# Trusted Electronic Signature using Hybrid Public Key Infrastructures

Pitchya Tangsombatvichit[1], Utharn Buranasaksee[2], Sittikorn Mangkala[3], Ekachai Naowanich[4]

Faculty of Science and Technology
Rajamanagala University of Technology Suvarnabhumi
Phra Nakhon Sri Ayutthaya, Thailand
[1]pitchya.t@rmutsb.ac.th, [2]*utharn.b@rmutsb.ac.th, [3]sittikorn.m@rmutsb.ac.th, [4]ekachai.n@rmutsb.ac.th

*Abstract*—Electronic signatures make electronic transactions to be legally valid. One of the electronic transactions for government agencies is the issuance of electronic certificates. An electronic certificate is a document issued by government agencies to individuals or legal entities to certify the transactions from that government agency. The advantage of choosing a PDF document is that the document format supports storing documents and electronic signatures in a single file. This makes the process of creating, verifying, and keeping documents simple. However, government agencies are required to purchase the certificates from a certificate authority. The existing method is that government agencies need to purchase digital certificates for every user. This method has a high annual cost. Therefore, this paper proposed a method for generating e-signatures for electronic certificates by combining the certificates from certificate authority which is based on the centralized public key infrastructure, and the certificates from blockchain protocol which is based on a decentralized public key infrastructure. The proposed method does not only reduce the cost of the certificates from a certificate authority, but the signing process for the users is also more convenient while the electronic certificate remains compatible with the existing software.

***Keywords-public key infrastructure; electronic signature; blockchain***

## I. INTRODUCTION

Since electronic signature has been legalized in Thailand [1–4], the transactions that have been done electronically adopt the use of electronic signature into the process. Though the definition of electronic signature could be used with any electronic data [1], document signing is one of the most widely adopted use cases for electronic signature. According to the Act., the law does not specify any technology but defines only the outcomes and the properties of the electronic signature instead. However, to make the use of electronic signature compatible throughout the country, Electronic Transactions Development Agency (ETDA) has proposed the specification for the document signing of the government agency called Recommendation of Electronic Certificate Specification [5]. The recommendation contains the standards and the guidelines for the preparation of electronic certificates to be reliable, legally bound, legally enforceable, and can be used just like a conventional transaction method previously practiced. Therefore, the use of a Portable Document Format (PDF) has been recommended. The main advantages of using PDF documents are that the documents will be rendered the same across devices and platforms using any PDF reader software. In addition, the PDF document supports embedding digital signature which is an instance of electronic signature that make use of computer cryptography techniques.

Though the PDF file format has been standardized to ISO 32000-2[6], the initiation of the PDF was proprietary to Adobe Inc. As a result, the system of digital signature in PDF documents is built upon the centralized entities called Certificate Authorities (CAs). The CAs are made of the chain of trust in which the root certificate authorities are the top-most ones that have been trusted and their public keys are updated in every operating system. Each root certificate authority can define its subordinate by which the public key of the subordinate has been signed by the private key of the upper ordinate. In addition, the signing process allows the upper ordinate to specify the limitations such as allowing sub-ordinate creation or the duration of the trust. As a result, any entities that want to become the subordinate CA must pay the annual fee which makes the cost of the CA itself high. The sets of CAs, the chain of trust, and the procedures to maintain together are called public key infrastructure (PKI).

In Thailand, Thailand National Root Certification Authority (Thailand NRCA) [7] has been established by the Ministry of Digital Economy and Society and operated by the Electronic Transactions Development Agency. The main purpose of Thailand NRCA is the help organizations in Thailand purchase digital certificates at a more affordable price while maintaining the chain of trust from the root CA. However, as the Thailand NRCA has its own cost, the document signing certificates issued by Thailand NRCA are still annually charged.

According to ETDA recommendation [5], the electronic certificate should be signed in the name of the person who holds the position in the government agency and the name of the government agency. Furthermore, the signing process requires a digital certificate from CAs. The cost of the digital certificates can be seen as valuable if the number of users in the organizations is a few and there are many documents needed to be signed. On the other hand, using the certificate from CA can be costly and unpredictable if the number of users is high and dynamic, and when the users sign documents several times a year. For example, hospitals and patients, government agencies, and the people who contact those agencies.

Some implementations [8], [9] reduce the cost of digital certificates by skipping the use of digital certificates in the name of the person who holds the position in the government agency. This kind of implementation tries to mitigate the security issues by achieving a higher authenticator assurance level (AAL) by which the users are required to enter a one-time password (OTP) that typically has a 30-second slot from various channels. This not only makes the user experience complicated and slow, but the security of the system is still also prone to compromise by internal administrators.

Though there have been existing works that were proposed to create digital signatures for document signing using blockchain technology [10], the process of embedding digital signatures is not supported in conventional PDF software. To maintain the document's hash value, the document file was untouched. As the result, the existing system [10] produces the signing result in two separate files which are the original document and the Certificate of Completion (CoC). The original document is the electronic certificate issued by the government agency and the CoC contains the users' intention, the hash values of the original document, and the transaction identifiers of digital signatures that are stored in the blockchain. The existence of the document could be verified by the date and time of the blockchain transaction. While maintaining the security of the document signing process, implementing digital signatures using blockchain technology makes the process of creating, signing, verifying, and maintaining the document radically change from the traditional ecosystem.

To solve the problems, we propose a system that uses a hybrid public key infrastructure which is built on the centralized PKI and the decentralized PKI using blockchain technology. Using our method, the organization could greatly reduce the number of digital certificates that are required to purchase while the security of digital signature is not compromised, and the compatibility of PDF reader software remains the same.

The organization in this paper starts with the introduction of the problems of current electronic signatures in electronic certificates in Section 1. Then we discuss and analyze the related works in Section 2. After that, Section 3 discusses the proposed method of using hybrid public key infrastructures. In Section 4, we evaluate the cost model and compare the manipulation process of the PDF document in the proposed method to those in centralized PKI and decentralized PKI alone. Finally, the conclusion is drawn in Section 5.

## II. Related works

In this section, we first discuss the requirements for electronic certificates issued by government agencies in Thailand. Then, the existing works are categorized and analyzed.

### *A. Related Laws and Recommendations*

According to Electronic Transaction Act. [1–4], there are 3 types of electronic signatures. The first type is a general electronic signature, which is referred to as Section 9 e-signature. The Section 9 e-signature is electronic information that indicates the user's intention and has a mechanism to indicate the owner of the signature. The main problem of the general electronic signature is that the objector has no obligation to prove untrustworthy, but the claimant has the burden of proving trustworthy. The second type is a trusted electronic signature, which is referred to as Section 26 e-signature. The Section 26 e-signature is the electronic signature that allows the user to create the signature without the intervention of the server and the signature creation process has a mechanism to associate with the owner of the signature. This type of signature could be created using organizational-signed digital certificates or blockchain-based electronic signatures. The last type is the trusted electronic signature that relies on CAs, which is referred to as Section 28 e-signature. The Section 28 e-signature has the same requirements as the Section 26 does but requires the mechanism to associate the owner of the signature via a trusted organization such as CAs. In both the Section 26 and the Section 28 e-signature, the claimant does not have obligation to prove trustworthy, but the objector has a burden to prove the untrustworthy instead. The difference between these trusted e-signatures is that the Section 28 e-signature has a more solid mechanism to identify the owner of the signature without a doubt. When signing the document using a trusted e-signature, the process of identification and authentication of the information system must conform to both the identity assurance level (IAL) [11] and the authenticator assurance level (AAL) [12]. The information systems that implement trusted electronic signatures must pass the minimum of IAL 2.1 and AAL 2 [13].

An electronic certificate is a document issued by a government agency. Since the information types in the electronic certificate are mainly text, tables, and figures, ETDA recommends using PDF documents as the main file format for electronic certificates [5]. This is because the PDF file format is widely adopted, supports the electronic signature functionality, and supports the timestamp functionality. The timestamp function allows a document to embed the validated result of the electronic signature inside the document to ensure long-term archiving of the document. However, as the PDF file format evolves and many software vendors have developed their PDF software, some

PDFs may be correctly rendered in one software, but not in another. Therefore, Adobe Inc. introduced a new standard called PDF/A [14] which is for long-term archiving documents. The PDF/A standard limits the functionality inside the PDF file and enforces more strict rules to ensure renderability across PDF software. Therefore, the ETDA recommendations indicate that the electronic certificate must be in PDF/A format.

### B. *Existing works*

When the PKI was established on the Internet [15], the root CA are formed by a few organizations that are responsible for the security of the entire Internet. In the centralized PKI, these CAs involve a high cost of maintaining security, therefore the cost passes down to the sub-ordinate CAs. In the document signing context, the technology is mature and widely adopted. However, the cost may not be affordable in some cases especially when the number of users is high and dynamic, and each user signs several times a year.

After the emergence of the concept of trust in a trustless environment, blockchain becomes one of the most popular protocols that have extensively relied on asymmetric cryptography. There are two groups of existing studies. The first group focuses on building the infrastructure of the PKI [16–21] which aims to solve the problem of traditional PKI by adapting blockchain as a storage layer and using the public key as the identity of the user. The other group makes use of smart contracts on Ethereum-based blockchain [22–26] or UTXO blockchain [10]. The works in this group allow the users to sign the document without a trusted third party. However, none of them solve the problem of compatibility with conventional PDF software.

## III. HYBRID PUBLIC KEY INFRASTRUCTURES

To solve the problem of compatibility between traditional PKI and blockchain-based PKI, we proposed the extension from [10] by designing the system to use both traditional PKI and blockchain-based PKI. We extend 3 steps in addition to the previous work to make the document format that supports hybrid public key infrastructures. There are 3 steps for document preparation as shown in Figure 1. Step 1, the system performs conversion of another document format to a PDF document when the staff uploads the file. The staff is the person who is responsible for uploading and sending the electronic certificate and may not have a legal right to sign the document. Furthermore, the staff may send the same document multiple times. Once the document is chosen to be sent, in step 2, the system reserves the unique key for that send called send identifier. Then, the system converts the uploaded PDF document to PDF/A-3 format. The PDF/A-3 is one of the PDF/A standards that support file embedding into the PDF document. If the conversion is successful, the system signed the document using the digital certificate from CA. However, if the conversion is failed, the system will simply sign the PDF document using the digital certificate from CA. By using digital certificates from CA, the basic validation on proof of source could be verified using conventional PDF software. The digital certificate that the system uses is in the name of the government agency only.

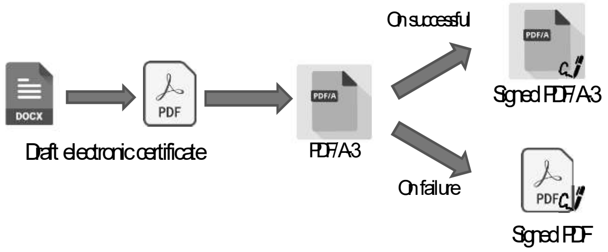


Figure 1. Document Preparation Process

Once the staff has chosen the recipients of the document, the system sends notifications to the user via various channels. The users will submit their intention through the web and confirm the intention using their private key. The confirmation is done by creating a blockchain transaction that refers to the hash value of the signed PDF document. The system remains no change to the signed PDF document. Therefore, every user that signs the same document and the send identifier will refer to the same hash value.

To generate the output that supports the digital signature at the user level without modifying the signed PDF document, we proposed a new structure of Certificate of Completion (CoC) as shown in Figure 2. The proposed CoC is the system-generated PDF/A-3 document in which the metadata file and the signed PDF document as an original document are embedded. The content of the CoC contains the document information, the user's intention, and the date/time of the signature. The metadata file is an XML file that contains verification information and the blockchain transaction. With the embedded metadata file, modifying or updating the CoC does not result in changing the hash value of the original document. In addition, the CoC supports 2 methods of document verification. The former method allows the user to upload the CoC through the web application, and the latter method allows the user to use the mobile application to scan the QR code provided inside the CoC. The former method is suitable when the user has a digital copy of the file while the latter method is suitable when the user has a printed copy of the document. In the verification process, the system checks for the integrity between the values stored in the database against those in the blockchain and provides the user with the validation result.

Once the CoC is requested, the system also signs the CoC using the digital certificate from CA. Though the CoC contains the blockchain transaction that indicates the existence of the PDF document and the users' electronic signature, the verification needs a few more steps that require user instruction. Therefore, to improve the user experience, the system also submits the signed CoC to the timestamp server to prove the existence of the CoC.

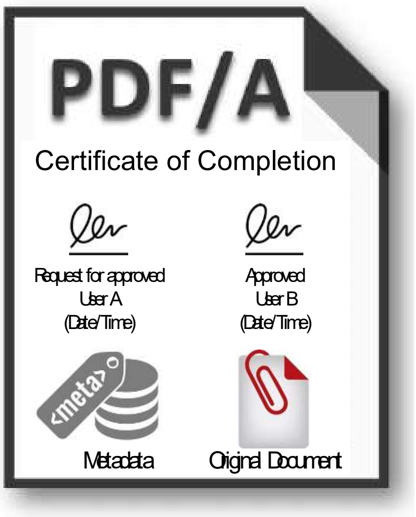
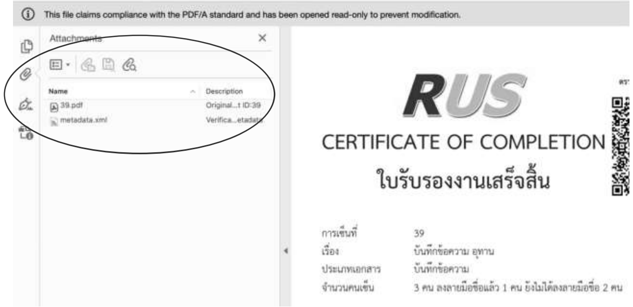


Figure 2. Proposed design of Certificate of Completion



This file claims compliance with the PDF/A standard and has been opened read-only to prevent modification.

| Name | Description |
|---|---|
| 39.pdf | Original...t ID:39 |
| metadata.xml | Verifica...etadata |

RUS

CERTIFICATE OF COMPLETION

ใบรับรองงานเสร็จสิ้น

| | |
|---|---|
| การเซ็นที่ | 39 |
| เรื่อง | บันทึกข้อความ อุทาน |
| ประเภทเอกสาร | บันทึกข้อความ |
| จำนวนคนเซ็น | 3 คน ลงลายมือชื่อแล้ว 1 คน ยังไม่ได้ลงลายมือชื่อ 2 คน |

Figure 3. Example CoC opened in conventional PDF software

Finally, the timestamped signed CoC is returned to the user. The user who has a digital copy of the file can use any conventional PDF software to open the CoC. Figure 3 shows the example of the CoC in which the metadata file and the signed original file are embedded.

When many government agencies are passing the electronic certificate, the CoC could be treated as an original document. As a result, the CoC as an embedded file is wrapped inside another CoC that is generated from another agency system. This nested structure makes the output CoC archivable as everything is packed in a single PDF file.

## IV. PROPOSED METHOD EVALUATION

In this section, we analyze the proposed method against the method using digital certificates from CA and the method that fully utilizes blockchain technology. The result is shown in Table 1.

TABLE I. COMPARISON OF PUBLIC KEY INFRASTRUCTURE IN DOCUMENT SIGNING

| Issues | Centralized Public Key Infrastructure | Decentralized Public Key Infrastructure | Hybrid Public Key Infrastructures |
|---|---|---|---|
| Cost model | High | No cost | Low |
| Association between the key and the owner | Widely accepted | Intra-oganization | Organization level is widely accepted |
| The private key can be used cryptographic device to achieve AAL3 | Not supported | Supported | Supported |
| Validation using conventional PDF software | Supported | Not supported | Supported |
| Archivable file | Single file | Multiple file | Single file |
| Timestamp Server | Required | Not supported | Supported |

### A. *Cost model*

While a digital certificate is required for each user in the centralized PKI, the hybrid method requires only one digital certificate. This greatly reduces the cost of the digital certificate. Furthermore, the cost between decentralized PKI and hybrid PKI is insignificant.

### B. *Association between the key and the owner*

Since the user needs to submit official documents and the public key to CA, the user information is stored in the digital certificate and certified by a trusted third party. Therefore, the association is widely accepted. On the other hand, the system that uses decentralized PKI stores e-KYC information in the database. The process of e-KYC could be trusted intra-organization. However, the hybrid PKI provides proof of source by a trusted third party as the digital certificate at the organization level is used.

### C. *Authentication requirement*

Since one of the properties of a multifactor cryptographic device is that the private key can neither be imported nor exported [12], the process of obtaining the digital certificate from CA requires the users to import their digital certificates to their devices. Therefore, the device cannot satisfy the cryptographic device's property. This makes achieving AAL 3 difficult as the OTP is still required. While the private key in the decentralized PKI can be randomly generated and remained encrypted in the device, the same key pair could be used as a multifactor cryptographic device to achieve AAL 3.

### D. *Validation process*

The validation process in centralized PKI can be done through conventional PDF software while the decentralized PKI does not provide a typical way to verify without building a custom application or system to verify the document. The hybrid PKI provides the bridge between those PKIs by which the user can validate the document through conventional PDF software. Once the validation is passed, the user may perform a deep validation on decentralized PKI can be done afterward.

### *E. Archiving process*

Since digital signature functionality is built in PDF format, the centralized PKI and the hybrid PKI could make a signed document in a single file. However, the system that uses the decentralized PKI cannot embed electronic signature data unless the file's hash value is changed.

### *F. Timestamp server*

In the centralized PKI, the signed document cannot prove its existence since the file creation unless the file was submitted to a timestamp server. A timestamp server keeps track of a unique identified value of each document and embeds the result in the PDF document. However, the timestamp functionality in the decentralized PKI is not supported as it makes the file’s hash value change. The system that uses decentralized PKI must provide an additional channel to verify the file's existence. However, the hybrid PKI supports the timestamp functionality on the CoC which is compatible with conventional PDF software as well as the date/time of the blockchain transaction when the document is deeply validated.

### *G. Implementation and Usage*

We have successfully implemented the document management system using the proposed method to create a Section 26 trusted e-signature for every user in the Faculty of Engineering and Architecture [1], the Rajamanagala University of Technology Suvarnabhumi. The system has 136 registered users which can save the cost of the certificate from CA 204,000 baht per year. The system has issued 15,138 trusted electronic signatures and saved the printed paper for 96,000 pages.

## V. Conclusion

In this paper, we have discussed the issues when using the centralized PKI to support the digital signature of electronic certificates and the shortcomings of decentralized PKI in the document signing context. Then, we proposed the hybrid PKI method that makes use of both centralized PKI and decentralized PKI. The proposed method greatly reduces the cost of digital certificates from CA while supporting the functionalities in a traditional ecosystem. The hybrid PKI improves the user experience in validation and archiving electronic certificates when compared to the use of electronic signatures that rely on the decentralized PKI only.

## References

[1] Electronic Transactions Development Agency, “Electronic Transaction Act. (1) 2001.” https://ictlawcenter.etda.or.th/laws/detail/eta-act-2544 (accessed Oct. 01, 2021).

[2] Electronic Transactions Development Agency, “Electronic Transaction Act. (2) 2008.” https://ictlawcenter.etda.or.th/laws/detail/eta-2-act-2551 (accessed Oct. 01, 2021).

[3] Electronic Transactions Development Agency, “Electronic Transaction Act. (3) 2019.” https://ictlawcenter.etda.or.th/laws/detail/eta-3-act-2562 (accessed Oct. 01, 2021).

[4] Electronic Transactions Development Agency, “Electronic Transaction Act. (4) 2019.” https://ictlawcenter.etda.or.th/laws/detail/eta-4-act-2562 (accessed Oct. 01, 2021).

[5] Electronic Transactions Development Agency, “ETDA Recommendation on ICT Standard for Electronic Transactions: Electronic Certificate,” 2017.

[6] PDF Association, “ISO 32000 (PDF) – PDF Association.” https://www.pdfa.org/resource/iso-32000-pdf/ (accessed Oct. 14, 2022).

[7] Thailand National Root Certification Authority, “Thailand National Root Certification Authority.” https://www.nrca.go.th/ (accessed Oct. 02, 2021).

[8] Fusion Solution Co.Ltd., “Design and Implement Digital E Signature Solution.” https://www.fusionsol.com/products/digital-signature-solution/ (accessed Oct. 02, 2021).

[9] Creden Asia Co.Ltd., “Creden.co.” https://creden.co/ (accessed Oct. 02, 2021).

[10] Buranasaksee U., Tangsombatvichit P., “Trusted Electronic Signature According to Thai Laws using UTXO Blockchain,” International Journal of Applied Computer Technology and Information Systems, vol. 11, pp. 26–31, 2021, Accessed: Oct. 14, 2022. [Online]. Available: http://203.158.98.12/actisjournal/index.php/IJACTIS/article/view/401

[11] Electronic Transactions Development Agency, “ETDA Recommendation on ICT Standard for Electronic Transactions: Digital Identity - Identity Proofing Requirements,” 2021.

[12] Electronic Transactions Development Agency, “ETDA Recommendation on ICT Standard for Electronic Transactions: Digital Identity - Authentication Requirements,” 2021.

[13] Electronic Transactions Development Agency, “ETDA Recommendation on ICT Standard for Electronic Transactions: Electronic Signature Guideline,” 2020.

[14] PDF Association, “ISO 19005 (PDF/A).” https://www.pdfa.org/resource/iso-19005-pdfa/ (accessed Oct. 14, 2022).

[15] R. Perlman, “Overview of PKI trust models,” IEEE Netw, vol. 13, no. 6, pp. 38–43, Nov. 1999, doi: 10.1109/65.806987.

[16] L. Axon and M. Goldsmith, “PB-PKI: A Privacy-aware Blockchain-based PKI,” 2017, doi: 10.5220/0006419203110318.

[17] E. Karaarslan, E. A.-I. C. Standards, and undefined 2018, “Blockchain based DNS and PKI solutions,” ieeexplore.ieee.org, Accessed: Oct. 14, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8515149/

[18] F. Li, Z. Liu, T. Li, H. Ju, H. Wang, and H. Zhou, “Privacy-aware PKI model with strong forward security,” International Journal of Intelligent Systems, 2020, doi: 10.1002/INT.22283.

[19] L. Axon, “Privacy-awareness in blockchain-based PKI,” 2015.

[1] https://fea.thaismartcontract.com

[20] K. Lewison and F. Corella, "Backing Rich Credentials with a Blockchain PKI *," 2016, Accessed: Oct. 14, 2022. [Online]. Available: https://pomcor.com/blog/

[21] A. Yakubov, W. Shbair, A. Wallbom, D. Sanda, and R. State, "A Blockchain-Based PKI Management Framework," 2018, Accessed: Oct. 01, 2021. [Online]. Available: https://orbilu.uni.lu/handle/10993/35468

[22] J. L. Ferrer-Gomila, M. Francisca Hinarejos, and A. P. Isern-Deyà, "A fair contract signing protocol with blockchain support," Electron Commer Res Appl, vol. 36, p. 100869, Jul. 2019, doi: 10.1016/J.ELERAP.2019.100869.

[23] L. Zhang, H. Zhang, J. Yu, and H. Xian, "Blockchain-based two-party fair contract signing scheme," Inf Sci (N Y), vol. 535, pp. 142–155, Oct. 2020, doi: 10.1016/J.INS.2020.05.054.

[24] M. Mut-Puigserver, M. Magdalena Payeras-Capella, and M. A. Cabot-Nadal, "Blockchain-based contract signing protocol for confidential contracts," Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA, vol. 2019-November, Nov. 2019, doi: 10.1109/AICCSA47632.2019.9035363.

[25] J. L. Ferrer-Gomila and M. F. Hinarejos, "A Multi-Party Contract Signing Solution Based on Blockchain," Electronics 2021, Vol. 10, Page 1457, vol. 10, no. 12, p. 1457, Jun. 2021, doi: 10.3390/ELECTRONICS10121457.

[26] Z. Wan, R. H. Deng, D. Kuo, and C. Lee, "Electronic Contract Signing without using Trusted Third Party," Proc West Mark Ed Assoc Conf, vol. 9408, pp. 386–394, 2015, doi: 10.1007/978-3-319-25645-0.