Certificate Authority Capacity and Digital Signature Market Demand in Promoting Interoperability in Malaysia.

A.H. Azni[1,2*], *Farida Ridzuan*[1,2], *Sakinah Ali Pitchay*[1,2], *Najwa Hayaati Mohd Alwi*[1,2], *Maziahtusima Ishak*[3], and *R. Radzali*[1]

[1]Faculty Science and Technology, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Negeri Sembilan, Malaysia
[2]Cyber Security and System Research Unit, Faculty Science and Technology, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Negeri Sembilan, Malaysia
[3]Faculty of Major Language Studies, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Negeri Sembilan, Malaysia

Abstract. The adoption of digital signatures is becoming increasingly popular among Malaysian users due to its many advantages, including increased security, convenience, and cost savings. However, one of the challenges that users face is the lack of cross Certification Authority (CA) interoperability, which hinders the ability to use digital signatures across different platforms and services. To address this challenge, there is a growing need for promoting cross CA interoperability in Malaysia, which would enable users to use digital signatures seamlessly across various platforms and services. This paper aims to identify the CA capacity and digital signature market demand in promoting cross CA interoperability. This can be achieved through the qualitative interviews from CAs operating in Malaysia to gather views on interoperability across their platforms, the value and implications of such practice, and to establish the potential relationship between interoperability and increased Digital Signature efficiency and market demand. The interview data is analyzed using Atlas.ti and meta-analysis. Based on the result, the adoption of digital signatures and the promotion of cross CA interoperability are critical for advancing Malaysia's digital economy and enhancing the country's overall competitiveness. With the right infrastructure and policies in place, Malaysia can become a leader in the use of digital signatures and the promotion of cross CA interoperability, which would benefit both individuals and businesses alike.

1 Introduction

The Digital Signature Act 1997 (DSA 1997) and Digital Signature Regulations 1998 (DSR 1998) provide the licensing framework for providing digital signatures in Malaysia, including the type of services, the qualification requirements, applications, and the respective fees. The

* Corresponding author: ahazni@usim.edu.my

DSA 1997 defines a digital signature as an electronic method of authentication that uses a mathematical algorithm to validate the authenticity and integrity of a digital document or message [1]. The act also provides for the recognition of digital signatures as legally binding and enforceable in electronic transactions. On the other hand, the DSR 1998 further provides detailed requirements for the creation, verification, and storage of digital signatures. The regulations specify the technical standards that must be used to create and verify digital signatures, including the use of public key cryptography and the X.509 certificate format [2]. The acts also provide for the accreditation and regulation of Certification Authorities (CAs) that issue digital certificates and provide other services related to digital signatures. CAs are required to comply with strict security and operational standards and are subject to regular audits and inspections.

For a digital signature to be valid, enforceable, and effective in Malaysia, it must be certified and validated by licensed certification authorities. CA's main function is to issue a subscriber's certificate upon application as an identity to be listed in the certificate under the DSA 1997. Despite the presence of multiple CAs in Malaysia, the lack of interoperability among them creates challenges for users who need to use digital signatures across different platforms. Currently, a user who obtains a digital certificate from one CA cannot use the same certificate on another CA's platform [3]. This limits the flexibility and ease of use of digital signatures, which can be a barrier to wider adoption and usage of digital signatures in Malaysia. Therefore, there is a need to explore the feasibility of establishing interoperability among different CAs in Malaysia and identify potential strategies and approaches for achieving this goal. In this paper, the author wants to answer the following question:

i. What is the capacity of Certificate Authority to meet current and forecasted medium-term demand for interoperability?
ii. What is the relationship between increased digital signature efficiency and interoperability against potentially higher market demand?

Hypotheses H1 until H4 have been made to examine the relationship increased digital signature efficiency and interoperability against potentially higher market demand by using Atlas.ti.

H1: Facilitating Condition (Demand Capacity) positively influences the users' intention to use digital signature.
H2: Performance, ease of use and effort expectancy positively influences the users' usage intention to use digital signature.
H3: Initial trust in digital signature technology mediates the relationship between performance expectancy and usage intention.
H4: Government regulations moderate the relationship between facilitating conditions and usage intention.

2 Methodology

This study employs a qualitative research design, specifically utilising semi-structured interviews. The method described is commonly employed as a qualitative strategy to acquire a comprehensive comprehension of a particular subject [4]. The objective of this approach is to collect data from CAs by carefully selecting individuals who are directly involved in their operations. Figure 1 illustrated the research flow diagram.

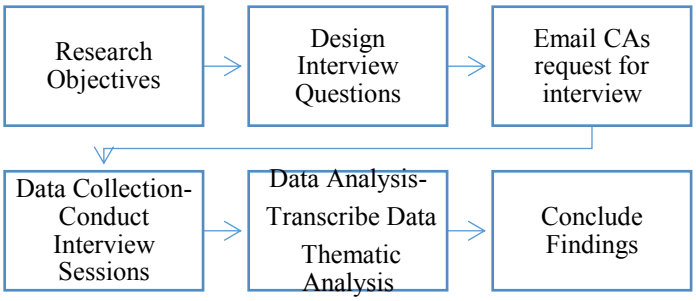

Fig. 1. Research Flow Diagram

2.1 Selection criteria used for interview subjects.

The aim of this study is to gather the in-depth understanding on interoperability challenges among CAs, therefore the qualitative method (interview) has been utilized. The selection of the representative for interview session will encompass individuals holding managerial and operational positions, so facilitating the acquisition of diverse perspectives on the issues at hand. Inclusion criteria for the participants were:

- Malaysians aged 18 years old and above,
- a minimum of 5 years of work experience in the area of digital certificate and digital signature.

A total of fifteen (15) interviewee /respondents from managers and technical level from three (3) CAs agreed to an invitation to participate in an interview session. Each participant was asked semi-structured, in-depth questions to elicit response corresponding to the research objective via face-to-face and online interviews.

2.2 Steps involved in conducting and transcribing interviews.

Invitation emails were sent to the Four (4) CAs and only three (3) responded and agreed for interview sessions. Face-to-face and online interviews were conducted with CAs and 15 managers as well as technical personal representing their companies were interviewed in August 2023.

Verbal consent for participation and audio-record the interview was obtained during the interviews. The researchers emphasised maintaining the anonymity of the participants and the confidentiality of the study findings. The researchers used triangulation as a strategy to allow for consistency checks across multiple sources and achieve an adequate representation of the phenomenon under study. The interview transcripts were analysed using thematic analysis to help the researcher pe-ruse the data, listen to the respondents' accounts, and reflect analytically on the findings.

In order to validate the semi-structured interview's content, the assessment made by various experts from Malaysian Communications and Multimedia Commission (MCMC) on different aspects of the interview was taken into account. Next, the interview data will be subjected to analysis utilising the software tool Atlas.ti. Atlas.ti facilitates the analysis of interview material by organising it thematically and generating summaries of the findings [5]. The findings hold significant im-portance in comprehending the interoperability difficulties and potential collaborative solutions from the standpoint of collective action. Table 1 below shows the interview questions asked during the data collection session. The participants were provided with questionnaires in advance of the interview session to facilitate their preparation for accurate responses. The following sections will discuss the results of the interview and analysis by Atlas ti.

Table 1. Questions on the Capacity and Market Demand among the CAs

No	Questionnaires on **Capacity and Market Demand among the CAs**
1	How do you ensure that Digital Signature (DS) services are available and can provide the necessary digital certificates to support the use of digital signature technology?
2.	How do you ensure that the necessary technical infrastructure is in place to support the adoption of digital signature technology?
3.	How do you ensure that the necessary security measures are in place to protect against unauthorized access or misuse of digital signature technology?
4.	What are the security mechanisms in place in digital signature technology to authenticate/verify sensitive documents or transactions?
5.	Does human resource (HR) contribute to meet the current and forecasted medium-term demand of Digital Signature (DS)? If Yes, can you elaborate on how HR can contribute to meet the current and forecasted medium-term demand of Digital Signature (DS)? If No, please elaborate more.
6.	Does cost/price play any role in meeting the demand for Digital Signature (DS)?
7.	Can you describe the training and support programmes provided to users to facilitate the adoption and effective use of digital signature technology?
8.	Can you describe any efforts to educate users about digital signature technology to improve their understanding and trust in its use?
9.	How do you envision the role of government agencies or regulatory bodies in promoting and facilitating interoperability among CAs?

3 Result and Discussion

CAs play a critical role in the digital security infrastructure by issuing digital certificates that verify the authenticity of websites, applications, and users. As technology continues to advance, the demand for secure digital transactions and communications is increasing. This paper presents initial findings on the capacity of the CAs in Malaysia to meet both the current and forecasted medium-term demand for digital certificates and interoperability. The assessment was conducted through interviews. The data on the infrastructure capabilities, security in place, resources, cost and training were collected through interview and analyzed using Atlas.ti.

3.1 What is the capacity of Certificate Authority to meet current and forecasted medium-term demand for interoperability?

Based on analysis using Atlas.ti, the capacity of the CA to meet current demand is shown in Table 2. The overall results show that the CAs are currently equipped to handle the current demand for digital certificates. It shows that the infrastructure of the CA emphasis on the three important aspect which are the high efficiency setup, backup protocols and key generation process. The infrastructure was equipped with hardware security to protect all private keys and backups for roots. Backups must also be kept offline for added security. Furthermore, the root, which is the master key generating all sub-roots must follow a stringent process for key generation, ensuring the right procedures are adhered to with evidence and witnesses [6].

The analysis also shows that the need for rigorous training, both in-house and overseas, underscores the complexity of digital signature technology. Such training ensures that personnel can handle challenges and stay updated with the latest advancements in the field. The focus on costs associated with digital signature, from user on boarding to system protection, highlights the economic challenges in widespread digital signature adoption [7]. Balancing security and cost is crucial for broader acceptance. The mention of organizations replacing physical operations with digital signature indicates a trend towards digital transformation, driven by both economic and operational efficiencies. Indirectly, the government plays a pivotal role in digital signature adoption, from providing licensing to promoting awareness. Collaborative efforts between CAs and government agencies can significantly boost digital signature adoption rates.

While CAs exhibit varying levels of scalability and automation, the majority are taking proactive steps to prepare for the forecasted medium-term increase in demand. By focusing on infrastructure enhancement, process optimization, training and collaboration, these CAs aim to ensure the continued issuance of secure and reliable digital certificates to meet the evolving needs of the digital landscape.

Table 2: Capacity of Certificate Authorities to meet current demand.

Variable		CA 1	CA2	CA3	Frequency
Infrastructure	High-Efficiency Setups	√	√	√	3
	Backup Protocols	√	√	√	3
	Key Generation Process	√	√	√	3
Security Mechanism	Key lifespan	√	√	√	3
	Awareness and Training	√	√	√	3
	Trust Verification	√	√	√	3
Human Resources	Training	√	√	√	3
	Industry growth	√	√	√	3
Cost and Adoption	Economic Considerations	√	√	√	3
	Digital Transformation	√	√	√	3
Regulatory Support and Government Involvement	Government's Role	√	√	√	3
	Legislative support	√	√	√	3

3.2 What is the relationship between increased digital signature efficiency and interoperability against potentially higher market demand?

The establishment of a clear relationship between increased Digital Signature (DS) efficiency and interoperability is crucial for understanding their potential impact on market demand and adoption. Finding from the interviews data, the relationship between increased digital signature (DS) efficiency and interoperability against potentially higher market demand and adoption of digital signatures have several key points as shown in Figure 2.

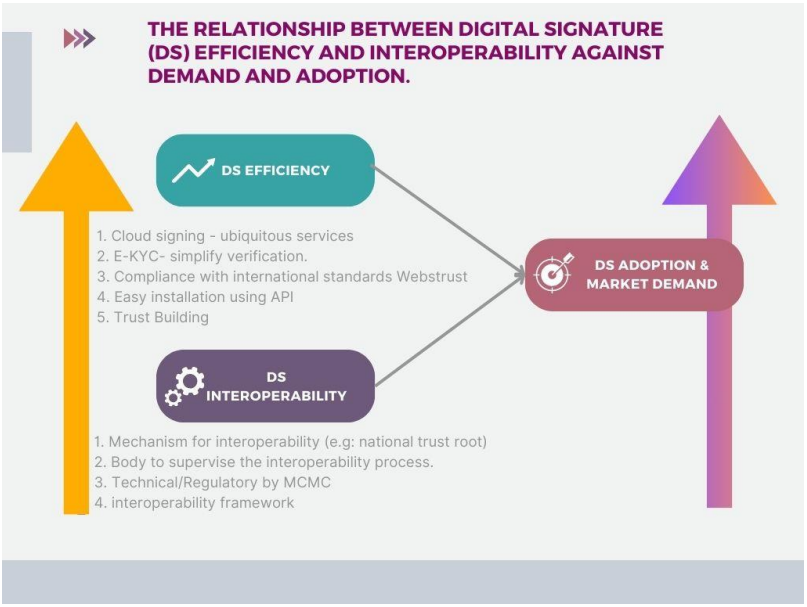

Fig. 2 : Relationship between Digital Signature Efficiency and Interoperability against Market Demand

In all three interviews, there is a consensus that digital signatures significantly improve efficiency and productivity in various tasks and workflows. They eliminate the need for physical signing, printing, and scanning of documents, enabling users to sign and approve documents from anywhere with an internet connection. Digital signatures also facilitate the enforcement of standard operating procedures (SOPs) by allowing for predefined signing sequences and timestamps, ensuring compliance with regulations.

CA1 mentions MAMPU's role as a hub for distributing certificates from different Certificate Authorities (CAs) in Malaysia. This interoperability ensures that certificates from various CAs can be used across different government agencies. CA2 highlights collaborations with other digital signature providers and the use of eKYC platforms to enhance verification methods. These collaborations contribute to interoperability in the digital signature ecosystem. CA3 mentions partnerships and technology integration to convert electronic signatures into digital signatures, emphasizing the importance of interoperability between different solutions.

All three interviews discuss efforts to promote the adoption of digital signature technology, such as workshops, roadshows, and awareness campaigns. here is a focus on approaching targeted organizations and individuals to demonstrate the benefits and use cases of digital

signatures. Digital signatures are perceived as highly useful and productive, leading to increased efficiency in various tasks, which can drive market demand and adoption [8].
Trust in digital signature technology is crucial for its adoption. The interviews mention various efforts to inform users about the benefits and limitations of digital signatures. These efforts include social media promotion, workshops, direct pitches to organizations, and proof of concept demonstrations. Compliance with international standards, such as WebTrust certification, is highlighted as a way to ensure trust in digital signature technology [9].

Based on the analysis, relationship diagram in Figure 2 have been made to identify the relationship between increased digital signature efficiency and interoperability against potentially higher market demand. Therefore, the data was consistent with H1, H2, H3 and H4.

4 Conclusion

The relationship between increased DS efficiency and interoperability is crucial for driving higher market demand and adoption of digital signatures. Efficient digital signature processes, coupled with interoperability between different providers and platforms, can enhance user experiences and productivity, ultimately leading to greater trust and adoption of this technology [10]. Efforts to promote digital signatures and build trust among users play a pivotal role in driving adoption within both government and private sectors. In conclusion, while there are comprehensive measures in place to ensure the security, availability, and adoption of DS technology, challenges persist. These challenges range from human-related vulnerabilities to economic considerations and the need for regulatory support. Addressing these challenges requires a multi-faceted approach, involving technological advancements, user education, industry collaboration, and regulatory support.

This research was funded by the Malaysian Communications and Multimedia Commission (MCMC) under the Digital Society Research Grants 2023 Cycle 1 (USIM/MCMC/FST/LUAR-K/42623).

References

1. Jamaluddin, M. N., Jamaludin, M. Z., Din, N. M., & Said, N. H. M. *Date time stamping with digital signature infrastructure*, in Student Conference on Research and Development (2002).
2. Hunt, Ray. *PKI and digital certification infrastructure*, in Proceedings. Ninth IEEE International Conference on Networks, ICON 2001, (2001).
3. Brands, Stefan. *Rethinking public key infrastructures and digital certificates: building in privacy*. Mit Press, (2000).
4. Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. *Systematic methodological review: developing a framework for a qualitative semi-structured interview guide.* Journal of advanced nursing, 72(12), 2954-2965, (2016).
5. Smit, B. *Introduction to ATLAS. ti for Mixed Analysis.* The Routledge Reviewer's Guide to Mixed Methods Analysis, 52, 331-42, (2021).
6. Backhouse, J., Hsu, C., & McDonnell, A. *Toward public-key infrastructure interoperability.* Communications of the ACM, 46(6), 98-100, (2003).

7. Kolodinsky, J. M., Hogarth, J. M., & Hilgert, M. A. *The adoption of electronic banking technologies by US consumers.* International Journal of Bank Marketing, 22(4), 238-259, (2004).
8. Earl, J., & Kimport, K. *Digitally enabled social change: Activism in the internet age.* Mit Press, (2011).
9. Gupta, A., Tung, Y. A., & Marsden, J. R. *Digital signature: use and modification to achieve success in next generational e-business processes.* Information & Management, 41(5), 561-575, (2004).
10. Patton, M. A., & Jøsang, A. *Technologies for trust in electronic commerce. Electronic Commerce Research*, 4, 9-21, (2004).