electronic signature systems [2].

Qualified Electronic Signatures (QES) are increasingly critical for secure digital transactions; however, previous studies have largely focused on system design and legal frameworks rather than end-user experiences. Among these, the work of Çağal and Bıçakcı [2] provided a significant contribution by systematizing QES use cases and identifying usability challenges through cognitive walkthroughs. Their research primarily emphasized the conceptual categorization of different QES implementations and highlighted potential usability barriers based on expert evaluations.

Building upon this foundation, the present study aims to empirically assess and compare user experiences with token-based and remote electronic signature systems. By conducting a controlled user study involving real participants, this research moves beyond theoretical analyses and provides concrete evidence regarding the usability and security perceptions associated with these two signature methods. Thus, it addresses a critical research gap by transitioning from systematized design paradigms to user-centered experimental validation.

2 E-Signature Methods and Their Implementation

Electronic signatures (e-signatures) ensure authentication and verification of digital documents and data. According to the European Union's regulation *eIDAS* (Electronic Identification, Authentication, and Trust Services), e-signatures are classified as follows [5]:

- **Simple Electronic Signature (SES)**: Basic verification methods associated with digital documents (e.g., scanned signatures, email confirmations).
- **Advanced Electronic Signature (AES)**: A signature uniquely linked to the signatory, ensuring identity verification and document integrity.
- **Qualified Electronic Signature (QES)**: The highest legally recognized e-signature issued by a trusted service provider (TSP) based on qualified certificates.

Token-based electronic signatures typically fall under the category of qualified electronic signatures (QES). Remote electronic signatures can qualify as QES if they are created by a Qualified Trust Service Provider (QTSP) using secure signature creation devices (QSCD) or equivalent secure environments.

According to the eIDAS Regulation (EU No 910/2014), a remote signature meets the QES requirements if it ensures the same level of security as a local QSCD [5]. However, as of 2025, remote qualified electronic Signatures are not yet legally recognized in Türkiye. Local regulations require the use of physical qualified signature creation devices (QSCD) for QES compliance [11].

2.1 Remote Electronic Signatures

2.1.1 Definition and Technological Infrastructure

Remote electronic signatures allow users to authenticate and sign documents online without requiring physical devices. Identity verification is performed through methods such as

- Video identification,
- Mobile authentication (e.g., OTP-based verification),
- e-ID (electronic identity card) verification.

The signature creation data are securely stored in cloud-based infrastructures managed by trusted service providers, following standards such as ETSI TS 119 432 [19].

Advantages:

- Device-independent: Accessible via computers, tablets, or smartphones.
- No installation required: No software or driver installation is required.
- High accessibility: Can be used from anywhere.

Disadvantages:

- Security concerns: Vulnerable to phishing attacks and credential theft. Initiatives like the Cloud Signature Consortium have proposed standardized frameworks to enhance the security and interoperability of cloud-based electronic signature services [20].
- Limited legal recognition: Not legally accepted in all jurisdictions (e.g., not yet recognized in Türkiye).

2.1.2 Acquisition Process

1. **Application**: Users apply online through a trusted service provider.
2. **Identity Verification**: Users undergo verification via video call, biometric authentication, or bank eID integration.
3. **Certificate Issuance**: A remote signature certificate is generated and securely stored in the provider cloud.
4. **Activation**: Users receive an OTP or mobile notification to activate their signature.

2.1.3 Usage Process

1. **Signing**: The user uploads the document to the platform and authorizes the signature via OTP or biometric confirmation.
2. **Verification**: Signed documents are validated through TSPs or eIDAS-compliant verification systems.
3. **Management**: Users access and manage signed documents via the service provider's online portal.

2.2 Token-Based Electronic Signatures

2.2.1 Definition and Technological Infrastructure

Token-based electronic signatures use physical devices such as USB tokens, smart cards, or SIM cards to store cryptographic keys, which must be securely managed following key management standards such as NIST SP 800-57 [22]. Authentication is based on possession of the device and the entry of a PIN / password.

Advantages:

- High security: Requires both physical possession and user authentication.
- Strong legal validity: Recognized as QES in most legal frameworks.

Disadvantages:

- Requires setup: The installation of software and drivers is necessary.
- Device dependency: If the token is lost, the sign-in cannot be performed.

2.2.2 Acquisition Process

1. **Application**: Users apply through an authorized electronic certificate provider.
2. **Identity Verification**: Users verify their identity physically at a certification authority's office or via a notary.
3. **Device Issuance**: A USB token or smart card is issued to the user.
4. **PIN and Certificate Activation**: Users connect the device to their computer and set up their PIN.

2.2.3 Usage Process

1. **Signing**: Users connect the USB token or smart card, open the signing software, and enter their PIN to sign documents.
2. **Verification**: Signed documents can be verified via Adobe Trust Center or eIDAS-compliant systems.

3. **Device Management**: Users must reset their PIN if forgotten and renew certificates upon expiration.

3 Usability

Usability is regarded as one of the most crucial components of quality for every type of product [10]. Usability is regarded as one of the most crucial components of quality for every type of product [10, 14, 18]. The concept of usability is applicable to a variety of product types. Testing the usability of hardware and software products is a growing trend as the subject of usability engineering gains popularity every day [9]. Usability, in the context of e-signature systems, is essential not only for ensuring user satisfaction but also for promoting wider adoption. The complexity of these systems can lead to user frustration, errors, and potential security vulnerabilities. As electronic signatures are increasingly used for both personal and professional purposes, understanding the factors that influence their usability becomes crucial for improving their design and user experience. Previous research has highlighted that while many users perceive e-signatures as secure, there is often a disconnect between user perceptions and actual usability [2]. This paper aims to explore the usability of two commonly used types of e-signatures—token-based and remote e-signatures—by evaluating their acquisition, installation, and usage from a user experience perspective.

4 Related Work

The usability and adoption of electronic signatures, particularly Qualified Electronic Signatures (QES), have been explored in several studies. However, existing research predominantly focuses on technical, legal, or security aspects rather than end-user usability and comparative experiences between token-based and remote signing methods.

Cagal and Bicakci [2] analyzed the usability of Qualified Electronic Signatures (QES) by categorizing system designs and usage scenarios across Turkey and the European Union. Their study used cognitive walkthroughs to identify usability barriers in different QES implementations. While their work highlights system design flaws, it does not directly compare different QES methods (e.g., token-based vs. remote) in an experimental setting, which our study addresses.

Wang [3] examined the legal frameworks of electronic signatures across countries such as the United States, United Kingdom, Germany, and China. The study emphasized that legal inconsistencies hinder cross-border digital signature adoption. Although Wang's study is crucial for understanding regulatory challenges, it does not evaluate usability from an end-user perspective. Our research complements this by focusing on user experience rather than legal interoperability.

Truong and Minh-Tuan [4] studied the use of digital signatures supported by Hardware Security Modules (HSM) in Vietnam's e-invoicing system. Their

focus was mainly on enhancing security in a specific industry context. However, their study did not investigate usability challenges faced by end-users across different signature methods, which is the primary aim of our study.

Radka et al. [6] evaluated the implementation of the eIDAS regulation in the Czech Republic, particularly the legal and procedural aspects of QES adoption. Although their work sheds light on regulatory inconsistencies within the EU, it does not analyze the impact of these regulations on user experience or preferences between signature methods.

Lax et al. [8] discussed vulnerabilities in digital document signing systems and proposed solutions to enhance system robustness. While their work is significant for system designers, it does not address the user's practical experiences during acquisition, installation, and usage phases of e-signature systems, which our study explores.

Paz and Pow-Sang [10] conducted a systematic review on usability evaluation methods for software products. Their findings stress the importance of integrating usability engineering into system design. However, they do not specifically apply these principles to the context of electronic signatures, leaving a gap that our study aims to fill by applying usability evaluation specifically to token-based and remote e-signature systems.

Last et al. [12] designed and evaluated a prototype for signing digital documents using digital identity wallets. Their study focuses on improving the security and intuitiveness of signing processes through verified personal attributes, but does not directly compare different QES systems from a usability perspective as our study does.

ENISA (European Union Agency for Cybersecurity) [13] provided security guidelines for the appropriate use of qualified electronic registered delivery services. Although this guideline focuses on improving trust and interoperability in electronic communications, it does not address the comparative usability challenges between token-based and remote e-signatures that our study investigates.

Research Gap: While previous studies have addressed regulatory frameworks, security aspects, specific system designs, and general usability principles, there is a lack of empirical research comparing the usability and security perceptions of token-based and remote Qualified Electronic Signature systems through user-centered experiments. Our study addresses this gap by conducting a direct comparative usability evaluation with real users, analyzing acquisition, installation, usage experiences, and security perceptions systematically.

5 Methodology

To investigate the usability of token-based and remote electronic signatures, a user-centered study was conducted with 20 participants. The study aimed to evaluate the acquisition, installation, and usage processes of these two e-signature methods, with a particular focus on user experience and security perceptions. Participants were selected based on their diverse professional backgrounds, which allowed for a comprehensive analysis of usability across different

user groups.

The study was organized into three main phases: the acquisition phase, the installation phase, and the usage phase. Each phase was assessed through surveys designed to capture participants' experiences, preferences, and security perceptions.

5.1 Ethical Considerations

This study involving human participants was reviewed and approved by the Social and Human Sciences Scientific Research and Publication Ethics Board/Istanbul Technical University. The approval reference number is 571 dated 04 November 2024. All participants provided informed consent prior to their participation. Participants were assured that their responses would be anonymized, participation was voluntary, and they could withdraw from the study at any time without consequences.

5.2 Preliminary Survey: Participant Background and Expectations

Before engaging in the usability study, participants completed a preliminary survey to collect demographic information and assess their prior experience with electronic signatures. The survey included the following key questions:

- Age range (19-24, 25-29, 30-34, 35-39, 40-44, 45+)
- Gender (Male/Female)
- Education level (High School, Associate's, Bachelor's, Master's, Doctorate)
- Prior experience with electronic signatures (Yes/No)
- Type of electronic signature previously used (Remote, Token-based, Mobile, ID card-based)
- Satisfaction level with prior e-signature usage (1: Not satisfied at all - 5: Very satisfied)
- Self-reported proficiency in using computers and mobile devices (1: Not competent at all - 5: Very competent)
- Previous experience with digital identity verification (e.g., e-Government, banking authentication, etc.)
- Expected ease of e-signature acquisition (1: Should be very difficult - 5: Should be very easy)
- Open-ended question: If you have used an e-signature before, please describe your experience.

These responses provided valuable context regarding participants' expectations and familiarity with digital authentication processes.

5.3 Phase 1: Acquisition of E-Signatures

During the acquisition phase, participants were not required to individually register for a new token-based or remote e-signature system. Instead, electronic signatures that had been previously obtained by the researchers were used for the study.

This decision was made to protect participants' personal data and to avoid imposing financial costs on them, as acquiring an electronic signature would have required participants to share sensitive personal information with third-party providers and to cover the associated acquisition fees.

The acquisition processes were explained to the participants in detail by the researchers, simulating the key steps typically involved in real-world acquisition procedures. Specifically, the identity verification phase was reenacted by the researchers to demonstrate the authentication steps required for each e-signature method. Participants were informed about standard procedures, including application, identity verification, and credential activation, but were not required to perform these actions themselves.

Following the simulated acquisition process, participants completed an acquisition survey in which they rated statements on a 5-point Likert scale (1: Strongly Disagree - 5: Strongly Agree):

- Preference for an online acquisition process
- Perceived ease of acquiring a token-based e-signature
- Perceived ease of acquiring a remote e-signature
- Perceived security of the identity verification process
- Technical issues that would be expected during acquisition

Additionally, participants selected their preferred acquisition method based on the simulation and provided qualitative feedback on their impressions of the process.

5.4 Phase 2: Installation and Setup

In the installation phase, participants were required to install the necessary software for the token-based e-signature system, while remote e-signature users set up their profiles for signing documents online. The installation process was carefully observed to identify any issues related to system compatibility, user errors, and overall ease of installation.

Participants completed an installation survey, where they rated the following statements:

- Ease of installing the token-based e-signature software
- Clarity of installation instructions
- Preference for an e-signature system that does not require installation

Participants were also asked to choose their preferred installation method and explain their reasoning.

5.5 Phase 3: Usage and Security Perceptions

The usage phase involved participants signing documents using both the token-based and remote e-signatures. The signing process was evaluated based on factors such as ease of use, time taken to complete the task, the clarity of the interface, and any technical issues encountered.

Participants rated their experiences with both methods using the following criteria:

- Ease of signing documents using a token-based e-signature
- Speed of the token-based signing process
- Absence of technical issues with the token-based system
- Perceived security of token-based e-signatures
- Ease of signing documents using a remote e-signature
- Speed of the remote signing process
- Absence of technical issues with the remote system
- Perceived security of remote e-signatures

Participants also indicated which method they found more secure and more usable, providing justifications for their choices.

5.6 Task Design and Survey Mapping

In order to comprehensively assess the usability and security perceptions of token-based and remote electronic signatures, participants were assigned a series of tasks during the study. Each task was carefully designed to simulate real-world scenarios and was followed by targeted surveys to capture user feedback and experiences.

- **Task 1: Observation of E-Signature Acquisition Processes**

  Participants were provided with a detailed walkthrough of the acquisition processes for both remote and token-based electronic signatures. The researchers explained each step of the acquisition procedures, including application submission, identity verification, and certificate activation. As part of the simulation, participants were shown examples of the actual online forms required for the acquisition of remote and token-based electronic signatures. The process was demonstrated through screenshots of real-world form submission interfaces.

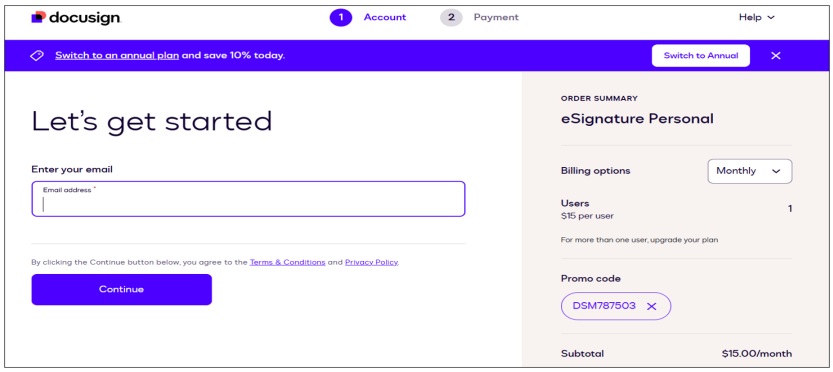


Figure 1: Example of an Online Application Form for Remote E-Signature Acquisition

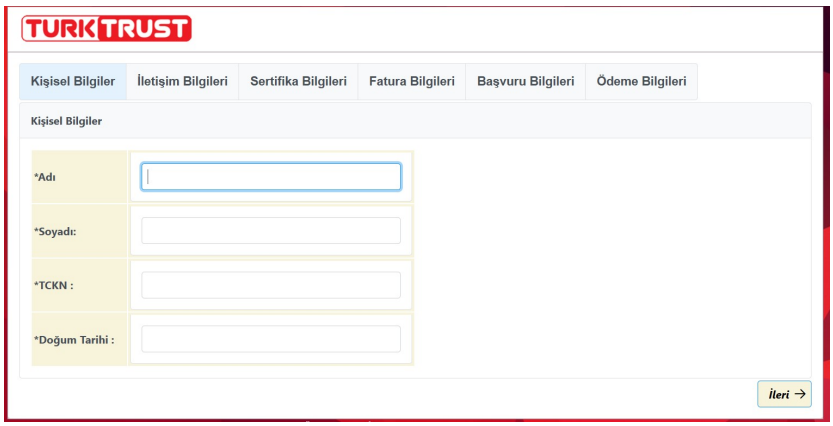


Figure 2: Example of an Online Application Form for Token-Based E-Signature Acquisition

The screenshots helped participants visualize the required data fields and steps involved in obtaining an e-signature, making the simulation more realistic. After the demonstration, participants were asked to complete the *Acquisition Survey* to evaluate the perceived ease, security, and potential difficulties associated with the acquisition phase.

Associated Survey: Acquisition Survey

- **Task 2: Token-Based E-Signature Software Installation**

  Participants were instructed to install the token-based e-signature software using the installation guide provided by the e-signature service provider. The guide detailed two major steps: the installation of the Palma software and the activation of the token.

  Following the installation, participants were guided through the activation

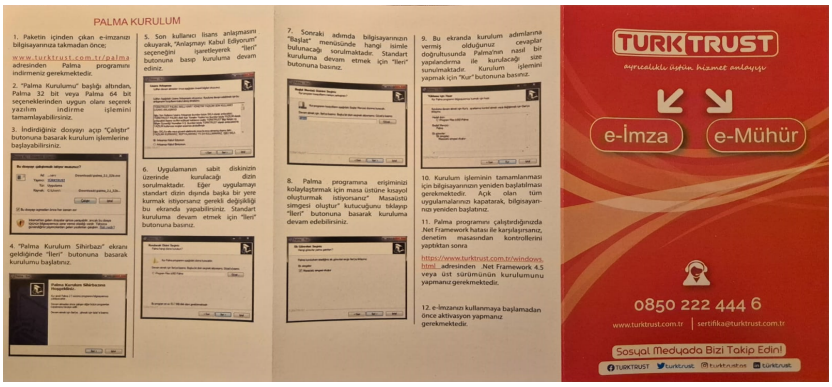


Figure 3: Installation Steps for Palma Software Required for Token-Based E-Signature

process, which included setting up the service agreement and configuring the necessary authentication settings.

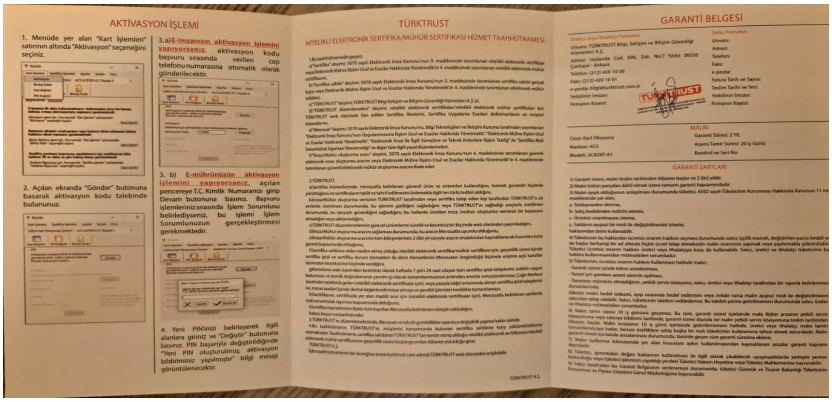


Figure 4: Activation Process and Service Agreement for Token-Based E-Signature

Participants were observed during the installation and activation tasks. Any technical difficulties or support needs were recorded by the researchers. Participants subsequently completed the *Installation Survey* to evaluate their experiences.

Associated Survey: Installation Survey

- **Task 3: Signing a Document with Token-Based E-Signature**

  Participants were tasked with signing a PDF document using a USB token device. They connected the token to their computers, launched the signature application (Palma), entered their PIN codes, and completed the

signing process.

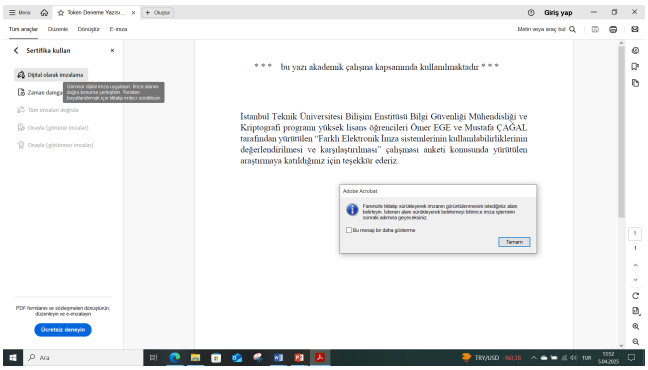


Figure 5: Interface for Signing a Document Using a Token-Based E-Signature

During this task, participants were observed for any difficulties related to accessing the token device, entering the PIN, or interacting with the signing software. Participants subsequently evaluated their experience by completing the *Token-Based Usage Survey*.

Associated Survey: Token-Based Usage Survey

- **Task 4: Verification of a Document Signed with Token-Based E-Signature**

  Participants were asked to verify the authenticity of a document they had signed using the token-based e-signature. They used Adobe Reader's signature verification functionality to check the validity of the electronic signature.

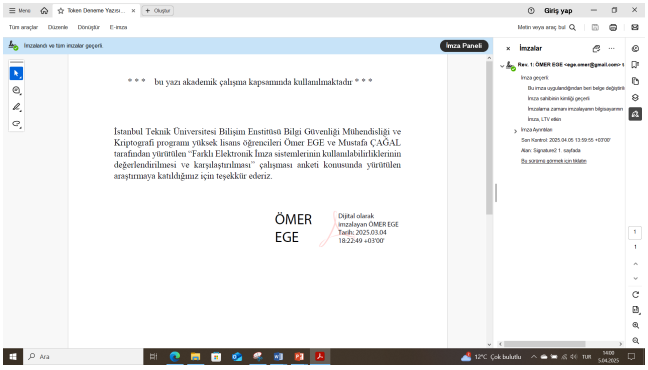


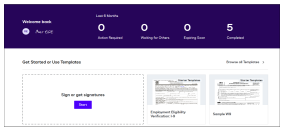
Figure 6: Verification of a Token-Based Signed Document in Adobe Reader

Participants were observed while performing the verification, and any difficulties in understanding verification indicators or system messages were noted.

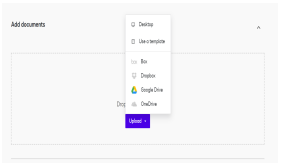
Associated Survey: Token-Based Usage Survey (Verification Section)

- **Task 5: Signing a Document with Remote E-Signature**

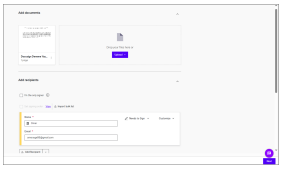
  Participants signed a PDF document using a web-based remote signature platform (DocuSign). They logged into the platform, uploaded a document, and completed the signing process by verifying their identity via a One-Time Password (OTP) sent to their registered mobile number.



(a) Step 1: Login to the Platform



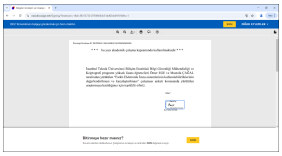
(b) Step 2: Upload the Document



(c) Step 3: Add Recipients

(d) Step 4: Place Signature Field

(e) Step 5: Check the status



(f) Step 6: Complete the Signature

Figure 7: Remote E-Signature Signing Steps (1–6)

Participants were observed for usability issues such as difficulties in navigating the platform, uploading files, or completing the OTP verification. Participants subsequently completed the *Remote Usage Survey*.

Associated Survey: Remote Usage Survey

- **Task 6: Verification of a Document Signed with Remote E-Signature**

  Participants verified the authenticity of a document signed via the remote signature platform using the platform's built-in verification tool. This process included checking the digital certificate details and ensuring the document integrity.

  Participants were observed while reviewing the verification information, and any misunderstandings or difficulties were recorded.

  Associated Survey: Remote Usage Survey (Verification Section)

At the conclusion of all tasks, participants completed a final comparative survey where they evaluated both signature methods based on usability, perceived security, installation complexity, and overall preference. Qualitative feedback was also collected to capture deeper insights into user experiences and expectations.

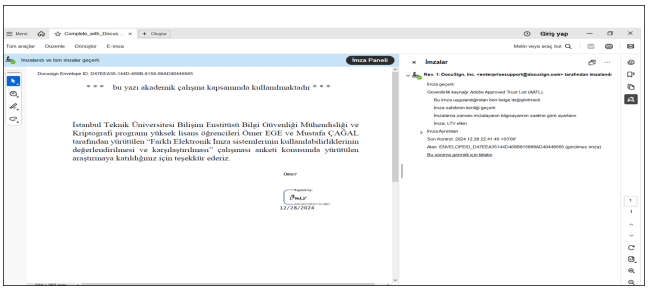


Figure 8: Verification of a Remote Signed Document on the Web Platform

5.7 Data Collection and Analysis

Data were collected through surveys completed by the participants at each phase of the study. These surveys included Likert-scale questions to assess the participants' satisfaction with the acquisition, installation, and usage processes. Participants were also asked to compare the two e-signature methods in terms of usability, security, and overall preference.

The results were analyzed using descriptive statistics and comparative analysis. Usability scores, error rates, and participant feedback were compared across both e-signature methods to determine which system provided a better overall user experience. Additionally, qualitative responses were examined to identify recurring themes and key concerns. This analysis aimed to contribute to the development of more user-friendly and secure e-signature systems that meet the needs of a wide range of users.

5.8 Hypotheses

Based on prior research and preliminary observations, the following hypotheses were formulated:

- **H1:** Remote electronic signatures will be perceived as more usable than token-based electronic signatures.
- **H2:** Token-based electronic signatures will be perceived as more secure than remote electronic signatures.
- **H3:** Participants will prefer remote electronic signatures over token-based signatures due to ease of acquisition and usage.

6 Results

This section presents the findings obtained from the user study conducted to evaluate the usability of token-based and remote electronic signatures. The results are categorized into three key areas: acquisition, installation, and usage, followed by an analysis of security perceptions and user preferences.

6.1 Participant Demographics

The study included 20 participants aged between 19 and 45+. Among them, 75% were male and 25% were female. Regarding educational background, 5% had an associate's degree, 65% held a bachelor's degree, 15% had a master's degree, and 15% had a doctorate.

Table 1: Participant Demographics

Demographic Category	Percentage (%)
Age 19–24	10.0
Age 25–29	10.0
Age 35–39	35.0
Age 40–44	20.0
Age 45+	25.0
Male	75.0
Female	25.0
Associate's Degree	5.0
Bachelor's Degree	65.0
Master's Degree	15.0
Doctorate	15.0

6.2 Acquisition Phase

Participants evaluated the ease of acquiring both token-based and remote e-signatures. The findings indicate that **75.0% of participants found the remote e-signature acquisition process easier** compared to token-based signatures. This preference is attributed to the fully online nature of the remote e-signature system, which eliminates the need for physical visits to a service provider or dealing with hardware tokens.

Furthermore, **75.0% of participants preferred an entirely online acquisition process**, highlighting the growing importance of digital accessibility and convenience in modern workflows.

The security perception during acquisition remained high for both methods, with an average rating of **4.7 out of 5** for the identity verification process.

6.3 Installation Phase

Installation complexity remained a significant factor influencing user experience. The findings reveal that **85.0% of participants preferred remote e-signatures** due to the absence of installation requirements. In contrast, token-based e-signatures necessitated software installation and configuration, which led to technical difficulties for many users.

The average difficulty rating for the token-based installation process was **3.2 out of 5**, with participants frequently reporting issues related to system compatibility, driver installation, and dependencies on external software such as Java or middleware applications. These challenges often resulted in increased setup time and reduced user satisfaction compared to the remote e-signature method.

6.4 Usage Phase

In terms of practical usage, **90.0% of participants found the remote e-signature process more accessible and user-friendly**. The simplicity of signing documents without requiring additional hardware was a key factor in this preference.

However, security perceptions varied between the two methods. **65.0% of participants considered token-based e-signatures more secure**, citing the need for a physical device as an additional layer of protection. Conversely, some participants expressed concerns about remote e-signatures, particularly regarding password-based authentication and the potential risk of unauthorized access.

Table 2: Survey Results for Usability and Security Perceptions

Survey Question	Remote E-Signature (%)	Token-Based E-Signature (%)
Found the acquisition process easy	75.0	25.0
Preferred an entirely online acquisition process	75.0	25.0
Rated identity verification security (Avg. 1-5)	4.7	4.55
Preferred installation process	85.0	15.0
Found installation process difficult (Avg. 1-5)	2.0	3.2
Found the usage process easy	90.0	10.0
Considered the method secure	20.0	80.0
Preferred method for signing documents	70.0	30.0

6.5 Task Performance Results

The task completion rates and task durations for each phase of the study were recorded to evaluate the operational feasibility and participant engagement. Table 3 summarizes the success rates and average time spent per task.
Analysis:

- **Task 1:** All participants successfully completed the observation of acquisition processes.

Table 3: Task Completion Rates and Average Time Measurements

Task	Completed Successfully (%)	Failed (%)	Average Time (minutes)
Task 1: Observation of E-Signature Acquisition Processes	100.0	0.0	N/A
Task 2: Token-Based E-Signature Software Installation	55.0	45.0	14.0
Task 3: Signing a Document with Token-Based E-Signature	100.0	0.0	N/A
Task 4: Verification of a Document Signed with Token-Based E-Signature	100.0	0.0	N/A
Task 5: Signing a Document with Remote E-Signature	100.0	0.0	N/A
Task 6: Verification of a Document Signed with Remote E-Signature	100.0	0.0	N/A

- **Task 2:** In the installation task, **55.0% of participants** successfully installed the token-based e-signature software without major issues, whereas **45.0%** encountered various technical difficulties.

  The primary challenges reported during the installation phase included:

  - **System Compatibility Issues:** Several participants faced difficulties identifying whether their computer was 32-bit or 64-bit, causing confusion in selecting and installing the correct driver versions.

    > One participant noted: *"I had no idea whether my computer was 32 or 64-bit. I downloaded the wrong driver twice and kept getting errors until I figured it out by trial and error. It felt like something only IT professionals could set up properly."*

  - **Software and Middleware Requirements:** Some participants struggled with missing or outdated middleware components such as Java or specific token management applications (e.g., Palma), leading to installation errors and delays.
  - **Incomplete Guidance:** Participants who lacked prior experience with token installations often needed to watch external instructional videos or rely on trial-and-error approaches, further prolonging the setup time.
  - **Cumulative Troubleshooting:** Participants encountering multiple minor issues (e.g., browser settings, security permissions) experienced compounded frustration, significantly extending the time required for successful installation.

  These challenges contributed to an average installation time of approximately **14 minutes**, which is relatively high for a standard software setup. This extended duration reflects the technical complexity of token-based systems, the variability in participants' device configurations, and the lack of streamlined, user-friendly installation processes.

  > One participant remarked: *"I thought it would be a simple setup, but it turned out to be way more complicated than I expected."*

- **Task 3 & 4:** All participants successfully signed and verified a document using the token-based e-signature. Minor technical issues such as delays in device recognition and occasional PIN entry errors were observed but did not prevent task completion.

- **Task 5 & 6:** Similarly, all participants were able to successfully sign and verify a document using the remote e-signature platform. The remote signing process was generally perceived as more intuitive, requiring fewer technical interactions and significantly reducing user errors.

Overall, the results highlight that while token-based e-signature systems offer strong security advantages, the installation phase poses a significant barrier to usability, especially for users with lower technical proficiency or unfamiliarity with system-level configurations.

6.6 User Preferences and Qualitative Insights

When asked about their preferred e-signature method, **70.0% of participants chose remote e-signatures**, whereas **30.0% opted for token-based e-signatures**.

Participants who preferred remote e-signatures primarily cited ease of access, the absence of installation requirements, and the ability to sign documents across multiple devices without physical dependencies. Some notable comments included:

- *"The ability to use it anywhere without extra hardware is a major advantage."* (Participant 8)
- *"I prefer a solution that does not require software installation or additional configurations. Installing programs sometimes causes security risks."* (Participant 13)
- *"Web-based signing feels faster and more practical. I can sign documents from any device without worrying about compatibility."* (Participant 3)
- *"Carrying an extra device increases the risk of losing it. I feel more comfortable with a method that does not require carrying anything."* (Participant 14)
- *"Program installation can lead to malware risks. I trust browser-based platforms more."* (Participant 17)

On the other hand, participants who preferred token-based e-signatures emphasized the perceived security benefits of physical devices. Their notable comments included:

- *"Having a physical device adds an extra layer of security. Even if my password is stolen, the attacker would still need the token."* (Participant 2)
- *"Token-based authentication provides more control over my electronic signature. I feel safer when a physical key is required."* (Participant 6)
- *"My signature key is not constantly exposed to the internet. That's why I prefer token-based solutions."* (Participant 19)

- *"Online platforms can be hacked. With a token, the risk is lower because it is in my possession."* (Participant 9)
- *"Even if remote signing is easier, I value security over convenience."* (Participant 11)

Overall, the qualitative insights reflect a trade-off between **usability and convenience** in remote e-signatures versus **enhanced perceived security** in token-based solutions.

This suggests that reducing the installation complexity could significantly improve user adoption rates for token-based e-signature systems.

6.7 Statistical Analysis of User Responses

In order to test the study hypotheses, statistical analyses were conducted based on users' survey responses.

6.7.1 Security Perception

Users were asked which e-signature method they found more secure. A chi-square test for goodness of fit revealed a statistically significant difference, $\chi^2(1, N = 20) = 7.20, p < 0.01$. A large majority of users (16 out of 20) perceived token-based e-signatures as more secure than remote e-signatures, strongly supporting Hypothesis 2 (H2).

6.7.2 Usability Perception

Users were asked which e-signature method they found more usable. A chi-square test indicated a statistically significant difference, $\chi^2(1, N = 20) = 12.80, p < 0.001$. A clear majority of users (18 out of 20) found remote e-signatures to be more usable than token-based e-signatures, strongly supporting Hypothesis 1 (H1).

6.7.3 Signing Method Preference

Users were also asked which e-signature method they would prefer for signing documents. A one-sided binomial test was conducted to evaluate whether significantly more users preferred remote e-signatures over token-based ones. The test result was marginally above the conventional threshold for statistical significance, $p = 0.058$, based on 14 out of 20 participants favoring the remote method. Although Hypothesis 3 (H3) was not fully supported, this finding indicates a notable trend toward significance, suggesting that convenience and ease of use may influence users' preferences in real-world signing scenarios.

Table 4: Summary of Statistical Tests

Evaluation	**Test**	**p-value**	**Result**
Security Perception	Chi-Square	< 0.01	Significant
Usability Perception	Chi-Square	< 0.001	Significant
Signing Preference	Binomial (One-sided)	0.058	Trend toward significance

7 Discussion

The findings of this study highlight key usability differences between token-based and remote e-signatures. The strong preference for remote e-signatures aligns with previous research emphasizing the importance of accessibility and ease of use in digital authentication systems.

7.1 Hypotheses Evaluation

The statistical analyses conducted support two out of the three initial hypotheses.

- **H1** (Remote e-signatures are perceived as more usable) was strongly supported, as a significant chi-square result ($p < 0.001$) indicated that a large majority of users found remote e-signatures more usable than token-based ones.
- **H2** (Token-based e-signatures are perceived as more secure) was also supported, with a statistically significant difference ($p < 0.01$) showing that most users perceived token-based e-signatures as offering higher security.
- **H3** (Users prefer remote e-signatures for signing documents) was not supported, as a one-sided binomial test revealed that the observed preference for remote e-signatures (14 out of 20 participants) did not reach conventional statistical significance ($p = 0.058$). Although the result falls just short of the commonly used 0.05 threshold, it indicates a notable trend toward significance, suggesting that users may be inclined to favor remote e-signatures for signing tasks under certain conditions.

These results clearly demonstrate that users differentiate strongly between the two systems in terms of usability and perceived security. Remote e-signatures were found to be significantly more usable, likely due to their minimal setup requirements and ease of access. Token-based e-signatures, on the other hand, were perceived as more secure, reflecting users' confidence in physical devices and hardware-backed protection. While the preference for remote e-signatures in signing tasks did not reach statistical significance, a notable trend toward significance was observed, suggesting that convenience may still play a critical role in user preferences. Taken together, these findings underscore the inherent

trade-off between usability and security, which should inform the design and deployment of electronic signature systems.

Demographic Factors and Signing Method Preference

Although the overall preference for remote e-signatures did not reach statistical significance, further exploratory analysis was conducted to examine how demographic variables—specifically education level, age group, and gender—might relate to signing method choices.

When grouped by education level, 5 out of 6 participants with postgraduate education (master's or doctorate) preferred remote e-signatures. Among those with undergraduate education or lower, the distribution was more balanced, with 9 favoring remote and 5 choosing token-based signing. This pattern may reflect differences in digital confidence and trust models; more educated users may prioritize accessibility and efficiency, while those with less experience may rely on tangible security cues such as physical tokens.

Age-related patterns were also observed. Both the youngest (19–24) and oldest (45+) participants mostly preferred remote signatures, while the 35–39 group showed a more even split between the two methods. This may suggest that middle-aged users weigh security and convenience more equally, or that generational familiarity with digital systems plays a role in shaping preferences.

Gender-based trends indicated that male participants (n=15) were more likely to prefer remote methods (11 remote, 4 token), whereas female participants (n=5) were nearly evenly divided (3 remote, 2 token). Some female participants also expressed concerns about technical complexity or the potential loss of physical devices, reflecting a nuanced relationship between perceived usability, risk, and device trust.

While no statistical inference was drawn due to the limited sample size, these preliminary findings suggest that individual preferences in secure digital signing are shaped not only by system characteristics but also by users' demographic backgrounds, security mindsets, and personal experiences with technology.

7.2 Impact of Technical Proficiency on Usability

Participants with higher technical proficiency completed token-based setup tasks faster and with fewer errors, suggesting that technical complexity remains a critical barrier for less experienced users. As one participant noted, *"I had to check whether my computer was 32-bit or 64-bit, which was confusing."* (Participant 12), highlighting how seemingly simple technical requirements can hinder successful installation.

Future implementations of token-based systems should focus on simplifying the setup process and offering clearer guidance to support a wider range of users.

Table 5: Signing Method Preference by Demographic Group

Group	Remote Preference	Token Preference	Total
Education Level			
Undergraduate	9	5	14
Postgraduate	5	1	6
Age Group			
19–24	2	0	2
25–29	1	1	2
35–39	4	3	7
40–44	3	1	4
45+	4	1	5
Gender			
Male	11	4	15
Female	3	2	5

7.3 Security vs. Usability Trade-off

The security versus usability trade-off was clearly evident in participants' feedback. This observation aligns with previous findings that authentication mechanisms often suffer from usability challenges, leading to user dissatisfaction and avoidance [23].

Remote e-signatures, while more usable and convenient, raised security concerns related to password protection. One participant expressed this by stating, *"Remote e-signatures are easier, but I always worry about my password being stolen."* (Participant 8). This finding aligns with earlier studies indicating that users often prioritize convenience over strict security measures [17].

Conversely, token-based signatures provided a higher sense of security through physical device possession but posed usability challenges, especially during setup and portability. Another participant commented, *"Even if it takes longer to set up, I trust a device I can hold in my hand."* (Participant 6). This user frustration is consistent with findings that users often rationally reject security measures perceived as excessively burdensome [24].

7.4 Implications for Adoption

Organizations prioritizing user convenience and scalability should consider remote e-signature systems, particularly when dealing with diverse user groups. Meanwhile, sectors with stringent security requirements may prefer token-based solutions despite their usability drawbacks.

Hybrid models that integrate strong authentication mechanisms into remote systems could help bridge the usability-security gap identified in this study. As one participant summarized, *"It would be perfect if I could have the ease of remote signatures with the security of a token."* (Participant 15).

7.5 Security Perception and Authentication

Several participants expressed concerns about password-based access being insecure and potentially vulnerable to unauthorized use. This concern was particularly evident in cases where no secondary code—such as a one-time passcode (OTP)—was requested during login, leading to the perception that entering a password alone was sufficient for accessing and signing documents.

In reality, platforms like DocuSign employ multiple layers of authentication to ensure document security. One-time passcodes are often used during identity verification before users can access or sign sensitive documents. These OTPs are typically delivered via SMS or phone call and remain valid for a limited time, usually around 10 minutes. This mechanism ensures that even if a password is compromised, unauthorized access is still prevented unless the attacker also has access to the user's phone.

Moreover, DocuSign and similar platforms support alternative authentication methods beyond passwords, including biometric verification, identity document validation, and knowledge-based authentication (KBA), depending on the configuration set by the document sender. Therefore, the belief that password entry is the sole gateway to digital signing contributes to a skewed sense of vulnerability. Addressing this gap in user understanding—through clear user communication and platform feedback—can help align perceived and actual security, ultimately improving trust in remote signature technologies.

8 Limitations and Future Work

8.1 Study Limitations

This study had a limited sample size of 20 participants, which may not fully represent broader user demographics. Additionally, all users were required to test both methods sequentially, potentially introducing bias in their evaluations.

8.2 Future Research Directions

Future studies should expand the sample size and include participants from diverse technical backgrounds. Additionally, evaluating hybrid models—such as biometric authentication in remote e-signatures—could provide deeper insights into balancing security and usability.

9 Conclusion

This study provides empirical insights into the usability and security perceptions of token-based and remote electronic signatures by analyzing acquisition, installation, and usage processes in a controlled user study.

The results indicate that:

- Remote e-signatures are perceived as significantly more usable than token-based e-signatures.
- Token-based e-signatures are perceived as significantly more secure than remote e-signatures.
- Although more participants preferred remote e-signatures for signing, this preference was not statistically significant.

Task performance analyses revealed that installation complexity was a key barrier for token-based e-signatures, affecting the overall user experience. In contrast, remote e-signatures required minimal setup and allowed participants to complete tasks more easily and intuitively.

Qualitative feedback further emphasized the usability-security trade-off, reflecting user preferences based on individual risk tolerance and situational needs.

This study extends the systematized framework established by Çağal and Bıçakcı [2] by providing empirical insights into how real users interact with token-based and remote electronic signature systems. While previous research identified potential usability barriers through expert-driven analyses, our findings offer concrete validation through user-centered experiments. The observed security-usability trade-off, user preferences, and task performance results not only confirm many of the theoretical challenges previously outlined but also reveal new nuances in user behavior and expectations.

Overall, this work complements prior system-level evaluations by emphasizing the importance of integrating usability engineering principles into the design of electronic signature systems. Future research should continue this trajectory by exploring hybrid models that balance security and usability, informed by both conceptual systematizations and empirical user studies.

9.1 Proposed Solutions for Improving Usability

To enhance both usability and security in e-signature systems, the following recommendations are proposed:

- Implement hybrid authentication models, combining biometrics and multi-factor authentication.
- Simplify the installation processes for token-based systems and explore web-based token authentication options.
- Develop user-centric interfaces with guided onboarding and real-time support features.
- Promote the consistent use of One-Time Passwords (OTP) as an additional security layer, especially in remote signing scenarios. OTPs offer a lightweight and widely familiar method to enhance trust without compromising usability.

Future work should expand the participant pool to include a more diverse user base and evaluate hybrid e-signature models that combine the strengths of both remote and token-based methods. Additionally, upcoming regulations such as the eIDAS 2.0 proposal are expected to facilitate wider adoption of remote Qualified Electronic Signatures across Europe [15]. Initiatives like the European Digital Identity Wallet Pilot aim to enhance cross-border digital identity verification and will likely impact the usability and adoption of remote e-signature systems [16]. Recent reports indicate that the adoption of electronic identification solutions across Europe continues to grow, as reflected in the Digital Economy and Society Index (DESI) 2023 [21].

Overall, this study underscores the need to design e-signature solutions that effectively balance security and usability to meet evolving user demands.

References

[1] K. Theuermann, A. Tauber ve T. Lenz, "Mobile-Only Solution for Server-Based Qualified Electronic Signatures," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, ss. 1-7, doi: 10.1109/ICC.2019.8762076.

[2] M. Cagal and K. Bicakci, "Evaluating the Usability of Qualified Electronic Signatures: Systematized Use Cases and Design Paradigms," arXiv preprint, 2024. Available: `https://arxiv.org/abs/2408.14349`.

[3] Wang, M. Do the regulations on electronic signatures facilitate international electronic commerce? A critical review. *Computer Law and Security Review.* **23**, 32-41 (2007), https://www.sciencedirect.com/science/article/pii/S0267364906000914

[4] M.-T. Truong and Q.-V. Dang, "Digital Signatures Using Hardware Security Modules for Electronic Bills in Vietnam: Open Problems and Research Directions," in *Future Data and Security Engineering: Big Data, Security and Privacy, Smart City and Industry 4.0 Applications*, Springer, 2020, pp. 469-475.

[5] European Parliament and the Council of the European Union. *Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).* Official Journal of the European Union, 2014.

[6] R. M. Pelikánová, E. D. Cvik, and R. MacGregor, "Qualified Electronic Signature - eIDAS Striking Czech Public Sector Bodies," *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, vol. 67, no. 6, pp. 1551-1560, 2019. doi:10.11118/actaun201967061551.

[7] Marshall, J. The relevance of electronic signatures in electronic transactions: An analysis of legal framework. *Journal Name.* **Volume Number** pp. Page Numbers (2025)

[8] Lax, G., Buccafurri, F. & And, G. Digital Document Signing: Vulnerabilities and Solutions. *Information Security Journal: A Global Perspective*. **24**, 1-14 (2015)

[9] Lodhi, A. Usability Heuristics as an assessment parameter: For performing Usability Testing. *2010 2nd International Conference On Software Technology And Engineering*. **2** pp. V2-256-V2-259 (2010)

[10] Paz, F. & Pow-Sang, J. Current Trends in Usability Evaluation Methods: A Systematic Review. *2014 7th International Conference On Advanced Software Engineering And Its Applications*. pp. 11-15 (2014)

[11] Information and Communication Technologies Authority (ICTA), Türkiye. Electronic Signature Law No. 5070 and related regulations. Available: `https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5070&MevzuatTur=1&MevzuatTertip=5`

[12] Y. Last, J. Geels, and H. Schraffenberger, "Design and Evaluation of a Prototype for Signing Digital Documents Using Digital Identity Wallets," arXiv preprint arXiv:2410.06857, 2024. Available: `https://arxiv.org/abs/2410.06857`

[13] European Union Agency for Cybersecurity (ENISA), "Security Guidelines on the Appropriate Use of Qualified Electronic Registered Delivery Services," 2017. Available: `https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-registered-delivery-`

[14] International Organization for Standardization, *ISO 9241-11:2018 - Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts*, ISO, 2018. Available: `https://www.iso.org/standard/63500.html`.

[15] European Commission, *Proposal for a Regulation on European Digital Identity (eIDAS 2.0)*, COM(2021) 281 final, 2021. Available: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281`.

[16] European Commission, *European Digital Identity Wallet Pilot Projects*, 2022. Available: `https://digital-strategy.ec.europa.eu/en/policies/european-digital-identity`.

[17] A. Sasse, S. Brostoff, and D. Weirich, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999, doi: 10.1145/322796.322806.

[18] J. Nielsen, *Usability Engineering*, Morgan Kaufmann, 1994.

[19] European Telecommunications Standards Institute (ETSI), *Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation*, ETSI TS 119 432 v1.1.1, 2019.

[20] Cloud Signature Consortium, *Cloud Signature Consortium White Paper*, 2016. Available: `https://cloudsignatureconsortium.org`.

[21] European Commission, *Digital Economy and Society Index (DESI) 2023*, 2023. Available: `https://digital-strategy.ec.europa.eu/en/policies/desi`.

[22] National Institute of Standards and Technology (NIST), *Recommendation for Key Management Part 1: General (Revision 5)*, NIST Special Publication 800-57, 2020.

[23] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," *IEEE Security & Privacy*, vol. 10, no. 1, pp. 96–102, 2012.

[24] C. Herley, "So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," in *Proceedings of the 2009 New Security Paradigms Workshop (NSPW)*, 2009.