

Authentication Changes for Registered Users of EFS-Web and Private PAIR

I. Summary

The United States Patent and Trademark Office (USPTO) is implementing a new authentication method for registered users of the USPTO's electronic filing system, EFS-Web, and Private Patent Application Information Retrieval (PAIR) system. The new authentication method involves a two-step process for logging in to both EFS-Web and Private PAIR and provides a number of benefits to users including enhanced security. All registered users of EFS-Web and Private PAIR, including registered patent practitioners, limited recognition patent practitioners, pro se inventors, and the support staff of these practitioners, will need to have a USPTO.gov account. Users who do not currently have a USPTO.gov account should take steps now to obtain an account by visiting <https://www.uspto.gov/AuthenticationChange> and following the instructions under the "Create a USPTO.gov Account" section.

Since October 2018, registered patent practitioners, limited recognition patent practitioners, and pro se inventors who currently have a Public Key Infrastructure (PKI) certificate (also known as digital certificates, EPF files, and/or certificates) have been able to link their PKI certificates to their USPTO.gov account. As of November 1, 2018, patent practitioners are able to sponsor support staff to work on their behalf. Use of PKI certificates may no longer be available after December 31, 2018. The new authentication method utilizes USPTO.gov accounts plus a temporary authentication code delivered by either email, phone call, or mobile device application. This authentication method also will be used in Patent Center, which is the next generation tool that will replace EFS-Web and PAIR and is anticipated to be available in 2020.

II. Background

Currently, EFS-Web and Private PAIR provide applicants secure authenticated access to electronically file and view their patent application information through the use of public key cryptography mechanisms (PKI certificates) that provide authentication. The USPTO has used PKI technology to facilitate secure access to electronic patent filing and application management since 2006.

Under the PKI Subscriber Agreement and the rules and policies of the USPTO including the Legal Framework for EFS-Web, PKI certificate holders may designate more than one employee to use their PKI certificate under the direction and control of the PKI certificate holder. The PKI Subscriber Agreement is available on the USPTO website at:

https://www.uspto.gov/sites/default/files/patents/process/status/private_pair/PKI_Subscriber_Agreement.pdf.

In 2016, the USPTO determined that replacement of PKI technology would be needed. Therefore, the USPTO is updating the authentication method for both EFS-Web Registered and Private PAIR. The new authentication method requires every user to have their own account, including support staff. Under the new authentication method, users are not permitted to share their credentials with other individuals.

III. Details of the Updated Authentication Method

The new authentication method being implemented in 2018 will replace PKI technology and provide the following benefits to users:

- Eliminates shared credentials: practitioners no longer have to share, and will no longer be permitted to share, accounts with support staff, who will have their own.
- Modernizes security process with two-step authentication: username/password plus a temporary authentication code delivered by either email, phone call or mobile device.
- Saves time by granting access to multiple USPTO systems with one consolidated sign-in.
- Facilitates USPTO's compliance with the Federal Information Security Management Act (FISMA) framework and National Institute of Standards and Technology (NIST) guidelines.
- Helps resolve browser compatibility issues.
- Gives users access to EFS-Web and Private PAIR until the planned full release of Patent Center in 2020.

The updated authentication method requires two steps and impacts all EFS-Web Registered and Private PAIR users. In addition, support staff (e.g., paralegals, docket clerks, office administrators, etc.) are impacted by this change. All users will need to obtain their own USPTO.gov account, which consists of a username (email address) and password. This will be used as the first step to log into EFS-Web Registered and Private PAIR. The USPTO's Financial Manager system currently uses this method of authentication. Users who do not currently have a USPTO.gov account should take steps now to obtain an account.

In order to establish the second step, users will need to go into their USPTO.gov settings to opt into using two-step authentication. The second step will provide an additional verification channel, consistent with the NIST Digital Identity Guidelines, to authenticate the user. For example, the user may choose to receive an email or phone call which will provide a 6-digit code that is to be entered along with their USPTO.gov password. Alternately, users may download a free authenticator app on their mobile phone to provide the additional secure verification. Instructions regarding two-step authentication is posted at the USPTO website at:
<https://www.uspto.gov/learning-and-resources/account-faqs>.

Once the user authenticates using the second step, the user has the option to select a checkbox so that only the first step is required to authenticate back into the systems within a 24-hour period, using the same computer.

Patent Electronic System Subscriber Agreement

Users will need to subscribe to terms of use for access to the USPTO systems. The Patent Electronic System Subscriber Agreement will be posted on the USPTO website at: <https://www.uspto.gov/AuthenticationChange>. This subscriber agreement is considered a modification of the PKI subscriber agreement and continued use of the system will constitute agreement to the Patent Electronic System Subscriber Agreement.

The current Legal Framework for EFS-Web is published in the *Manual of Patent Examining Procedure*, Rev. 08.2017, Jan. 2018 (referred to herein as “MPEP”) § 502.05. It will be revised in accordance with this notice. The revised version will be posted on the USPTO Web site and incorporated into a future revision of the MPEP.

PKI Migration Tool

In October 2018, the USPTO released a migration tool that allows current PKI certificate holders to link customer numbers associated with their PKI certificate to their USPTO.gov account. As described above, the USPTO.gov account will serve as the first step to log into EFS-Web Registered and Private PAIR. The migration tool is exclusively authorized for use by practitioners and independent inventors who hold a current PKI certificate. Other individuals such as support staff are not authorized to use the migration tool. The use of the migration tool to link a PKI certificate to a USPTO.gov account can only occur once. After the migration is complete, current PKI certificate holders will be able to access EFS-Web Registered and Private PAIR using their new credentials. Although not recommended, PKI certificates may still be used after the migration up until the certificates are officially retired. Support staff will need to continue to use the shared PKI certificate to access EFS-Web Registered and Private PAIR until they are sponsored using the sponsorship tool discussed below.

Sponsorship Tool

On November 1, 2018, the USPTO released a sponsorship tool that allows practitioners to grant or remove sponsorship for support staff individuals (under the direction and control of sponsoring practitioners) to work on their behalf. The support staff individual must have already created a USPTO.gov account in order to be sponsored by a practitioner. After the sponsorship is complete, the support staff individual will be able to access EFS-Web Registered and Private PAIR using their new credentials. The support staff individual will have access to all applications associated with the customer number(s) of the sponsoring practitioner. The support staff individual must use their own credentials when accessing EFS-Web Registered and Private PAIR and may not use the credentials (e.g., the USPTO.gov account) of the practitioner or any

other individual. Each support staff member must have their own account; accounts may not be shared among support staff members. For further details, please refer to the Sponsorship Process section of the “Patent Electronic System Access Document,” available at <https://www.uspto.gov/AuthenticationChange>.

Identity Verification (Proofing)

The identity verification requirements for accessing USPTO systems are designed in view of the Digital Identity Guidelines created by the National Institute of Standards and Technology for use by government agencies in fulfilling the requirements of the Federal Information Security Management Act of 2002 (FISMA). The general contours of the identity proofing are as follows. Prospective users of USPTO Patent Electronic System are required to undergo an identity proofing and enrollment process whereby their identity evidence and attributes are collected, uniquely resolved to a single identity within a given population or context, then validated and verified. Current PKI certificate holders who migrate using the USPTO’s migration tool according to the procedure set forth in the Patent Electronic System Access Document will be considered to have met the identity proofing requirements. The Patent Electronic System Access Document also provides identity proofing procedures for new practitioners and inventors.

Each practitioner will be responsible for proofing the identity of the person being sponsored. The sole objective of the identity proofing is to ensure the user of the sponsored account is who they claim to be. The two-step identification provided by the USPTO.gov account and one-time code provides assurance that the user is the owner of that account; however, it is not designed to verify the real-world identity of that user. Each sponsoring practitioner will establish a procedure for identity proofing sponsored users and maintain a record of that procedure. In general, the identity proofing consists of three steps: resolution of the prospective sponsored user’s identity based upon identity evidence, validation of the evidence, and verification of the evidence. In the resolution step, each sponsored user must present acceptable evidence of their identity to be collected and stored by the practitioner. In the validation step, the authenticity, accuracy, validity of the identity evidence is confirmed. In the verification step, a linkage between the claimed identity and the real-life existence of the prospective sponsored user is confirmed. Practitioners will refer to the Verification Policy and Identity Proofing of Sponsored Users section of the “Patent Electronic System Access Document,” available at <https://www.uspto.gov/AuthenticationChange>, for details of this procedure.

IV. Contact Information

For information on how to create a USPTO.gov account and link your existing PKI certificate, please visit: <https://www.uspto.gov/AuthenticationChange>. If you need assistance creating your USPTO.gov account, please call the USPTO Contact Center (UCC) at 800-786-9199.

Questions or comments related to the new authentication method may be sent to
eMod@uspto.gov.

Date:

11/20/2018

Andrei Iancu

Andrei Iancu

Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office