

1. Introduction

This document explains “what’s new” with the next release of SPS (ReIP 7.1) from the perspective of SPS users (including DEO and CO user roles). This new release provides the ability for the SPS users to manage their credentials. This includes the ability to update “key components” of their credentials like encryption key/certificate, signing key/certificate, etc. The normal SPS activity remains unchanged. This document also contains information about upcoming changes to SPS, and to the list of supported operating systems and Java Plug-ins.

This new release is expected to be available on Monday August 20, 2007.

2. What’s New

2.1 All Roles – “Credential Management” Enhancement

All SPS users have a PKI Credential residing on their iKey token. Various components of this PKI Credential need to be updated when they reach close to end of their valid life time. The functionality to update a user’s credential is now built-in to SPS. In addition, certain events cause changes to be made to PKI Credential (ex: change of user’s last name, change of user’s agency name, PIN expiry, etc.). The current enhancements help users to manage their credential to handle such events with the assistance of their Primary Servicing RFC.

During normal login to SPS application, after entering their PIN, users may now encounter a “User Credential Status” screen similar to the one shown in Figure 1.



Figure 1: New “User Credential Status” popup

Note that the exact text in the “User Credential Status” popup may be different from the one shown in Figure 1: the date/time of the expiry may be different and in the future, the list of expiring components may be different and could include (Signing Key/Certificate, Encryption Key/Certificate, a pending Forced-Update, a pending DN (user/agency name) change, a pending PIN change, etc.) The buttons in the “User Credential Status” popup may be different from the one shown in Figure 1: the “Update” button may be enabled along with “Skip Update” button disabled to force the user to change their credential immediately.

Selecting “Update” button results in the management/updating of their credential and after a 3-10 minute wait period, the user is presented with the status of the activity as shown in Figure 2.

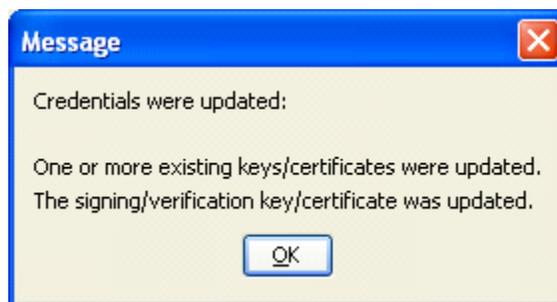


Figure 2: Result of "Credential Management" activity

Selecting “OK” button leads to the continuation of the usual SPS login process and the “User Credential Status” screens will not appear until the next time they are needed.

If a user does not login to SPS for a long time, they may find that their credential has already expired and can not be updated/managed automatically by the enhancements described here. If a user attempts to login to SPS with expired credentials, they get a pop-up error message with the text: "Your certificate had expired. Please contact helpdesk to create/recover the certificate." In this case the users are expected to follow the manual process to recover their credential. The current manual process to recover credentials when user forgets their PIN, losses their credential or when their credential is expired/compromised, remains unchanged.

3. Upcoming Changes to SPS

The next couple of releases of SPS are expected to offer a “Self Contained” version of SPS and to provide support for stronger versions of cryptographic components (SHA-2 and 2048-bit keys). The “Self Contained” version is expected to run SPS with out involving any standard browser or installed Java Plug-in on the user machine.

Windows XP (with latest patches and updates) is the only supported Operating System for SPS. Even though our official support will be dropped for Windows 2000, we expect (but can not guarantee) SPS to continue to function with Windows 2000 Operating System after June 2007. The support for Windows XP is expected to continue for the

foreseeable future. SPS support for the new Windows Vista Operating System is expected to be available early 2008.

SPS supports two versions of Java Plug-ins – version 1.4.2_13 and 1.5.0_11. SPS support for the new Java plug-in version 1.6.0_x is, expected to be available early 2008. Note that SPS no longer supports the Java Plug-in version 1.3.x_y. Users attempting to login to SPS using Java Plug-in version 1.3.x_y will receive an error message shown in Figure 3 and Figure 4.



Figure 3: Fatal Error pop-up message with Java plug-in Version 1.3.x_y

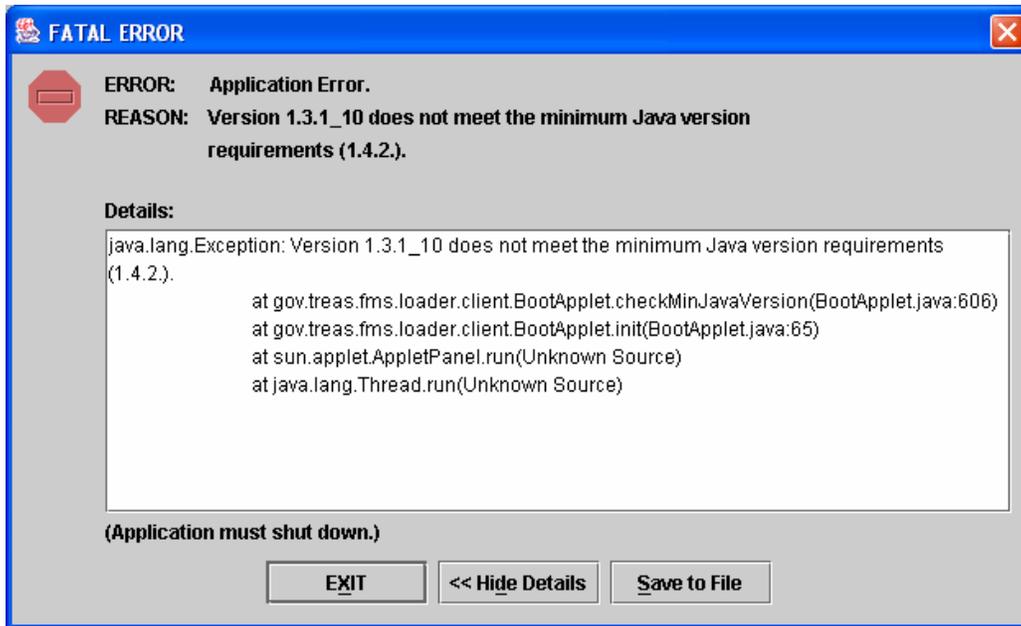


Figure 4: Fatal Error pop-up message with Java plug-in Version 1.3.x_y (Show Details)

4. For More Information

Please contact your servicing RFC (Regional Financial Center) for any questions, concerns or additional information.