SUPPORTING STATEMENT
United States Patent and Trademark Office
Public Key Infrastructure (PKI) Certificate Action Form
OMB CONTROL NUMBER 0651-0045
(February 2012)

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security services for the electronic business activities of the USPTO, including protecting the confidentiality of unpublished patent applications in accordance with 35 U.S.C. § 122 and 37 CFR 1.14, as well as protecting international patent applications in accordance with Article 30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 systems, 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the USPTO for transactions such as electronic filing of patent applications and viewing confidential information about unpublished patent applications.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 in 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 certificates and cryptographic software. When generating a new

certificate, customers 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.

This collection previously included the Certificate Self-Recovery Form as an information requirement. However, since the current online certificate recovery feature uses pre-generated access codes and does not collect any information from the customer, the Certificate Self-Recovery Form is being deleted from this collection.

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

Table 1: Information Requirements

Requirement	Statute	Rule
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

This collection allows for public access to secure USPTO online systems that require customers to obtain a digital certificate. This collection is used by the public 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 certificate revocation and recovery of lost certificates.

This collection contains the Certificate Action Form (PTO-2042), which is provided by the USPTO to ensure that customers submit 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 Quality Guidelines from Section 515 of Public Law 106-554, Treasury and General Government Appropriations Act for Fiscal Year 2001, apply to this information collection, and this information collection and its supporting statement comply with all applicable information quality guidelines, i.e. OMB and specific operating unit guidelines.

This proposed collection of information will result in information that will be collected, maintained, and used in a way consistent with all applicable OMB and 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

Form and Function	Form #	Needs and Uses
Certificate Action Form 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. • 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. • The Subscriber Agreement is used 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.

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 download 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" notarized signature after providing acceptable proof of identity. The Certificate Action Form must be mailed or hand delivered to the USPTO; 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 feature 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 applicant 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 USPTO 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 August 9, 2011 (76 Fed. Reg. 48807). The comment period ended on October 11, 2011. No public comments were received.

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 have 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 later online recovery 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 records 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 recovery 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 (GPEA). The confidentiality of patent applications is governed by statute (35 U.S.C. § 122) and regulation (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 GPEA, 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 to 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 applicants who have USPTO digital certificates. These directories only contain information for those USPTO 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 by regular U.S. mail or telephone.

11. Justification for Sensitive Questions

None 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 4,500 responses per year for this collection. None of the responses will be submitted electronically due to the notarization requirement.

- **Burden Hour Calculation Factors**
  The USPTO estimates that it will take the public approximately 30 minutes (0.5 hours) to read the instructions and subscriber agreement, gather the necessary information, prepare the Certificate Action Form, and submit the completed request.

- **Cost Burden Calculation Factors**
  The USPTO uses a professional rate of $340 per hour for respondent cost burden calculations, which is the median rate for attorneys in private firms as shown in the 2011 *Report of the Economic Survey* published by the American

Intellectual Property Law Association (AIPLA). The USPTO uses a paraprofessional rate of $122 per hour for respondent cost burden calculations, which is the average rate for paralegals as shown in the 2010 *National Utilization and Compensation Survey* published by the National Association of Legal Assistants (NALA). The USPTO uses an estimated rate of $30 per hour for independent inventors.

The USPTO expects that approximately 70% of the submissions for this information collection will be prepared by paraprofessionals, 15% by attorneys, and 15% by independent inventors. Using those proportions and the estimated rates above, the USPTO estimates that the average rate for all respondents will be approximately $141 per hour.

Table 3: Burden Hour/Burden Cost to Respondents

Item	Hours (a)	Responses (yr) (b)	Burden (hrs/yr) (c) (a) x (b)	Rate ($/hr) (d)	Total Cost ($/yr) (e) (c) x (d)
Certificate Action Form (including Subscriber Agreement) (PTO-2042)	0.50	4,500	2,250	$141.00	$317,250.00
Totals	**---------**	**4,500**	**2,250**	**----------**	**$317,250.00**

13. Total Annual (Non-hour) Cost Burden

The total (non-hour) respondent cost burden for this collection is estimated to be $11,025 per year, which includes $9,000 in notarization fees and $2,025 in postage.

Notarization Fees

There are costs associated with the notarization requirement for authenticating the signatures on the Certificate Action Form, for a total of $9,000 per year:

- 4,500 responses for Certificate Action Forms, at $2 each for notarization: $9,000

Postage Costs

The non-electronic items in this collection have associated first-class postage costs when submitted by mail, for a total of $2,025 per year:

- 4,500 Certificate Action Forms, at $0.45 postage: $2,025

The Certificate Action Form cannot be faxed or submitted electronically because it requires an original notarized signature.

14. Annual Cost to the Federal Government

Certificate Action Forms are processed at the USPTO by government contractors at an average cost to the USPTO of $60 per hour. The USPTO estimates that it takes approximately 5 minutes (0.08 hours) to process a Certificate Action Form request.

Table 4 calculates the burden hours and costs to the Federal Government for processing this information collection:

Table 4: Burden Hour/Burden Cost to the Federal Government

Item	Hours (a)	Responses (yr) (b)	Burden (hrs/yr) (c) (a) x (b)	Rate ($/hr) (d)	Total Cost ($/yr) (e) (c) x (d)
Certificate Action Form (including Subscriber Agreement) (PTO-2042)	0.08	4,500	360	$60.00	$21,600.00
Totals	**----------**	**4,500**	**360**	**----------**	$21,600.00

PKI also involves additional costs to the USPTO of approximately $450,000 per year for software and license fees. **Therefore, this information collection has a total government processing cost of approximately $471,600.**

15. Summary of Changes in Burden Since the Previous Renewal

Interim Approvals

- Notice of Action, August 2010: Revision of the Certificate Action Form (PTO-2042) to reflect revised procedures for associating PKI certificates with Customer Numbers. Under the new procedure, associating a practitioner with a Customer Number will automatically associate that practitioner's existing PKI certificate with the Customer Number, eliminating the need to submit a separate Certificate Action Form. Decreased burden by 206 responses, 103 hours, and $461 in annual (non-hour) costs.

Changes from the 60-Day *Federal Register* Notice

- **Increases in estimated responses and burden hours.** The total estimated annual responses and burden hours for this renewal have increased from the 1,857 responses and 929 burden hours published in the 60-Day *Federal Register* Notice to the revised estimates of 4,500 responses and 2,250 burden hours based on the availability of updated data.

- **Increases in estimated hourly rates.** The estimated hourly rate of $340 for attorneys used by the USPTO in this submission comes from the 2011 *AIPLA Report of the Economic Survey*. The 60-Day *Federal Register* Notice used the

previous attorney rate of $325 from the 2009 report to calculate the hourly cost burden for respondents. Due to the updated attorney rate and the increase in total burden hours noted above, the total annual respondent cost burden for this collection has been increased from the $129,131 that was reported in the 60-Day *Federal Register* Notice to $317,250.

- **Increase in annual (non-hour) cost burden.** The total estimated annual (non-hour) cost burden for this collection has been increased from the $4,531 that was reported in the 60-Day *Federal Register* Notice to $11,025. This revised estimate is due to the increased estimate for total annual responses, which consequently increased the total notarization fees and postage costs. Total estimate postage costs were also increased slightly due to the new USPS first-class letter rate of $0.45 effective January 22, 2012.

Change in Respondent Cost Burden

The total respondent cost burden for this collection has increased by $149,907, from $167,343 to $317,250, from the previous renewal of this collection in February 2009, due to:

- **Increases in estimated hourly rates.** The 2009 renewal used an estimated rate of $121 per hour for respondents to this collection, which was based on the expectation that 70% of submissions will be prepared by paraprofessionals at an estimated rate of $100 per hour, 15% by attorneys at $310 per hour, and 25% by independent inventors at $30 per hour. For the current renewal, the USPTO is using updated rates of $122 per hour for paraprofessionals and $340 per hour for attorneys, which yields a revised average estimated rate of $141 per hour for respondents.

- **Increases in estimated burden hours.** The total estimated burden hours have increased from 1,383 in the 2009 renewal to 2,250 for the current renewal due to overall increases in the estimated annual responses for this collection.

Changes in Responses and Burden Hours

For this renewal, the USPTO estimates that the annual responses will increase by 580 (from 3,920 to 4,500) and the total burden hours will increase by 970 (from 1,280 to 2,250) from the currently approved burden for this collection. These changes are due to the following program changes and administrative adjustments:

Program Changes (decrease of 351 hours):

- **Decrease of 2,063 estimated annual responses** for deleting the Certificate Self-Recovery Form; a **burden decrease of 351 hours.** This form is being

deleted because the current online certificate recovery feature relies on pre-generated access codes and does not collect “information” from the customer.

Administrative Adjustments (increase of 1,321 hours):

- **Increase of 2,643 estimated annual responses** for the Certificate Action Form (PTO-2042); a **burden increase of 1,321 hours.**

Changes in Annual (Non-hour) Costs

For this renewal, the USPTO estimates that the total annual (non-hour) costs will increase by $6,494 (from $4,531 to $11,025) due to administrative adjustments, as follows:

- **Increase of $5,286.** This collection is currently approved with a total of $3,714 in costs associated with the notarization requirement for the Certificate Action Form (PTO-2042). For this renewal, the USPTO estimates that the notarization costs will increase by $5,286 due to an increase in the total estimated responses for the Certificate Action Form.

- **Increase of $1,208.** This collection is currently approved with a total of $817 in postage costs associated with mailing responses to the USPTO. For this renewal, the USPTO estimates that the postage costs for mailed items will increase by $1,208 due to increases in total estimated responses and an increase in first-class postage rates from $0.44 to $0.45 per response.

16. Project Schedule

The USPTO does not plan to publish this information for statistical use or any other purpose. Due to privacy and confidentiality requirements for the encryption keys and recovery passwords, the USPTO does not plan to publish specific information about the digital certificates. Internal records will be kept for reporting and tracking purposes.

17. Display of Expiration Date of OMB Approval

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

18. Exceptions 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.