SUPPORTING STATEMENT
United States Patent and Trademark Office
Public Key Infrastructure (PKI) Certificate Action Form
OMB CONTROL NUMBER 0651-0045
April 2018

A. JUSTIFICATION

1. Necessity of Information Collection

The United States Patent and Trademark Office (USPTO) uses Public Key Infrastructure (PKI) technology to support electronic commerce between the USPTO and its customers. PKI is a set of hardware, software, policies, and procedures that provide important security services for the electronic business activities of the USPTO, including protecting the confidentiality of unpublished patent applications in accordance with 35 U.S.C § 122 and 37 CFR 1.14, as well as protecting international patent applications in accordance with Article 30 of the Patent Cooperation Treaty.

In order to provide the necessary security for its electronic commerce system, the USPTO uses PKI technology to protect the integrity and confidentiality of information submitted to the USPTO. PKI employs public and private encryption keys to authenticate the customer's identity and support secure electronic communication between the customer and the USPTO. Customers may submit a request to the USPTO for a digital certificate, which enables the customer to create the encryption keys necessary for electronic identity verification and secure transactions with the USPTO. This digital certificate is required in order to access secure online systems that are provided by the USPTO for transactions such as electronic filing of patent applications and viewing confidential information about unpublished patent applications.

For electronic commerce, particularly electronic filing, to be successful at the USPTO, the public must be confident that their information will be secure both during the transaction and while it is residence in the USPTO systems, that the integrity of the information will be assured, that their information will be released only to those who are authorized to access such information, and that measures are taken to authenticate the identity of persons submitting or trying to access the application and related information.

This information collection includes the Certificate Action Form (PTO-2042), which is used by the public to request a new digital certificate, the revocation of a current certificate, or the recovery of a lost or corrupted certificate. Customers may also change the name listed on the certificate or associate the certificate with one or more Customer Numbers. A certificate request must include a notarized signature in order to verify the identity of the applicant. The Certificate Action Form has an accompanying subscriber agreement to ensure that customers understand their obligations regarding the use of the digital certificate and cryptographic software. When generating a new certificate register to get a set of seven codes that will enable customers to recover a lost certificate online without having to contact USPTO support staff.

Table 1 provides the specific statutes and regulations authorizing the USPTO to collect the information discussed above:

Table 1: Information Requirements

IC Number	Requirement	Statute	Rule
1	PKI Certificate Request and Subscriber Agreement	35 U.S.C. §§ 2 and 122, Article 30 of the Patent Cooperation Treaty, and the Government Paperwork Elimination Act	37 CFR 1.14

2. Needs and Uses

Public access to secure USPTO online systems require USPTO customers to obtain a digital certificate. The public uses this information collection to request a new digital certificate, the revocation of a current certificate, or the recovery of a lost certificate. The USPTO uses the information in this collection to issue digital certificates and to process requests for certification revocation and recovery of lost certificates.

This information in this collection can be submitted using the Certificate Action Form (PTO-2042) to ensure that customers provide the necessary information for certificate requests. The accompanying subscriber agreement explains the regulations governing the use of the digital certificates and the software that creates and validates the encryption keys.

The information collected, maintained, and used in this collection is based on OMB and USPTO guidelines. This includes the basic information quality standards established in the Paperwork Reduction Act (44 U.S.C. Chapter 35), in OMB Circular A-130, and in the USPTO information quality guidelines.

Table 2 outlines how this collection of information is used by the public and the USPTO:

Table 2: Needs and Uses

IC Number	Form and Function	Form #	Needs and Uses

1	PKI Certificate Request and Subscriber Agreement	PTO-2042	• Used by the public to apply for a digital certificate, to request the revocation of a certificate, or to request recovery of an encryption key. • The Subscriber Agreement is used by the public to acknowledge acceptance of the regulations, terms, and conditions governing the use of digital certificates. • The Subscriber Agreement issued by the USPTO as a legally binding document indicating that the customer has read and agreed to the regulations governing the use of the digital certificate. • Used by the USPTO to issue a digital certificate and to process requests for certificate revocation, and key recovery. • Used by the USPTO to create the unique name needed for encryption key generation and certificate management. • Used by the USPTO to communicate with the customer about the certificate grant, revocation, or key recovery.

3. Use of Information Technology

PKI is a security technology that uses public/private key cryptography to enable secure online communication between the USPTO and its customers. PKI involves a package of hardware, software, policies, and procedures used to manage the implementation and use of the public/private keys that serve as the basis for the security services that PKI provides to the USPTO and its customers. These services include authentication, integrity, non-repudiation, confidentiality, and access control that are necessary to support secure communication for electronic commerce. This security is crucial to the creation of a trusted environment for transactions between the USPTO and its customers. PKI has also been identified as a security “best practice” for assurance in electronic commerce in both the commercial and Federal sectors.

The USPTO uses PKI technology to create the digital certificates and encryption keys. Customers may down the Certificate Action Form in PDF format from the USPTO Web site. The customer must complete and submit an original paper Certificate Action Form to the USPTO with a “wet” notarization signature after providing acceptable proof of identity. The Certificate Action Form must be mailed or hand delivered to the UPSTO; it cannot be faxed or submitted electronically because it requires an original notarized signature. The USPTO requires two forms of official identification, such as a driver’s license, U.S. passport, government ID badge, military ID card, or a current student ID card, and at least one of these forms of ID must include a picture of the customer. This physical proof of identity is necessary in order to tie the customer’s identity to internal access verification systems and would not be possible if the information were submitted electronically.

The certificate self-recovery features allows customers to recover a lost certificate without having to contact USPTO support staff. At key generation or in a later secure session, customers may download a set of single-use complex passwords that can be invoked later as part of the verification process to recover their own lost certificates online.

When the USPTO receives the request for a digital certificate, the customer information from the completed certificate action form is added to the PKI software database, which enables customers to create their user profiles and obtain their private encryption keys. After the USPTO processes the request for a digital certificate, a reference number and authorization code are sent to the customer separately. The authorization code is emailed to the customer, while the reference number is provided by U.S. mail and/or telephone contact with a representative from the USPTO Electronic Business Center. Upon receiving the reference number and authorization code from the USPTO, the customer may then use this information to create the encryption keys through the USPTO Web site. The PKI software is provided as a web browser applet that does not require a separate installation or software package.

The public and private keys are linked to each other and must be used as a pair. For example, the public key will only validate signatures that are created by its corresponding private signing key. The private key is kept private and is unique to a single user. The public key, however, is available to other users and is used to validate transactions marked by the sender's private key. The public key signature and encryption keys are incorporated in digital certificates issued by the USPTO Certificate Authority.

The USPTO expects to implement PKI security services for other automated information systems that are currently in use or in development to support additional electronic filing, processing, and commerce initiatives. PKI enables the USPTO to offer a secure environment for electronic communication and commerce with the patent application community, registered patent attorneys and agents, international business partners and Intellectual Property Offices, the Patent and Trademark Depository Libraries, USPTO employees and support contractors, and others with whom the USPTO does business requiring a guarantee of authenticity and confidentiality. By implementing PKI, the UPSTO has demonstrated to the patent and trademark community its commitment to the integrity, security, and confidentiality of its electronic transactions.

4. Efforts to Identify Duplication

This information is not collected elsewhere and does not result in a duplication of effort.

5. Minimizing Burden to Small Entities

This collection does not impose a significant economic burden on small entities or small businesses. The USPTO expects that the burden will be the same whether the application originates from a small entity or a large corporation because the digital certificates are granted only to individuals. The same information is required from every customer and is not available from any other source.

6. Consequences of Less Frequent Collection

This information is collected only when a customer applies for a digital certificate, requests that their certificate be revoked, or requests recovery of lost keys. This information is collected only when a customer requests the relevant service from the USPTO and could not be conducted less frequently. If the information were not collected, the USPTO would not be able to issue or revoke digital certificates, and subscribers would not be able to recover lost keys. If customers do not obtain a digital certificate, they cannot use secure electronic systems at the USPTO for filing patent applications or accessing confidential patent application information online.

7. Special Circumstances in the Conduct of Information Collection

There are no special circumstances associated with this collection of information.

8. Consultation Outside the Agency

The 60-Day Notice was published in the *Federal Register* on January 29th, 2018 (83 CFR 4037). The comment period ended on March 30th, 2018. One comment was received.

The comment contained four separate parts. Two of the four parts concurred with the utility of the information collected and the accuracy of the USPTO's burden hour estimates. The two remaining parts of the comment suggested more stringent methods of verifying the applicant's identity, such as notarizing at places at places that require both a photo identification and documents providing address (such as utility bills), or as an alternative to notarization, requiring the submission of credit card information to verify identity. These suggestions were not adopted because the additional information are unnecessary and the requirements would be burdensome to respondents.

The USPTO has long-standing relationships with groups from whom patent application data is collected, such as the American Intellectual Property Law Association (AIPLA), as well as patent bar associations, independent inventor groups, and users of our public facilities. Their views are expressed in regularly scheduled meetings and considered in developing proposals for information collection requirements. There has been no comments or concerns expressed by these or similar organizations concerning the time required to provide the information covered under this program.

9. Payment or Gifts to Respondents

This information collection does not involve a payment or gift to any respondent.

10. Assurance of Confidentiality

In order for the USPTO to issue or revoke a digital certificate or to recover a lost encryption key, the USPTO must collect personal information from customers. The USPTO uses the Certificate Action Form to collect the necessary personal information such as the customer's name, mailing address, phone number, and email address. The

information collected on the Certificate Action Form is used by the USPTO to authorize the creation and revocation of a digital certificate and to perform key recovery. The customer's name is used by the USPTO to create the distinguished name, which is a unique identifier used to identify a digital certificate holder. The email address is an essential piece of information for communicating with the customer. For the certificate self-recovery option, customers are provided with a set of single-use complex passwords to facilitate late online recover of a lost certificate. The USPTO issues these passwords to customers when they enter their email address to enroll in the self-recovery option. The email addresses and passwords are maintained in a secure database.

Due to security and privacy concerns regarding the digital certificates, private signing keys, and other private customer information, the USPTO does not plan to disseminate the information in this collection to the public in any form, paper or electronic. Distribution of this information could support attacks such as "identity spoofing" on the USPTO system, where someone could attempt to use another certificate holder's private information to revoke a certificate or recover a lost encryption key.

The personal information collected on the Certificate Action Form is stored in a system of record in which information can be retrieved by a personal identifier. This information is subject to the Privacy Act of 1974 and is covered by a system of records notice entitled "PAT/TM-16 USPTO PKI Registration and Maintenance System" that was published in the *Federal Register* on April 25, 2000 (65 Fed. Reg. 24178). The Certificate Action Form also has an associated Privacy Act Statement to inform applicants of the reasons for collecting the information and how the information they are providing will be used by the USPTO. Personal information collected from subscribers during the process of issuing or revoking digital certificates or during key recover is stored locally and handled as sensitive information. The USPTO stores paper records in lockable file cabinets or in file cabinets in secure areas. Electronic records are stored in secured premises with appropriate measures taken to limit electronic access to authorized personnel who require access for the performance of their official duties.

The information in this collection is treated confidentially to the extent allowed under the Privacy Act (5 U.S.C. § 552a), the Freedom of Information Act (5 U.S.C § 552), and the Government Paperwork Elimination Act (GEPA). The confidentiality of patent applications is governed by statute (35 U.S.C. § 122) and regulations (37 CFR 1.11 and 1.14). The USPTO has a legal obligation to maintain the confidentiality of the contents of unpublished patent applications and related documents. Applications for digital certificates and associated records for the renewal or suspension of digital certificates are considered to be related documents. This information is also protected under the mandates of the GEPA, which instructs agencies that the information collected from the public to facilitate the issuance of digital certificates cannot be used for any purpose other than facilitating communication with the USPTO and that only the information needed to process the request should be collected.

Since PKI is instrumental for secure electronic communication between the USPTO and its customers, the USPTO has implemented additional technological measures that protect the security and integrity of this information. The servers that house this information operate in security zones that are protected by firewalls. Server directories that are accessible from outside the USPTO do not contain information about patent applications who have USPTO digital certificates. These directories only contain information for those UPSOT entities that are authorized to correspond or interact with USPTO external customers or contacts. The encryption keys are protected by software on the USPTO servers and the customers' client machines. The authorization code and reference number required for subscribers to generate their encryption keys using the PKI software are sent to customers by separate methods for additional security. The USPTO sends the authorization code to the customer by email and the reference number is sent by regular U.S. mail or telephone.

11. Justification for Sensitive Questions

Noe of the required information in this collection is considered to be sensitive.

12. Estimate of Hour and Cost Burden to Respondents

Table 3 calculates the burden hours and costs of this information collection to the public, based on the following factors:

- **Respondent Calculation Factors**
  The USPTO estimates that it will receive approximately 3,825 total responses per year for this collection. None of the responses will be submitted electronically due to the notarization requirement.

- **Burden Calculation Factors**
  The USPTO estimates that it will take the public approximately 30 minutes (0.50 hours) to read the instructions and subscriber agreement, gather the necessary information, prepare the Customer Action Form, and submit the completed request.

- **Cost Burden Calculation Factors**
  The USPTO uses a professional rate of $438 per hour for respondent cost burden calculations, which is the media rate for intellectual property attorneys in private firms as shown in the 2017 *Report of the Economic Survey* published by the American Intellectual Property Law Association (AIPLA). The USPTO uses a paraprofessional rate of $145 per hour for respondent cost burden calculations, which is the average rate for paralegals as shown in the 2017 *National Utilization and Compensation Survey* published by the National Association of Legal Assistants (NALA). The USPTO estimates an estimate rate of $47.71 for independent inventors, which is based on the mean hourly rate for engineers according to the Bureau of Labor Statistics Occupational Employment Statistics (17-2199).

The USPTO estimates that the combined average hourly rate of these three estimates for all respondents is approximately $210.24.

Table 3: Burden Hour/Burden Cost to Respondents

IC Number	Item	Hours (a)	Estimated Annual Responses (b)	Burden (hrs/yr) (a) x (b) = (c)	Rate ($/hr) (d)	Total Cost ($/hr) (c) x (d) = (e)
1	PKI Certificate Request and Subscriber Agreement	0.50 (30 minutes)	3,825	1,912.50	$210.24	$402,084.00
	TOTAL	**- - - -**	**3,825**	**1,912.50**	**- - - -**	**0402,084.00**

13. Total Annual (Non-hour) Cost Burden

This collection has non-hourly cost burdens in the form of notarization fees paid by the public and associated postage costs for mailing items to the USPTO.

Notary Fees

The USPTO estimates that the cost of notarizing the Certificate Action Form is $6, based on the average of the State Notary Fee estimates published by the National Notary Association. All of the Certificate Action Forms are required to be notarized. There is a total of $22,950 per years in fee as outlined in Table 4 below.

Table 4: Non-hour Cost Burden to Respondents

IC Number	Information Collection Instrument	Estimated Annual Responses (a)	Notarization fee ($) (b)	Total non-hour cost burden (yr) (a) x (b) = (c)
1	PKI Certificate Request and Subscriber Agreement	3,825	$6.00	$22,950.00
Total	……..	**3,825**	……	**$22,950.00**

Postage Costs

The non-electronic items in this collection have associate first-class postage costs ($0.49) when submitted by mail. The Certificate Action Form cannot be faxed or submitted electronically because it requires an original notarized signature. The USPTO estimates that the postage costs per year will be $1,874.25.

Total

The total (non-hour) respondent cost burden for this collection is estimated to be $24,824.25 per year, which includes $22,950 in notarization fees and $1,874.25 in postage costs.

14. Annual Cost to the Federal Government

The USPTO employs government contractors to process the Certificate Action Forms.

The USPTO estimates that the cost of government contractors is $56.74, which is based on the Bureau of Labor Statistics' Occupational Employment Statistics for "Management Occupations" (11-0000).

The USPTO also estimates that it takes an employee 5 minutes (0.08 hours) to process the Certificate Action Form request.

Table 5 calculates the burden hours and costs to the Federal Government for processing this information collection:

Table 5: Burden Hour/Cost to the Federal Government

IC Number	Item	Hours (a)	Responses (yr) (b)	Burden (hrs/yr) (a) x (b) (c)	Rate ($/hr) (d)	Total Cost ($/hr) (c) x (d) (e)
1	PKI Certificate Request and Subscriber Agreement	0.08 (5 minutes)	3,825	191.25	$56.74	$10,851.53
	TOTAL	**- - - -**	**3,825**	**191.25**	**- - - - -**	**$10,851.53**

15. Reasons for Change in Burden

A. Changes in Collection since previous OMB approval in 2015

OMB previously approved the renewal of this information collection in April 2015. The current collection contains:

- 4,500 responses
- 2,250 burden hours
- $338,287.50 in respondent hourly cost burden
- $11,025 in annual (non-hour) costs

No changes have been made to this collection since its approval in April 2015.

B. Changes proposed in this request to OMB

The proposed collection, as outlined in the tables above, seeks to modify the existing collection. The proposed collection contains an estimated:

- 3,825 responses
- 1,192.50 burden hours
- $402,084 in respondent hourly cost burden
- $22,950 in annual (non-hour) costs

Changes in Respondent Cost Burden

The total respondent cost burden for this collection has increased by $64,516.50 (from $338,287.50 to $402,084) from the previous renewal of this collection in April 2015:

- Increases in estimated hourly rates. The 2015 renewal used an estimated rate of $150.35, which was developed from the estimated attorney rate of $389 per hour, the estimated paraprofessional rate of $125 per hour, and the estimated independent inventors rate of $30 per hour. For the current renewal, the USPTO is using updated hourly rates of $438 for attorneys, $145 for paraprofessionals, and $47.71 for independent inventors, which yields a revised average estimated rate of $210.24 per hour for respondents.

- Decreases in estimated burden hours. The total estimated burden hours have decreased from 2,250 in the 2015 renewal to 1,192.50 for the current renewal due to overall decreases in the hourly burden estimates for respondents and decrease in respondent estimates. The estimated number of respondents for this collection has decreased by 675 (from 4,500 to 3,825), which results in the estimated burden hours decreasing.

Changes in Responses and Burden Hours

For this renewal, the USPTO estimates that the annual responses will decrease by 675 (from 4,500 to 3,825) and the total burden hours will decrease by 1,057.50 (from 2,250 to 1,192.50) from the currently approved burden for this collection.

Changes in Annual (Non-hour) Costs

For this renewal, the USPTO estimates that the total annual (non-hour) costs will increase by $11,925 (from $11,025 to $22,95), with the increase due to agency estimates.

16. Project Schedule

The USPTO does not plan to publish this information for statistical use. However, patent and trademark assignment records are available to the public at the USPTO Public Search Facilities and on the USPTO Web site.

17. Display of Expiration Date of OMB Approval

The forms in this information collection will display the OMB Control Number and the expiration date of OMB approval.

18. Exception to the Certificate Statement

This collection of information does not include any exceptions to the certificate statement.

B. COLLECTION OF INFORMATION EMPLOYING STATISTICAL METHODS

This collection of information does not employ statistical methods.