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

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security services for the electronic business activities of the USPTO, including protecting the confidentiality of unpublished patent applications in accordance with 35 U.S.C. § 122 and 37 CFR 1.14, as well as protecting international patent applications in accordance with Article 30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. 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.

PKI employs public and private cryptographic keys to authenticate the customer's identity and support secure 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the USPTO for transactions such as electronic filing of patent applications and viewing confidential information about unpublished patent applications.

This information collection currently 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 previously assigned Customer Numbers. The form is the critical tie between the physical identity and the digital identity that PKI supports. A certificate request must include a notarized signature in order to verify the identity of the applicant. The Certificate Action Form also 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 may provide additional information for a set of security questions and answers 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 for PKI Certificate Action Form

Requirement	Statute	Rule
PKI Certificate Request and Subscriber Agreement	35 U.S.C. § 2 and 35 U.S.C. § 122, Article 30 of the Patent Cooperation Treaty, Government Paperwork Elimination Act	37 CFR 1.14
Certificate Self-Recovery Form (Electronic)	35 U.S.C. § 2 and 35 U.S.C. § 122, Article 30 of the Patent Cooperation Treaty, Government Paperwork Elimination Act	37 CFR 1.14

2. Needs and Uses

This collection allows for public access to secure USPTO online systems for transactions such as electronic filing of patent applications and retrieving confidential patent application information, which 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 online self-recovery form allows the public to recover lost keys without having to contact support staff at the USPTO.

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 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/Uses of Information Collection for PKI Certificate Action Form

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.
Certificate Self-Recovery Form (Electronic)	None	• Used by the public to obtain a set of single-use passwords that may later be used to recover a lost certificate online without contacting USPTO support staff. • Used by the USPTO to allow users to recover their own certificates electronically without additional support.

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 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.

For the certificate self-recovery feature, the customer may submit the necessary information electronically in order to be able to recover a lost certificate in real time without having to contact USPTO support staff. At key generation or in a later secure session, the customer has the option of downloading a set of single-use complex passwords that can be invoked later as part of the verification process allowing customers 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 collected only when a customer applies for a digital certificate, requests that a digital certificate be revoked, or requests recovery of a lost encryption key. 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 believes 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 October 23, 2008 (73 Fed. Reg. 63134). The comment period ended on December 22, 2008. 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 required 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 of a sensitive nature.

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 4,126 responses per year for this collection, as outlined in Table 3 below.

  The USPTO estimates that approximately 50% of the total annual responses for this collection will be submitted electronically (for online self-recovery of certificates).

- **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. The USPTO estimates that it will take the public approximately 10 minutes (0.17 hours) to complete and electronically submit the information required for Certificate Self-Recovery.

- **Cost Burden Calculation Factors**
  In 2007 the Committee on Economics of Legal Practice of the American Intellectual Property Law Association published a report that summarized the results of a survey with data on hourly billing rates. The professional rate of $310 per hour is the median rate for attorneys in private firms as published in that report. For this collection, the USPTO expects that 70% of the submissions will be prepared by paraprofessionals, 15% by attorneys, and 15% by independent inventors. Using these proportions and the estimated rates of $100 per hour for paraprofessionals, $310 per hour for attorneys, and $30 per hour for independent inventors, the USPTO estimates that the average rate for all respondents will be approximately $121 per hour. These are fully-loaded hourly rates.

Table 3: Burden Hour/Burden Cost to Respondents for PKI Certificate Action Form

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	2,063	1,032	$121.00	$124,872.00
Certificate Self-Recovery Form (Electronic)	0.17	2,063	351	$121.00	$42,471.00
Totals	---------	**4,126**	**1,383**	----------	**$167,343.00**

13. Total Annualized Cost Burden

There are no capital start-up costs, maintenance costs, or fees associated with this information collection. However, this collection does have annual (non-hour) cost burden in the form of recordkeeping costs and postage costs associated with the Certificate Action Form.

This collection has recordkeeping costs due to the notarization requirement for authenticating the signatures on the Certificate Action Form. The USPTO estimates that the average fee for having a signature notarized is $2 and that 2,063 signed Certificate Action Forms will be submitted annually, for a total recordkeeping cost of $4,126 per year.

This collection also has postage costs for submitting the Certificate Action Form to the USPTO by mail. The Certificate Action Form cannot be faxed or submitted electronically because it requires an original notarized signature for identity verification. The USPTO estimates that the first-class postage cost for a mailed Certificate Action Form will be 42 cents and that it will receive 2,063 mailed responses annually, for a total postage cost of approximately $866 per year.

The total annual (non-hour) cost burden for this collection in the form of recordkeeping costs ($4,126) and postage costs ($866) is estimated to be $4,992 per year.

14. Annual Cost to the Federal Government

Certificate Action Forms are processed at the USPTO by the Information Technology Security Program Office. The USPTO estimates that it takes a GS-12, step 1 employee approximately 10 minutes (0.17 hours) to process a Certificate Action Form request. The current hourly rate for a GS-12, step 1 employee is $33.43. When 30% is added to account for a fully-loaded hourly rate (benefits and overhead), the hourly rate for processing the Certificate Action Forms is $43.46 ($33.43 + $10.03). The processing for electronic certificate self-recovery is fully automated and no staff time is required.

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 for PKI Certificate Action Form

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)	0.17	2,063	351	$43.46	$15,254.00
Certificate Self-Recovery Form (Electronic)	0.0	2,063	0	N/A	$0.00
Totals	----------	**4,126**	**351**	----------	$15,254.00

PKI also involves additional costs to the USPTO of approximately $200,000 per year for software licenses, support, system maintenance, and development costs. **Therefore, the total annual cost to the federal government for this collection is $215,254.**

15. Reason for Change in Burden

Summary of Changes Since the Previous Renewal

This information collection is currently approved with a total of 4,126 responses and 1,383 burden hours per year. For this renewal, the USPTO is maintaining these burden estimates for annual responses and hours.

The total annual (non-hour) cost burden for this renewal of $4,992 is an increase of $103 from the current approved total of $4,889 in annual (non-hour) costs for this collection. This increase in annual costs for the current renewal is due to administrative adjustments.

Change in Respondent Cost Burden

The previous renewal of this collection was approved in February 2006 with an estimated total respondent cost burden of $143,832 per year. The 2006 renewal used an estimated rate of $104 per hour for respondents to this collection, which was a weighted average of the estimated rates of $81 per hour for paraprofessionals (70% of respondents), $286 per hour for attorneys (15% of respondents), and $30 per hour for independent inventors (15% of respondents).

For the current renewal, the USPTO has revised the estimated rate for respondents to $121 per hour in order to reflect the updated hourly rates of $100 for paraprofessionals, $310 for attorneys, and $30 for independent inventors (using the same proportions as the previous weighted average). At the revised rate of $121 per hour, the 1,383 burden hours for this renewal yield a respondent cost burden of $167,343, which is an increase of $23,511 from the total respondent cost burden in the 2006 renewal. This increase is due to the increase in the estimated hourly rate for respondents in this collection.

Changes in Responses and Burden Hours

The USPTO does not expect any changes in the estimated annual responses or burden hours for this renewal.

Changes in Annual (Non-hour) Costs

For this renewal, the USPTO estimates that the total annual (non-hour) costs for this collection will increase by $103, from $4,889 to $4,992 per year. This increase is due to updating the estimated postage costs for submitting the Certificate Action Forms to the USPTO by mail. **Therefore, this collection has a total increase in annual (non-hour) cost burden of $103 due to administrative adjustments.**

[Note: The previously approved estimate of $4,889 in annual costs for this collection is listed as $5,000 in the current inventory system. The $111 difference is due to rounding the estimate to the nearest thousand dollars in order to accommodate the legacy inventory system. This rounded figure was carried over when the legacy data was migrated to the current inventory system. Consequently, the annual cost burden increase of $103 for this collection that is due to administrative adjustments is displayed as a *decrease* of $8 in the current inventory system in order to compensate for the previously rounded figure and to result in the new annual cost burden of $4,992 for this collection as described above.]

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

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.

REFERENCES

A. The USPTO Information Quality Guidelines
B. Certificate Action Form (PTO-2042) and Subscriber Agreement
C. Certificate Self-Recovery Form
D. 60-Day Notice published in the *Federal Register* on October 23, 2008 (73 Fed. Reg. 63134)