



Bureau of the Fiscal Service

Integrated Trusted Registration Application

ITRA Self-Contained Users Guide

12/31/2014

Change Table

Version	Date	Change Description	Section/ Page	Author(s)
V1.0	06/30/2013	Release ITRA-SC (Self-Contained)	All	Joshua Sturgis Taylor Davenport Irina Yakovenko
V1.1	07/31/13	Incorporated comments from Preproduction testing team.	All	Joshua Sturgis
V1.2	12/31/2014	Support eToken 5100	Section 5	Irina Yakovenko

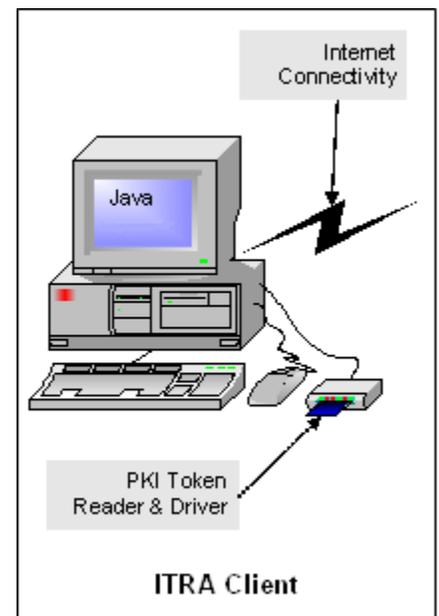
Table of Contents

1. INTRODUCTION.....	1
1.1 ASSURANCE LEVELS	1
1.2 ITRA FUNCTIONALITIES	2
1.3 SUPPORTING DOCUMENTATION	2
1.4 NOTATION CONVENTIONS	2
1.5 KEYBOARD-BASED NAVIGATION.....	3
1.6 HELPFUL HINTS	3
2. GETTING STARTED WITH ITRA.....	3
2.1 DOCUMENT ASSUMPTIONS.....	4
2.2 VARIABLE DEFINITIONS	5
2.3 LAUNCH ITRA.....	6
3. SELF SERVICE UPDATE.....	7
3.1 SELF SERVICE LOGIN	8
3.2 CHANGE CREDENTIAL PIN	11
4. SELF SERVICE CREATE/RECOVERY.....	13
5. TRA ASSISTED CREATE/RECOVERY.....	18
5.1 TRA ASSISTED CREATE.....	18
5.2 TRA ASSISTED RECOVERY	24
APPENDIX A – TROUBLESHOOTING TIPS.....	30
A-1 GENERAL ISSUES.....	30
A-1.1 ITRA Maintenance Page.....	30
A-1.2 ITRA Cannot Connect to Server	31
A-2 ISSUES WITH SECURITY TOKEN (iKEY).....	31
A-2.1 View iKey/eToken Contents	32
A-3 ISSUES WITH LOGIN TO ITRA.....	33
A-3.1 Your Certificate Has Expired.....	33
A-3.2 TRA Access Fails	34
A-4 ISSUES WITH CREDENTIAL MANAGEMENT	35
A-4.1 Bad Reference ID.....	35
A-4.2 Authorization Codes Do Not Match.....	36
A-5 COLLECT INFORMATION FOR HELPDESK TICKET.....	36
A-5.1 Capture Error Details for Helpdesk Ticket.....	36
A-5.2 Capture ITRA Execution Thumbprint	38

1. Introduction

The Integrated Trusted Registration Application (ITRA) is a system for creating, recovering, and maintaining PKI credentials. The client component of this system (the ITRA Client) is a PKI-token enabled Java client. The client workstation requires only that an approved token reader and driver be installed, along with an appropriately installed Java and PKI Token (iKey or eToken) reader and driver (such as SafeNet).

This document is a task-based user guide for ITRA-SC, which demonstrates the steps required to create/maintain user tokens (iKey or eToken). The appendices cover common issues, some error messages that may be received while running ITRA in either mode of operation, their possible solutions, and general troubleshooting.



1.1 Assurance Levels

ITRA currently supports token creation and maintenance of credentials at the following assurance levels:

Level-1/Rudimentary-Assurance Credentials:

- Do not require in-person proofing or a Trusted Registration Agent (TRA)
- End- users may create or recover their Level-1 tokens by using Self Service Create/Recover procedure
- End- users may update their Level-1 tokens and PINs by using Self Service Update procedure
- Example Level-1 application – TCIS, DebtCheck

Level-3/Medium Hardware-Assurance Credentials:

- In-person proofing required to obtain credential
- Trusted Registration Agent (TRA) required to create or recover Level-3 tokens by using the TRA Assisted Create/Recovery procedures
- End- users may update their Level-3 tokens and PINs by using Self Service Update procedure
- Example Level-3 application – SPS, ASAP

1.2 ITRA Functionalities

Token creation and maintenance within ITRA is accomplished via the following functions:

Self Service Update - Allows end-users to update the certificates, or change the credential PIN on his/her Level-1 or Level-3 token without assistance from a TRA. This function is primarily used by end-users to avoid expiration of tokens. Steps for accomplishing this task are captured in Section 3.

Self Service Create/Recovery - Allows end-users to create or recover his/her Level-1 token. This function is primarily used by end-users to create a new or recover a non-working Level-1 iKey or eToken. Steps for accomplishing these tasks are captured in Section 4.

TRA Assisted Create/Recovery – Allows a TRA to create or recover a Level-3 token. This function is primarily used to create or recover a non-working level-3 iKey or eToken. Steps for accomplishing these tasks are captured in Section 5.

1.3 Supporting Documentation

ITRA Self Contained Installation Guide – dated 31 July 2013.

1.4 Notation Conventions

For reference, the notation conventions used in this manual shall be in the following format:

- | | |
|------------------------------|---|
| Bold | Bold text without brackets or braces represent Specific menu names, menu selections , check boxes, data field descriptions within a form/panel, and the exact names of tabs, panels, screens, and frames. Do not bold common names (e.g. folder, menu, box, etc.). <ul style="list-style-type: none">○ Example: Select Satellite Tools menu option |
| | Bold text will also be used for exact data entries. <ul style="list-style-type: none">○ Example: Enter C:\Program Files\... |
| < Bold > | Bold text appearing between angle brackets represents sequential or simultaneous keystrokes on a keyboard. <ul style="list-style-type: none">○ Simultaneous: Press <Ctrl+Alt+Delete> |
| [Bold] | Bold text appearing between square brackets represents a window button that is selected via a mouse click |
| < <i>ITALICIZED</i> > | Bold ITALICIZED text in caps appearing between angle brackets represents a <i>variable</i> entry, with underscores between the words. User substitutes with correct values. Do not use spaces here. <ul style="list-style-type: none">○ Example: Enter <DATE_AND_TIME> |

→	Arrows are used to indicate sequential menu selections. <ul style="list-style-type: none"> ○ Example: Select File → Open
<u>Underline</u>	<u>Underlined text</u> represents a World Wide Web hyperlink. <ul style="list-style-type: none"> ○ Example: Request an Account <u>at this link</u>.
“ ”	Quotation marks will be used to indicate system-generated messages, prompts, window names, etc. <ul style="list-style-type: none"> ○ Example: “Applications” folder ○ Example: “Netbackup Installation Type” dialog box
{[MEDIA TITLE]}	Media titles will be bold Arial text 10-point font and enclosed in brackets with vertical bars when referenced within a procedure.

1.5 Keyboard-Based Navigation

If desired, the application can be navigated using only the keyboard or a combination of keyboard and mouse. The navigation keys and their functions are listed below:

- <Tab> – Always moves to the next component (entry blank, button, checkbox).
- <CTRL + SHIFT + Tab> – Always moves to the previous component.
- <CTRL + Tab> – Always skips to the first item in the next component.
- <Space Bar> – Activates dropdown items, radio buttons and checkboxes.
- <Alt + <letter>> – Jumps to the component with the *letter* underlined as a shortcut.

1.6 Helpful Hints

A Helpful Hint icon appears in the left margin throughout this manual. This icon highlights key instructions, information, and helpful hints. The example below illustrates how the Helpful Hint icon is used.



Helpful Hint: Do not remove iKey (or eToken) when ITRA is using it to write certificates. Removing the token while writing may damage the token.

2. Getting Started with ITRA

The following section will outline the prerequisites needed for users to accomplish the tasks outlined in this document.

2.1 Document Assumptions

Unless otherwise noted, it is required that the end user has already logged into the workstation and has installed the ITRA software prior to executing any task in this document. Installation requirements and instructions are contained in the *ITRA Self Contained Installation Guide*.

The ITRA users can get updated ITRA documentation by following the “ITRA Documents” link from the main ITRA web page, as shown on Figure 2-1.

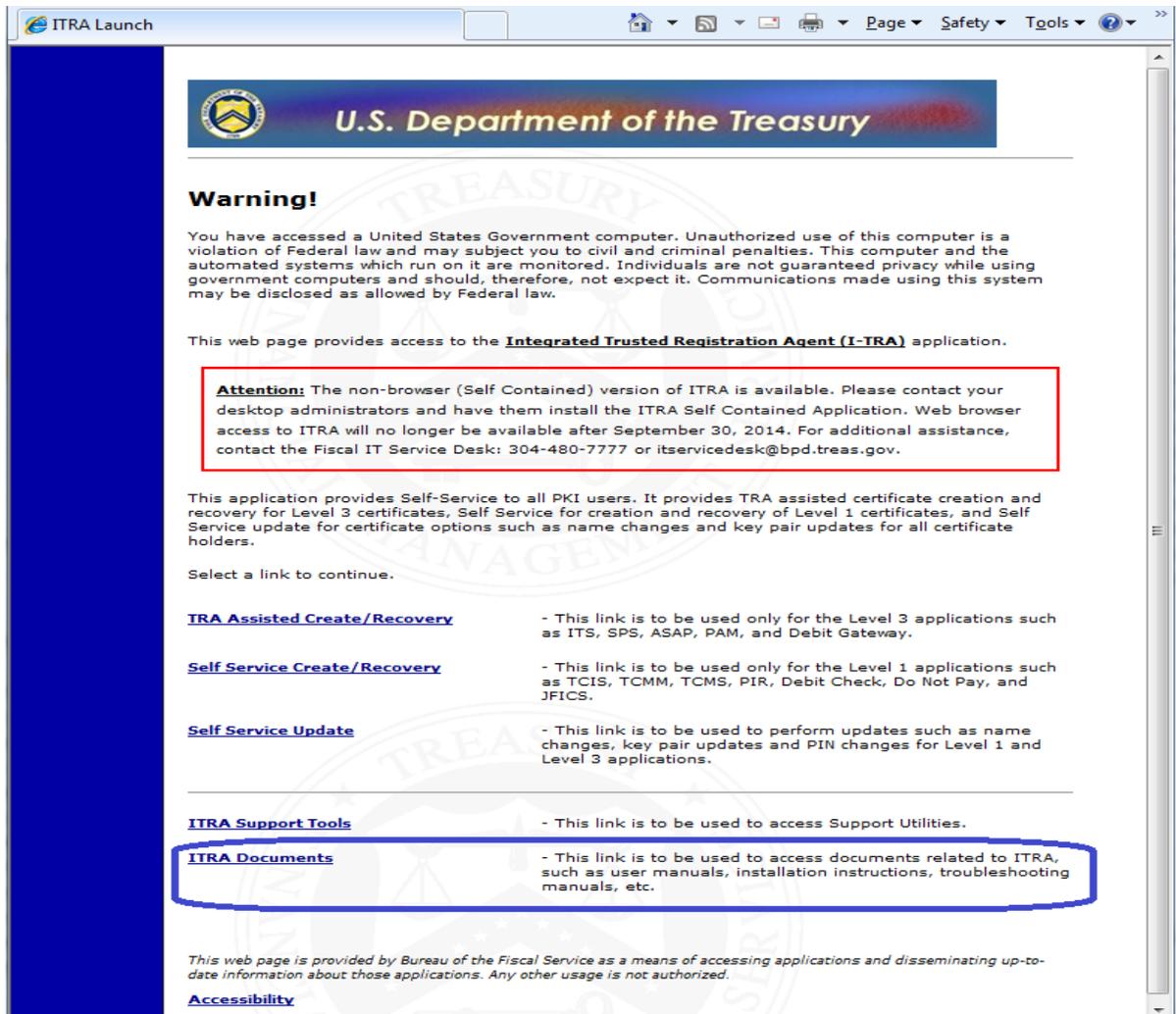


Figure 2-1 The main ITRA web page contains link to the ITRA Documents

NOTE: Installing ITRA requires System Administrator permissions. Users must contact their agency's system administrator(s) or call the Fiscal IT Service Desk for additional help.

2.2 Variable Definitions

The following table identifies and defines the various variables required to execute the tasks contained within this document. Task introduction text will identify which variables are required to accomplish the steps contained in the table.

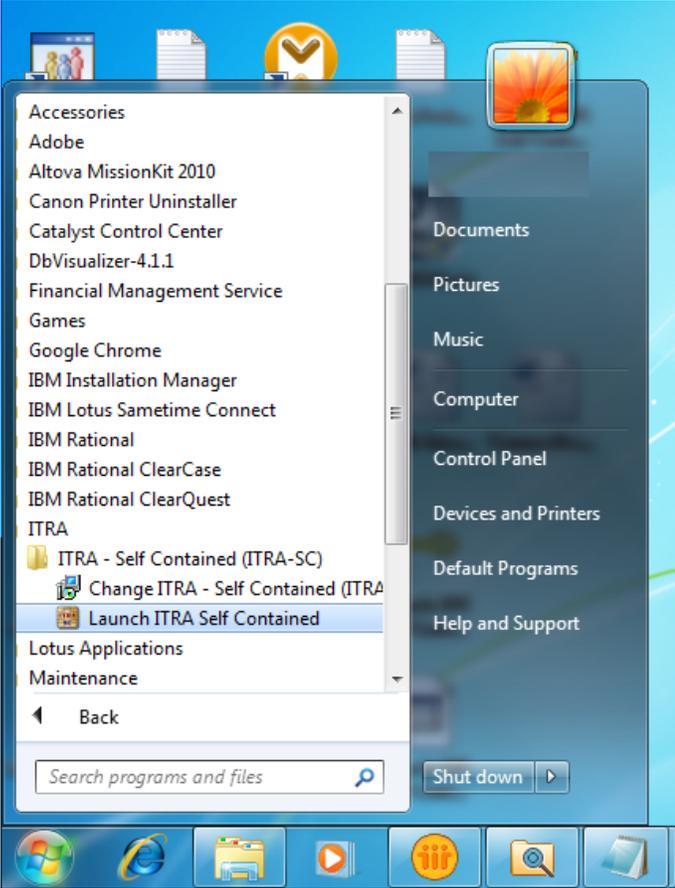
Table 2.2-1 Variable Worksheet

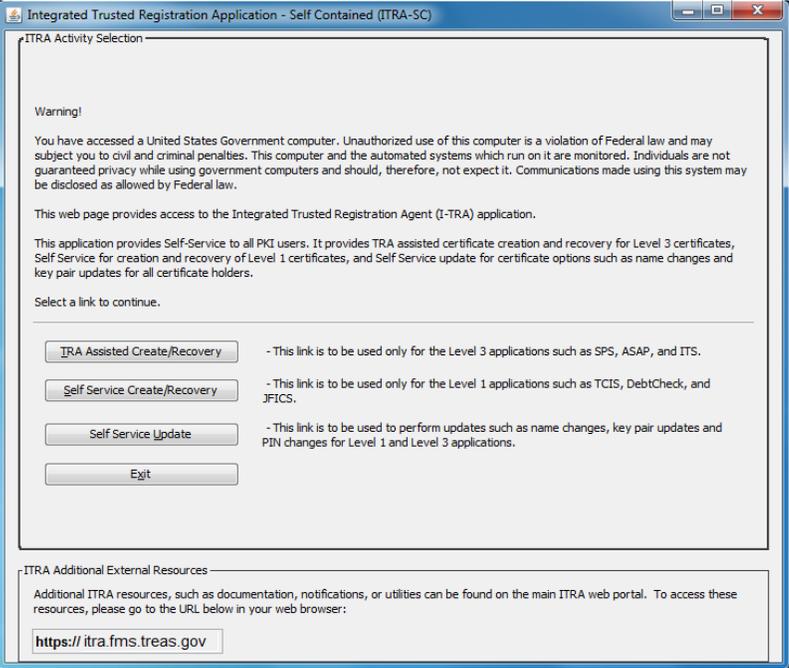
<i>Variable</i>	Definition	Value
<Credential PIN>	Password permitting applications access to read certificates contained on the iKey or eToken. Required format is: - 8 Characters <i>minimum</i> - Alpha-Numeric - Must contain 1 Uppercase, 1 Lowercase, 1 Numeric, & 1 Special Character	
<Reference Number>	8 Digit number provided by EICAM or CA Administrator. i.e. 14421747 Information can be obtained by contacting the Fiscal IT Service Desk @ 304-480-7777	
< <i>Authorization Code</i> >	12 Alpha-numeric characters provided by EICAM or CA Administrator. i.e. S8PE-48VP-97XJ Information can be obtained by contacting the Fiscal IT Service Desk @ 304-480-7777	
<User iKey>	A USB token (iKey or eToken) meant to hold users PKI Level-1 or Level-3 certificates. Used for proof of credentials or application authentication	
<TRA iKey>	A Level-3 USB token (iKey or eToken) containing the Trusted Registration Agent's (TRA) PKI certificates	

2.3 Launch ITRA

Perform the following steps to launch ITRA.

Table 2.3-1 Launch ITRA

Step	Instructions	Comments
1.	 <p>Click Start -> All Programs -> ITRA -> ITRA – Self Contained (ITRA-SC) -> Launch ITRA Self Contained</p>	<p>NOTE: The Start button icon is different in Windows XP</p> <p>Optional: double click on the icon on your desktop:</p> 

Step	Instructions	Comments
2.	 <p>Figure 2-2 Main ITRA Self Contained screen</p> <p>ITRA Self Contained main screen opens.</p>	<p>Clicking on button [Exit] will close the ITRA-SC window.</p> <p>The other three buttons will start the appropriate ITRA actions:</p> <ul style="list-style-type: none"> • [TRA Assisted Create/Recovery] • [Self Service Create/Recovery] • [Self Service Update]

3. Self Service Update

“ITRA Self Service Update” feature allows users to update their token with a new certificate and/or PIN when it is needed, without third party assistance. This section details the procedure to update the token and/or change their PIN. By following this procedure the user can avoid expiration of their token.

There are two primary forms of certificate update notifications. The first form is the end user receives an email from the issuing certificate authority stating their certificates/tokens are in need of an update. There are several reasons why tokens/certificates would require an update, the most common ones are: changes to certificate expiration, information added/removed from certificates, or the user’s PIN needs to be changed or has expired.

The second notification method would be via the “User Credential Status prompt” (Figure 3-1), when user logs into ITRA with the iKey or eToken:

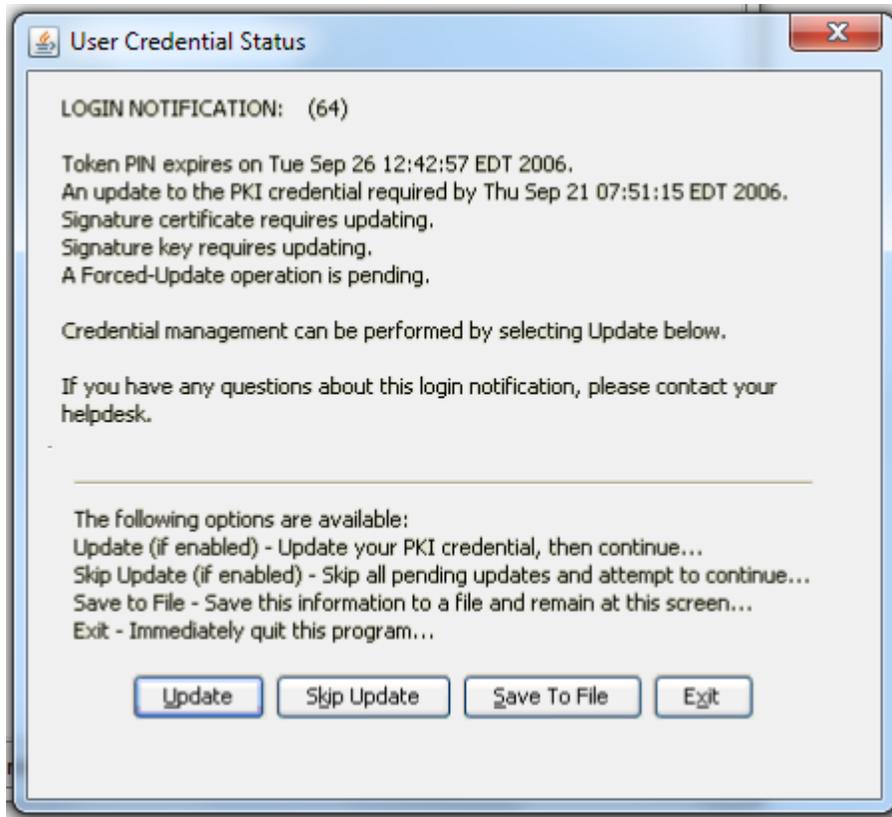


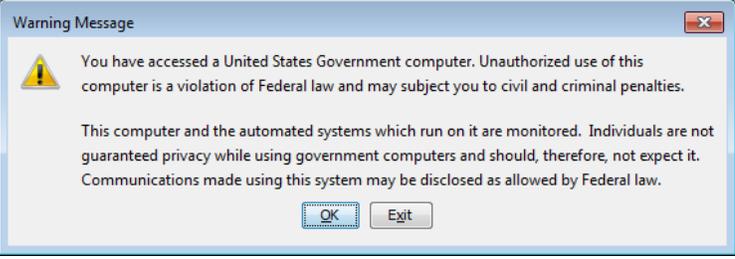
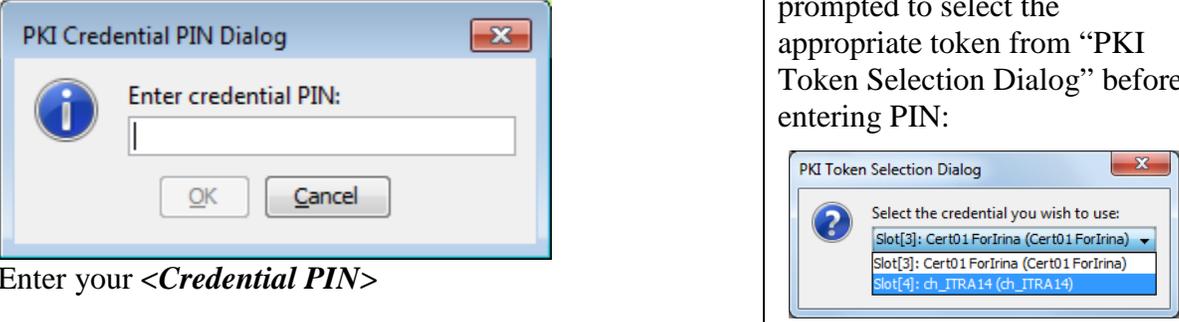
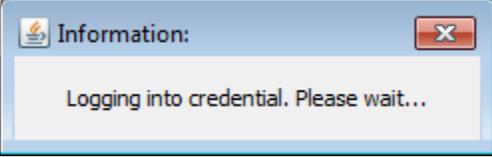
Figure 3-1- User Credential Status with pending updates

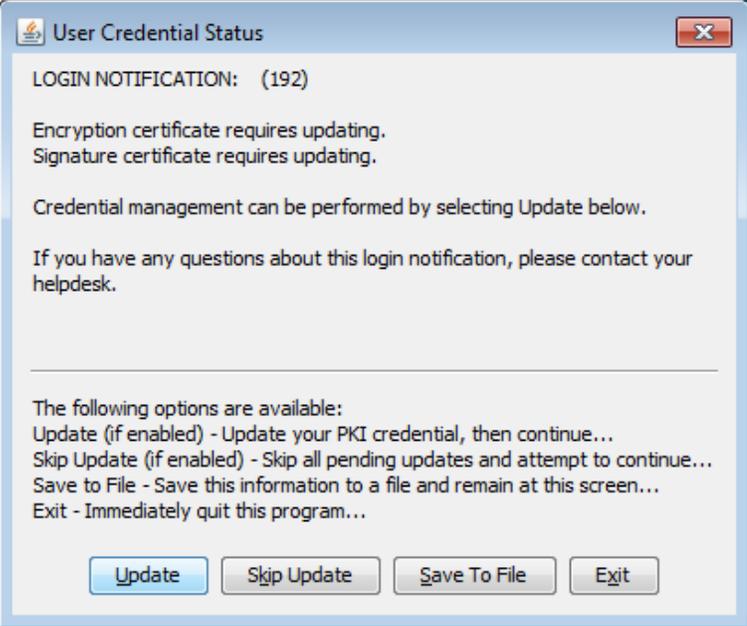
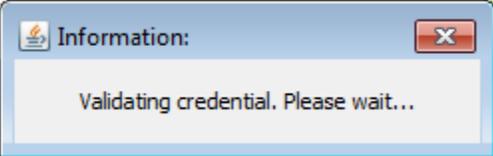
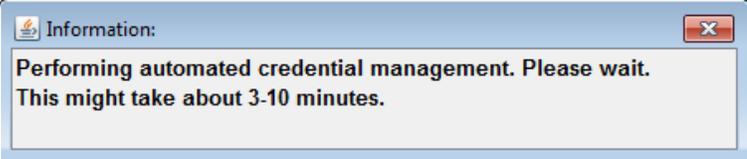
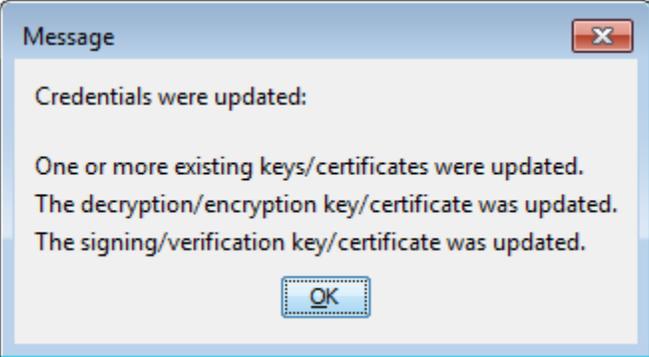
3.1 Self Service Login

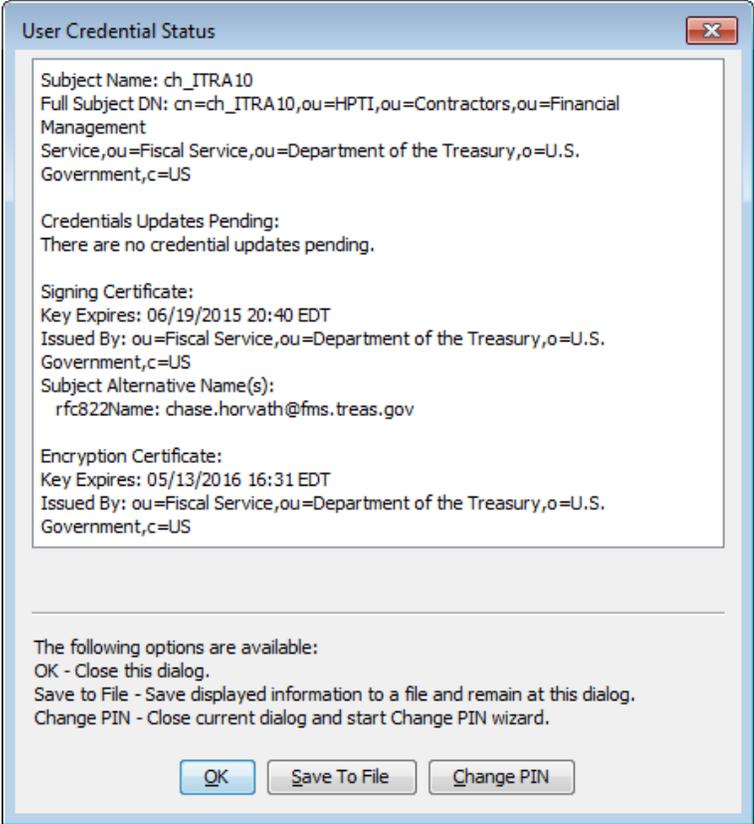
Perform the following steps to check if your ITRA token (Level-1 or Level-3) needs to be updated. When any updates are pending for your PKI credentials, you will be given an opportunity to update your ITRA token. The following variables are required to accomplish these steps: *<User iKey>*, *<Credential PIN>*

Table 3.1-1 Self Service Update

<i>Step</i>	Instructions	Comments
1.	Launch ITRA	Section 2.3 contains execution steps
2.	Insert your <i><User iKey></i> and click [Self Service Update]	

Step	Instructions	Comments
3.	 <p>Warning Message</p> <p>You have accessed a United States Government computer. Unauthorized use of this computer is a violation of Federal law and may subject you to civil and criminal penalties.</p> <p>This computer and the automated systems which run on it are monitored. Individuals are not guaranteed privacy while using government computers and should, therefore, not expect it. Communications made using this system may be disclosed as allowed by Federal law.</p> <p>OK Exit</p>	
4.	 <p>PKI Credential PIN Dialog</p> <p>Enter credential PIN:</p> <p>OK Cancel</p> <p>PKI Token Selection Dialog</p> <p>Select the credential you wish to use:</p> <p>Slot[3]: Cert01 ForIrina (Cert01 ForIrina)</p> <p>Slot[3]: Cert01 ForIrina (Cert01 ForIrina)</p> <p>Slot[4]: ch_ITRA14 (ch_ITRA14)</p>	<p>If multiple tokens are connected to your computer, you will be prompted to select the appropriate token from “PKI Token Selection Dialog” before entering PIN:</p> <p>Figure 3-2 Token selection</p>
5.	 <p>Information:</p> <p>Logging into credential. Please wait...</p>	

Step	Instructions	Comments
6.	 <p>Click [Update]</p>	<p><u>Note 1</u>: this notification dialog will only appear if the credentials updates are pending for user's PKI token. Otherwise, this and next steps will be skipped and the user will be taken directly to Step 10.</p> <p><u>Note 2</u>: the button [Skip Update] is disabled when updates are required to continue.</p> <p><u>Optional</u>: Click on button [Save To File]: the content of the displayed User Credential Status will be saved to local file.</p>
7.	 <p>Wait for Credential Validation to finish</p>	
8.	 <p>Wait for Credential Update to finish</p>	
9.	 <p>Credential Update is finished click [OK]</p>	<p>Credential update is complete.</p>

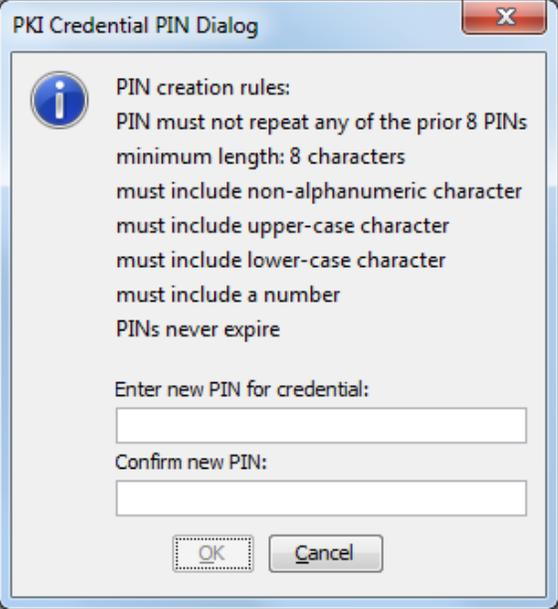
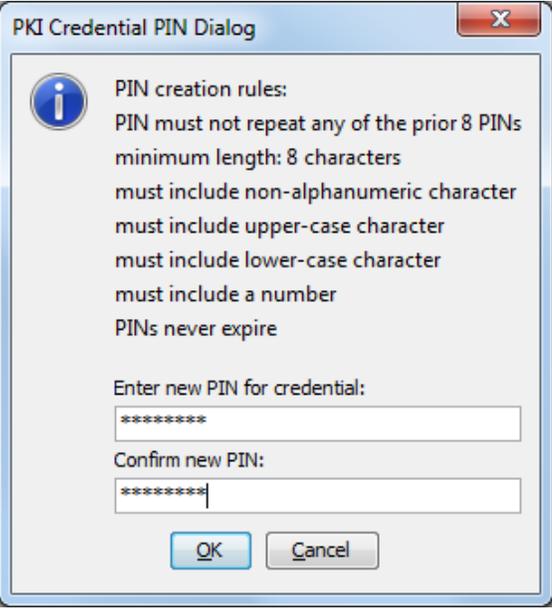
<i>Step</i>	Instructions	Comments
10.	 <p>Figure 3-3 User Credential Status Information</p> <p>Review the User Credential Status screen and click [OK] to close the window.</p>	<p>Options:</p> <ol style="list-style-type: none"> 1. Click on button [Save To File]: the content of the displayed User Credential Status will be saved to local file. 2. Click on button [Change PIN]: follow steps outlined in Section 3.2.

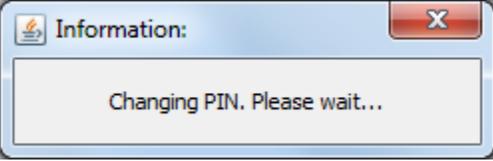
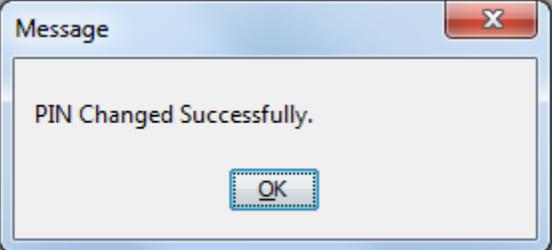
3.2 Change Credential PIN

Since the credential PIN is the equivalent to a credential’s password; it is strongly recommended users change their credential PIN, in accordance with the organizations password policy, i.e. every 60 or 90 days.

This process can be started only within **Self Service Update** ITRA function. The following steps outline the preferred method for users to change a level-1 or level-3 token’s credential PIN.

<i>Step</i>	Instructions	Comments
1.	<p>Perform Self Service Login with your token. The expected result is the Figure 3-3 User Credential Status Information. Click on button [Change PIN].</p>	<p>Section 3.1 contains execution steps</p>

Step	Instructions	Comments
2.	 <p>Figure 3-4 PKI Credential PIN (Change) Dialog</p> <p>Enter the new PIN in both boxes and click [OK] to continue.</p>	<p>The new PIN must meet all of the complexity rules set for your agency and displayed under “PIN creation rules”. The actual rules might differ from the example shown on Figure 3-4</p>
3.	 <p>The PIN will appear as a series of asterisks for security purposes. Click [OK]</p>	<p>If the PIN entered does not meet the complexity requirements listed under “PIN Rules” a pop-up window will appear to indicate which rule has been broken. See Figure 3-5 for an example:</p>  <p>Figure 3-5 PIN Not Compliant</p> <p>Click [OK] to return to the “PKI Credential PIN Dialog” to try again.</p>

Step	Instructions	Comments
4.	 <p>Please be patient while the PIN is being changed, which could take several seconds.</p>	
5.	 <p>Click [OK] to exit the ITRA.</p>	



Helpful Hint: At any time during the PIN change process the user may cancel the PIN change request by clicking the “Cancel” button. When the process is cancelled, ITRA will display the “Change PIN Cancellation”. (Figure 3-6) The application will close, requiring the user to log in again if needed.

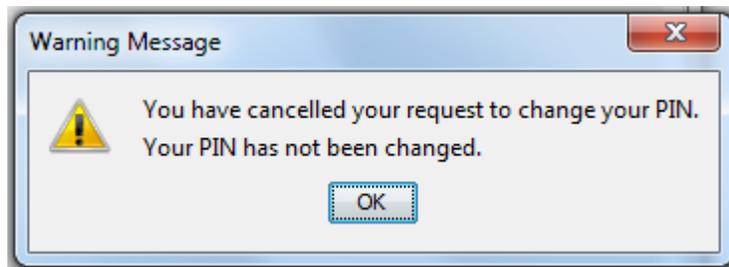


Figure 3-6 Change PIN Cancellation

4. Self Service Create/Recovery

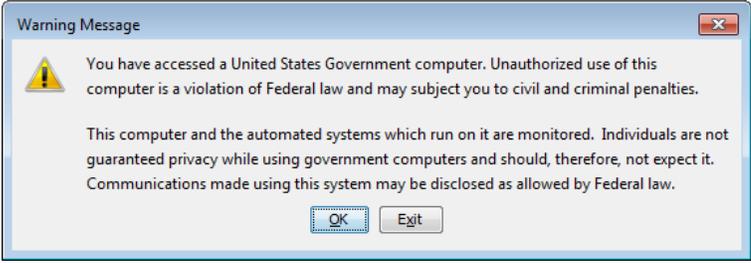
“ITRA Self Service Create/Recovery” feature allows users to create or recover his/her Rudimentary (aka Level-1) token with a new certificate, with no outside assistance. The following section details the procedure for users to follow for creating/recovering their token.

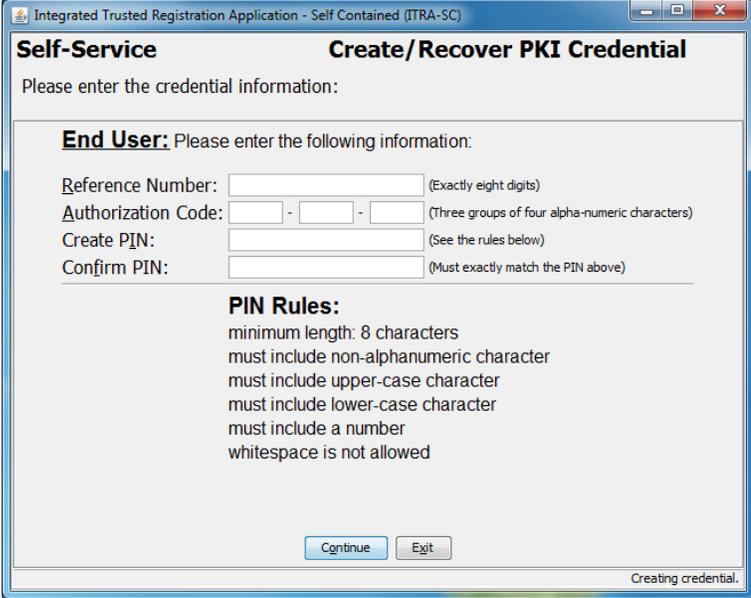
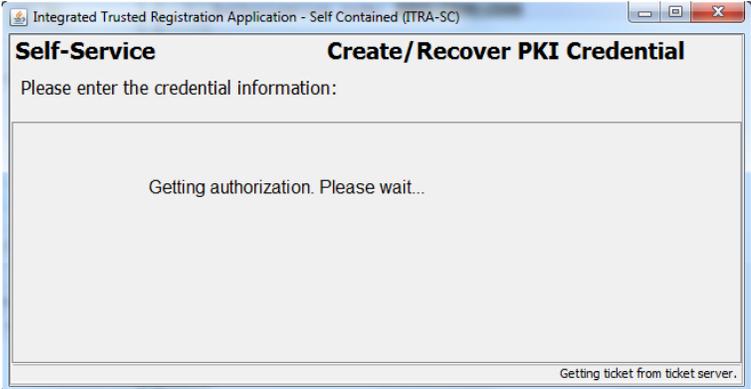
The following steps will create or recover a user’s Rudimentary (aka Level-1) token. The following is required to accomplish these steps: <*User iKey*>, <*Credential PIN*>, <*Reference Number*>, <*Authorization Code*>

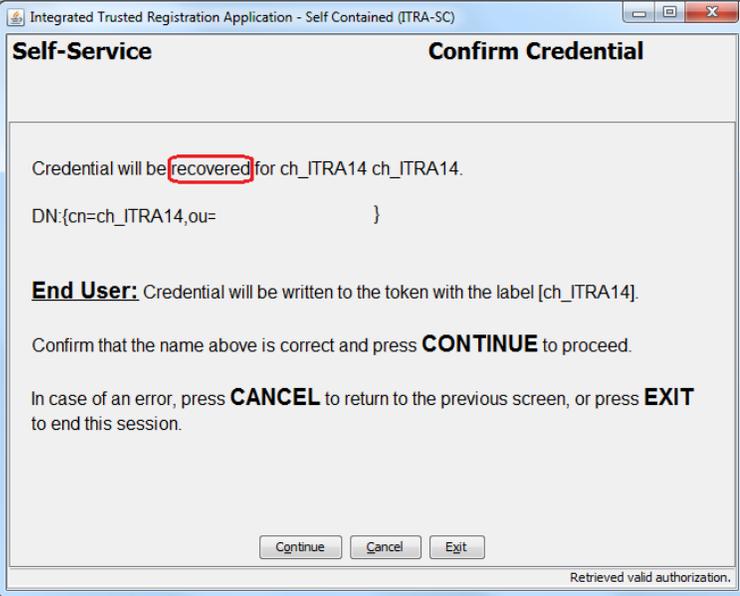
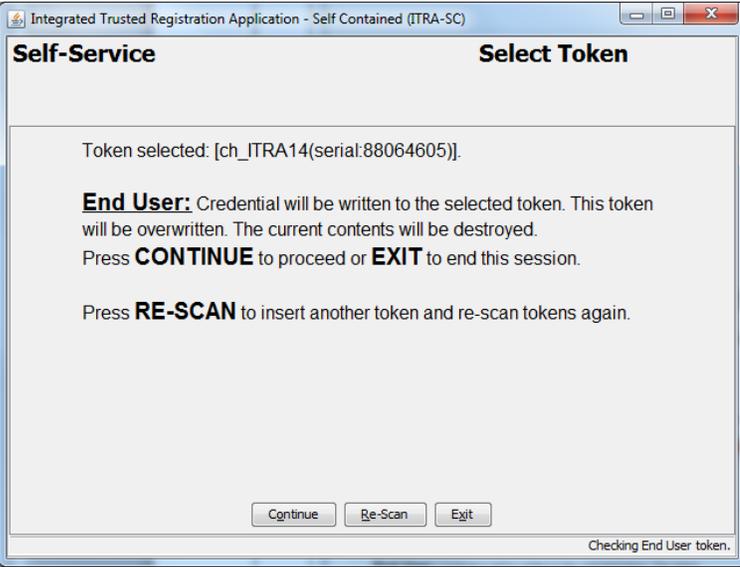


Helpful Hint: If there is no keyboard activity (mouse movement or keyboard entry) for 20 consecutive minutes, ITRA automatically, without prior warning, logs a user out.

Table 3.2-1 Self Service Create/Recovery

<i>Step</i>	Instructions	Comments
1.	Launch ITRA	Section 2.3 contains execution steps
2.	Click [Self Service Create/Recovery]	
3.	Ensure your token is inserted into the USB Reader and a light on the token is illuminated.	
4.	 <p>Read the Warning Message and click [OK]</p>	

Step	Instructions	Comments
5.	 <p>In the field “<u>R</u>eference Number” enter <i><Reference Number></i></p> <p>In the field “<u>A</u>uthorization Code” enter <i><Authorization Code></i></p> <p>In the field “Create <u>P</u>IN” enter <i><Credential PIN></i></p> <p>In the field “Confirm <u>P</u>IN” enter <i><Credential PIN></i></p> <p>Click [Continue]</p>	<p><u>Note:</u> <i><Reference Number></i> and <i><Authorization Code></i> can be obtained by contacting the Fiscal IT Service Desk @ 304-480-7777 and asking for “your Token’s Activation Codes”</p> <p><u>Note:</u> <i><Credential PIN></i> required format is described on the screen, under “PIN Rules”: - 8 Characters minimum - Alpha-Numeric - Must contain 1 Uppercase, 1 Lowercase, 1 Numeric, & 1 Special Character</p>
6.	 <p>Wait for the ITRA server to retrieve the authorization for the credential action.</p>	

Step	Instructions	Comments
7.	 <p>Review the displayed information and confirm the user’s name at the end of the first line.</p> <p>Click [Continue] to proceed.</p>	<p><u>Note:</u> The ITRA Self Service Application will identify whether the credential is being recovered or created. The steps through the application are identical in both cases. The screens will state which operation is being performed (see the circled word “recovered” in the snapshot – it will be replaced with “created” for credential being created.)</p>
8.	 <p>Confirm the correct token was selected and click [Continue]</p>	<p>If multiple tokens are connected to your computer, you will be prompted to select the appropriate token from “PKI Token Selection Dialog” (same as Figure 3-2). To confirm the correct selection, utilize the displayed serial number for token identification.</p> <p>To replace the incorrectly selected token, re-insert the correct token and click button [Re-Scan].</p>

Step	Instructions	Comments
9.	<p>Wait for ITRA to finish writing the selected credential to the selected token</p>	<p>While the system creates (or recovers) the credential, the status message will display information about the specific step that is being performed, in the top left corner of the screen.</p> <p>The examples are:</p>
10.	<p>Review displayed information for accuracy. Remove your token from the USB Reader and click [OK].</p>	<p>Token is now ready for use.</p>

5. TRA Assisted Create/Recovery

“TRA Assisted Create/Recovery” permits a Trusted Registration Agent (TRA) to create or recovery Level-3 tokens for users who require access to Level-3 applications such as SPS, ASAP, and ITS.

5.1 TRA Assisted Create

NOTE: A TRA is required for this process.

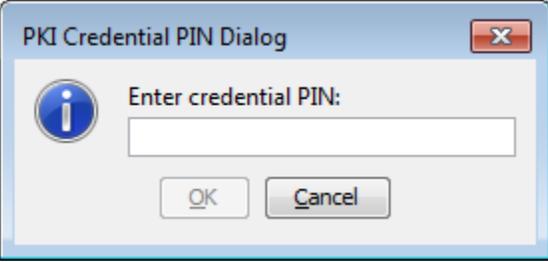
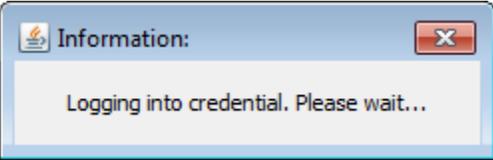
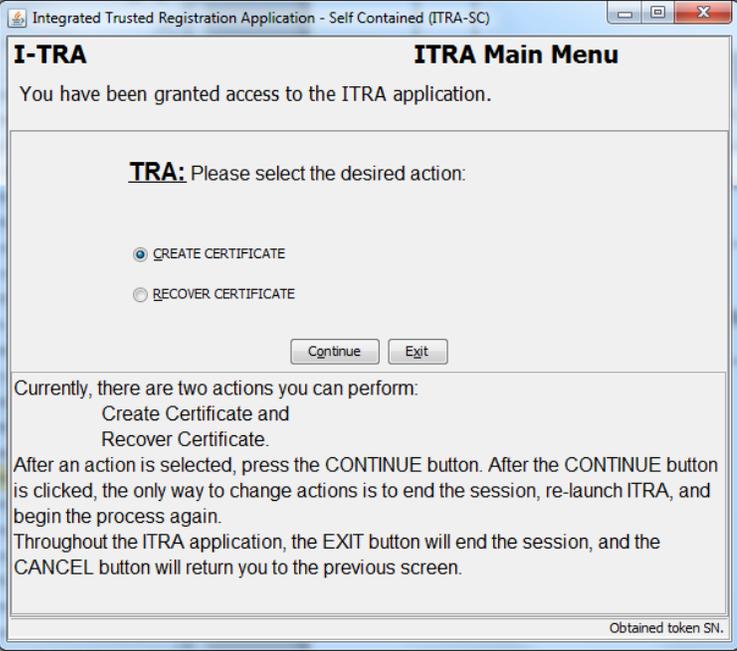
TRAs use the following steps to create a user’s Level-3 token. The following is required to accomplish these steps: <User iKey>, <Reference Number>, <Authorization Code>, <TRA iKey>, and two <Credential PIN> (the TRAs and the Users)

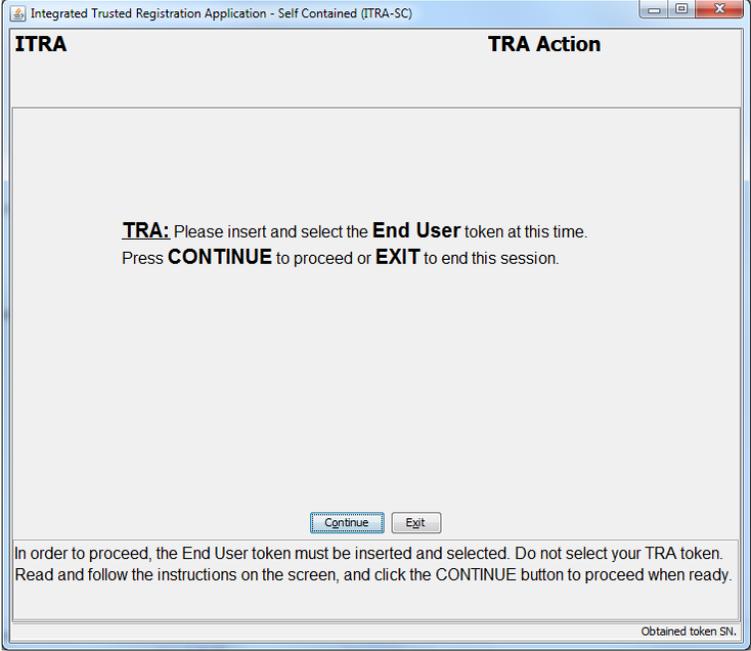
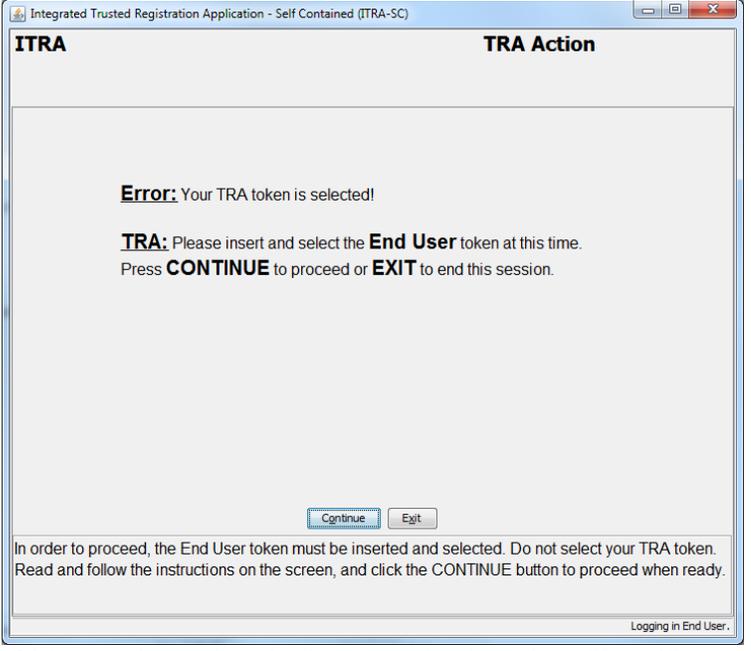


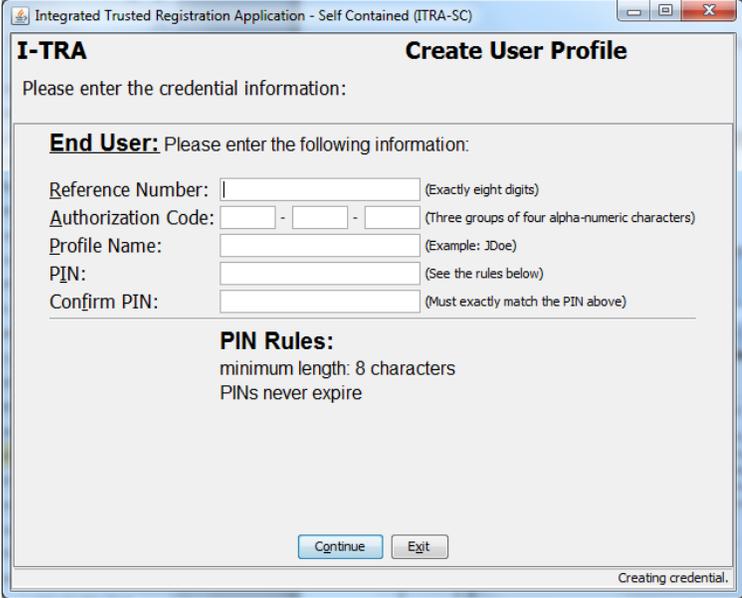
Helpful Hint: If there is no keyboard activity (mouse movement or keyboard entry) for 20 consecutive minutes, ITRA automatically, without prior warning, logs a user out.

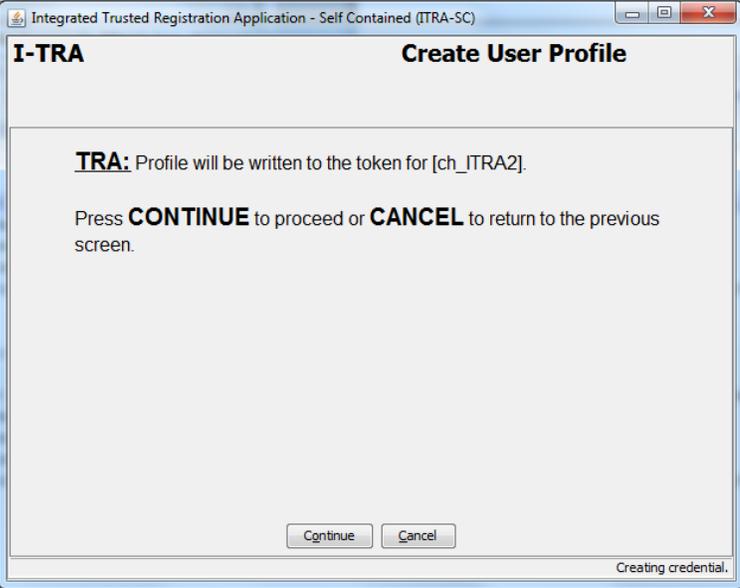
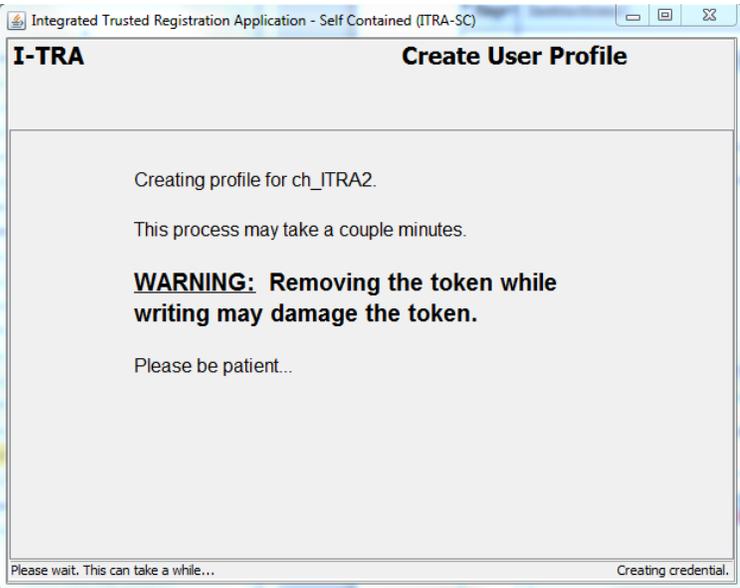
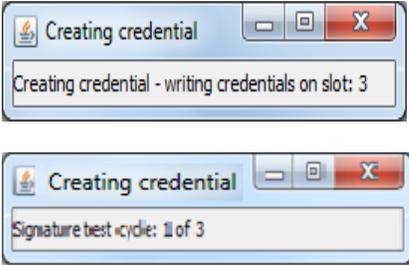
Table 5.1-1 TRA Assisted Create

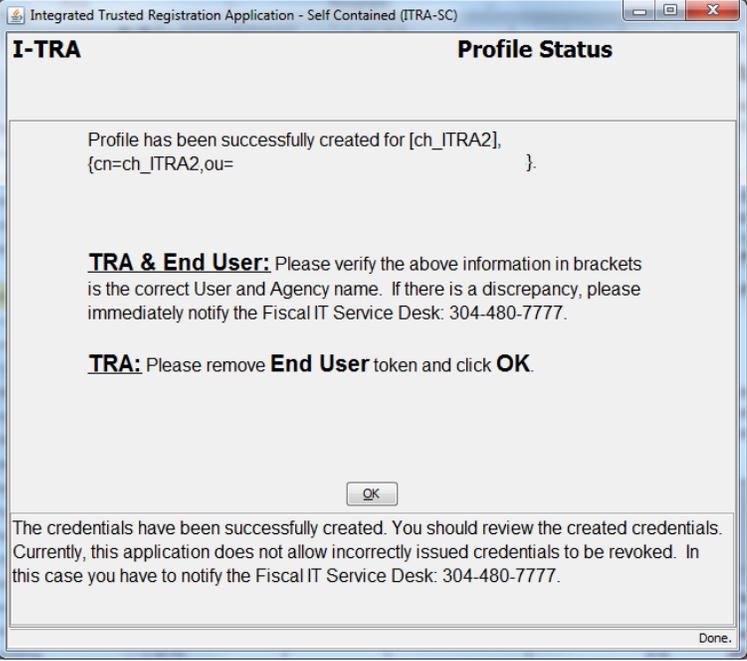
Step	Instructions	Comments
1.	Launch ITRA	Section 2.3 contains execution steps
2.	Click [<u>T</u>RA Assisted Create/Recovery]	
3.	Ensure that <TRA iKey> is inserted into the USB Reader and a light on the token is illuminated.	
4.	<div style="border: 1px solid #add8e6; padding: 10px; margin-bottom: 10px;"> <p style="font-size: small; margin: 0;">Warning Message ✖</p> <p style="margin: 5px 0;"> You have accessed a United States Government computer. Unauthorized use of this computer is a violation of Federal law and may subject you to civil and criminal penalties.</p> <p style="margin: 5px 0; font-size: x-small;">This computer and the automated systems which run on it are monitored. Individuals are not guaranteed privacy while using government computers and should, therefore, not expect it. Communications made using this system may be disclosed as allowed by Federal law.</p> <p style="text-align: right; margin: 0;"> <input type="button" value="OK"/> <input type="button" value="Exit"/> </p> </div> <p>Read the Warning Message and click [<u>O</u>K]</p>	

Step	Instructions	Comments
5.	 <p>Enter the TRA's <Credential PIN> and click [OK]</p>	<p>If multiple tokens are connected to your computer, you will be prompted to select the appropriate token from “PKI Token Selection Dialog” before entering PIN (see Figure 3-2).</p>
6.	 <p>Wait for the system to log you in.</p>	<p><u>Note:</u> if there are updates pending for the TRA credential, the “User Credential Status” screen will display information, similar to Figure 3-1. It is strongly recommended that TRA perform the pending credentials update, as described in Self Service Login process, Step 6.</p>
7.	 <p>Ensure the Create Certificate Radio button is selected and click [Continue]</p>	

Step	Instructions	Comments
8.	 <p>Insert and select <User iKey> in an USB slot and click [Continue]</p>	<p>If the User token is not inserted and selected, the ITRA application will inform the user with warning messages and on-screen text, until the User token selection is done properly.</p> <p>An example of Warning Message:</p> 
9.	 <p>If it's not done already, insert and select the <User iKey> and click [Continue]</p>	<p>This and similar additional instructions could be skipped if the User token selection is completed on Step 8.</p>

<i>Step</i>	Instructions	Comments
10.	 <p>In the field “<u>R</u>eference Number” enter <i><Reference Number></i></p> <p>In the field “<u>A</u>uthorization Code” enter <i><Authorization Code></i></p> <p>In the field “<u>P</u>rofile Name” enter desired text for the token label – it will help to better identify iKey in SafeNet reader.</p> <p>In the field “Create <u>P</u>IN” enter <i><Credential PIN></i></p> <p>In the field “Con<u>f</u>irm PIN” enter <i><Credential PIN></i></p> <p>Click [Continue]</p>	<p><u>Note:</u> <i><Reference Number></i> and <i><Authorization Code></i> can be obtained by contacting the Fiscal IT Service Desk @ 304-480-7777 and asking for “your Token’s Activation Codes”</p> <p><u>Note:</u> The “PIN Rules” displayed on the screen belong to the TRA user’s credential policy. The newly entered <i><Credential PIN></i> required format is:</p> <ul style="list-style-type: none"> - 8 Characters <i>minimum</i> - Alpha-Numeric - Must contain 1 Uppercase, 1 Lowercase, 1 Numeric, & 1 Special Character

<i>Step</i>	Instructions	Comments
11.	 <p>Review the information on the screen and click [Continue]</p>	
12.	 <p>Wait for ITRA to finish writing the selected credential to the selected token</p>	<p>While the system creates the credential, the status message will display information about the specific step that is being performed, in the top left corner of the screen.</p> <p>The examples are:</p> 

Step	Instructions	Comments
13.	 <p>Review displayed information for accuracy. Remove your token from the system and click [OK]</p>	



Helpful Hint: Some times, TRA might select to create a certificate, but the authorization codes had been issued for the key recovery. In such cases, the ITRA will display the “ITRA: Create Error” message (Figure 5-1). The TRA can select the “Recovery” option and proceed with credential recovery without re-entering authorization codes.

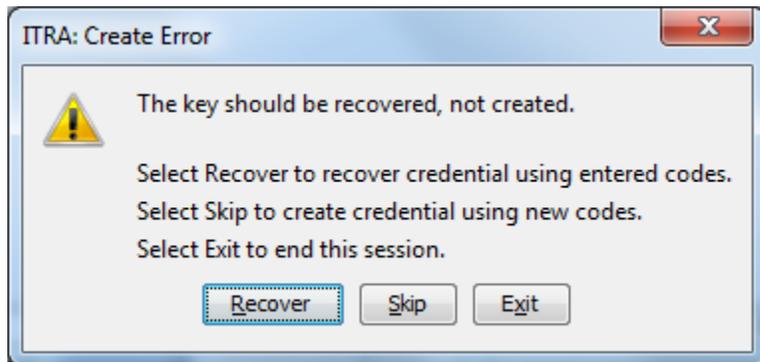


Figure 5-1 TRA Assisted Create Error: the Authorization Codes are valid for Key Recovery

5.2 TRA Assisted Recovery

NOTE: A TRA is required for this process.

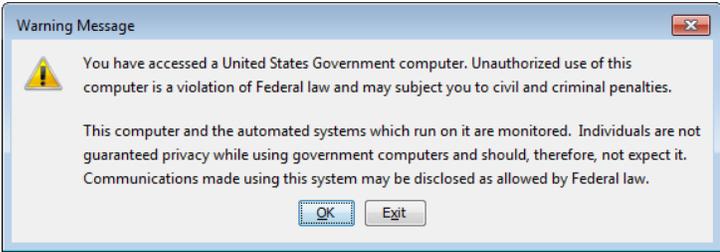
TRAs use the following steps to recover a user's Level-3 token. The following variables are required to accomplish these steps: <User iKey>, <Reference Number>, <Authorization Code>, <TRA iKey>, and two <Credential PIN> (the TRAs and the Users)

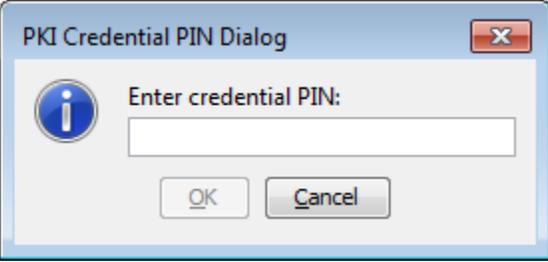
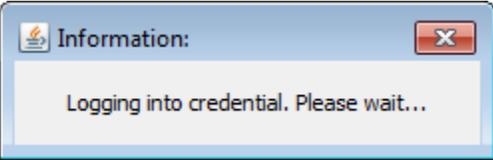
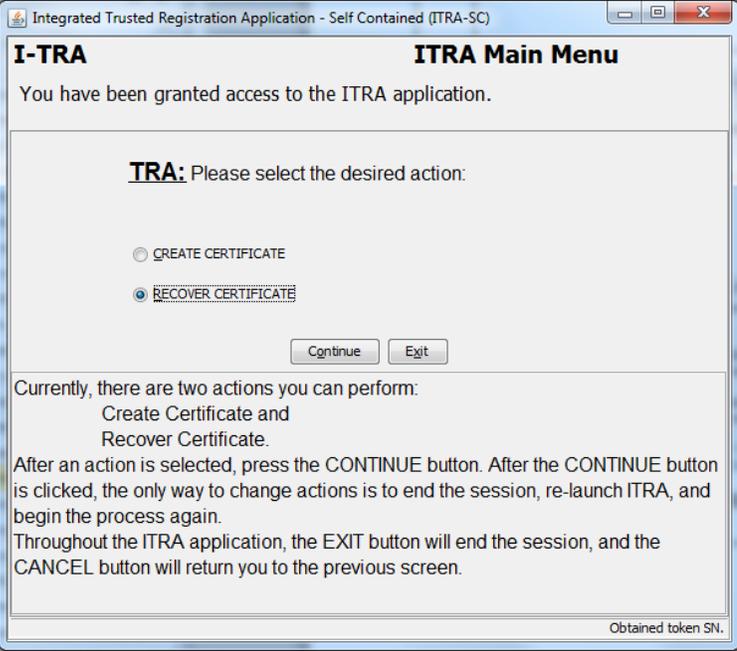


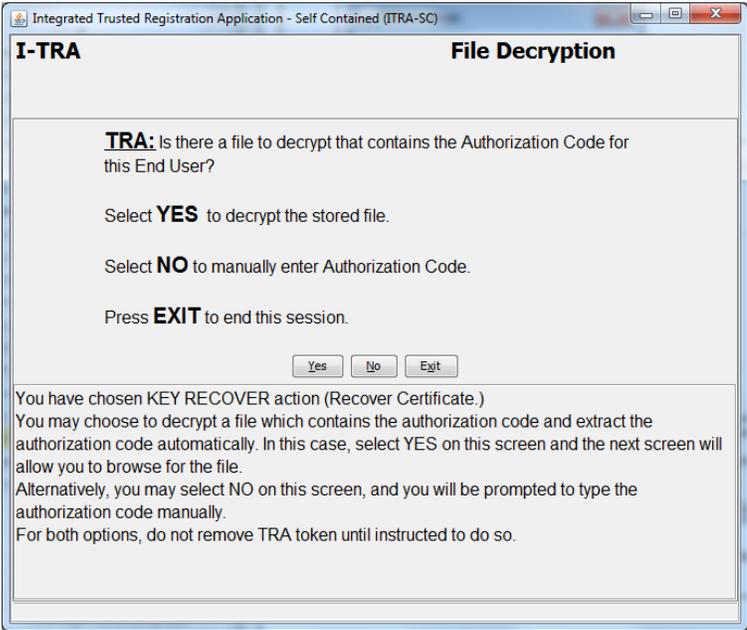
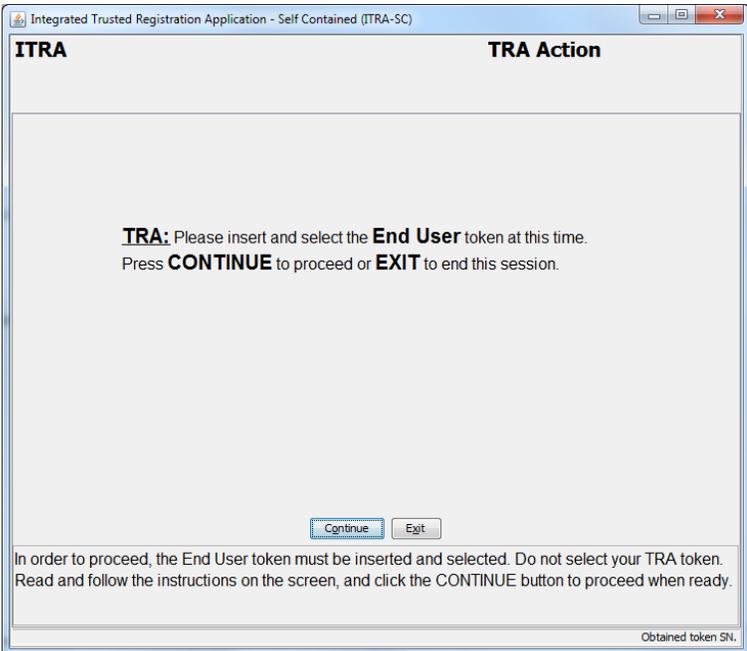
Helpful Hint: If there is no keyboard activity (mouse movement or keyboard entry) for 20 consecutive minutes, ITRA automatically, without prior warning, logs a user out.

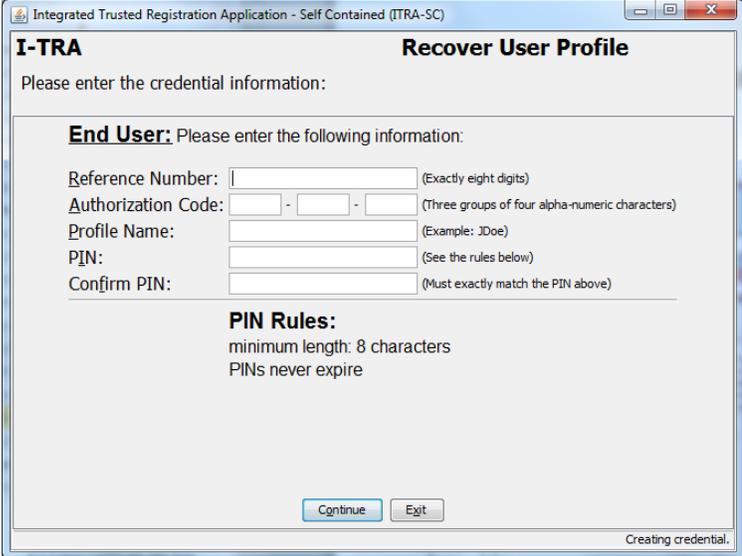
NOTE: TRA Assisted recovery will only recover the PKI Credential currently on the <Users iKey>.

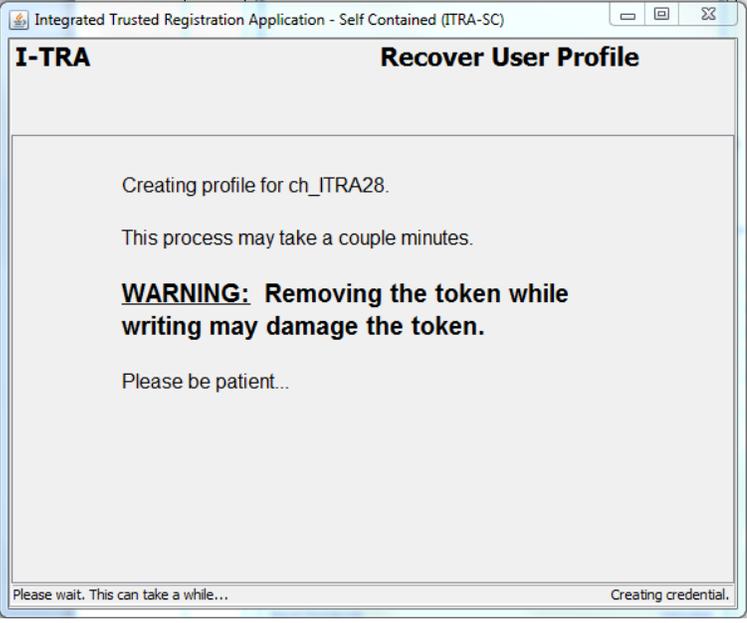
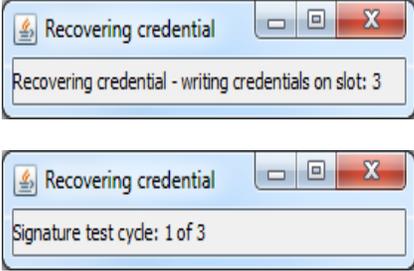
Table 5.2-1 TRA Assisted Recovery

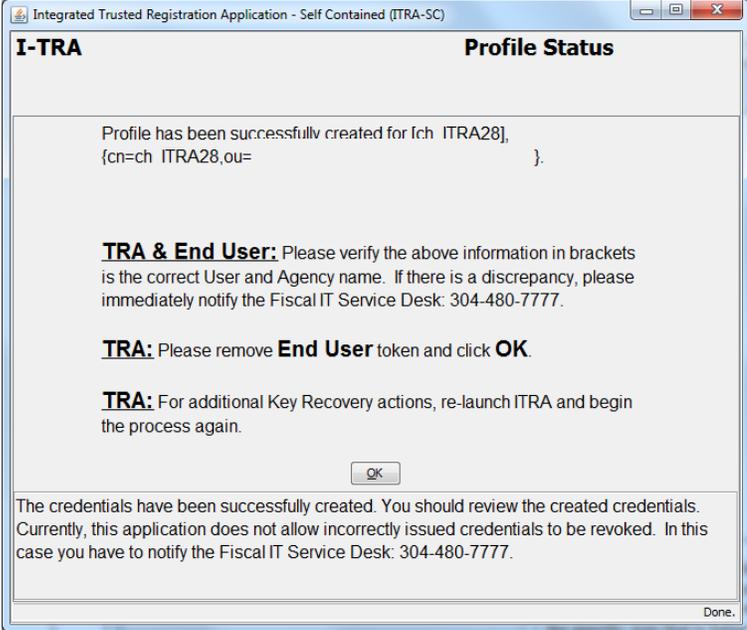
Step	Instructions	Comments
1.	Launch ITRA	Section 2.3 contains execution steps
2.	Click [T RA Assisted Create/Recovery]	
3.	Ensure that <TRA iKey> is inserted into the USB Reader and a light on the token is illuminated.	
4.	 <p>Read the warning and click [QK]</p>	

Step	Instructions	Comments
5.	 <p>Enter the TRA's <Credential PIN> and click [OK]</p>	<p>If multiple tokens are connected to your computer, you will be prompted to select the appropriate token from “PKI Token Selection Dialog” before entering PIN (see Figure 3-2).</p>
6.	 <p>Wait for the system to log you in</p>	<p><u>Note:</u> if there are updates pending for the TRA credential, the “User Credential Status” screen will display information, similar to Figure 3-1. It is strongly recommended that TRA perform the pending credentials update, as described in Self Service Login process, Step 6.</p>
7.	 <p>Ensure the Recover Certificate radio button is selected and click [Continue]</p>	

Step	Instructions	Comments
8.	 <p>The screenshot shows a window titled "Integrated Trusted Registration Application - Self Contained (ITRA-SC)" with a sub-header "I-TRA File Decryption". The main text asks: "TRA: Is there a file to decrypt that contains the Authorization Code for this End User?". Below this, it provides three options: "Select YES to decrypt the stored file.", "Select NO to manually enter Authorization Code.", and "Press EXIT to end this session.". At the bottom, there are three buttons: "Yes", "No", and "Exit".</p> <p>You have chosen KEY RECOVER action (Recover Certificate.) You may choose to decrypt a file which contains the authorization code and extract the authorization code automatically. In this case, select YES on this screen and the next screen will allow you to browse for the file. Alternatively, you may select NO on this screen, and you will be prompted to type the authorization code manually. For both options, do not remove TRA token until instructed to do so.</p>	<p>Note: Authentication Codes are seldom distributed via an encrypted file. If an encrypted file was received please contact IT Service Desk @ 304-480-7777 for proper instructions.</p>
9.	 <p>The screenshot shows a window titled "Integrated Trusted Registration Application - Self Contained (ITRA-SC)" with a sub-header "ITRA TRA Action". The main text says: "TRA: Please insert and select the End User token at this time. Press CONTINUE to proceed or EXIT to end this session.". At the bottom, there are two buttons: "Continue" and "Exit".</p> <p>In order to proceed, the End User token must be inserted and selected. Do not select your TRA token. Read and follow the instructions on the screen, and click the CONTINUE button to proceed when ready.</p> <p>Obtained token SN.</p>	<p>If the User token is not inserted and selected, the ITRA application will inform the user with warning messages and on-screen text, until the User token selection is done properly.</p> <p>An example of Warning Message:</p>  <p>The warning message dialog box is titled "Warning Message" and contains a yellow warning icon and the text: "Your TRA token is selected! Please select an End User token." with an "OK" button.</p>

Step	Instructions	Comments
10.	 <p>In the field “<u>R</u>eference Number” enter <Reference Number></p> <p>In the field “<u>A</u>uthorization Code” enter <Authorization Code></p> <p>In the field “<u>P</u>rofile Name” enter desired text for the token label – it will help to better identify iKey in SafeNet reader.</p> <p>In the field “Create <u>P</u>IN” enter <Credential PIN></p> <p>In the field “<u>C</u>onfirm PIN” enter <Credential PIN></p> <p>Click [Continue]</p>	<p>Note: <Reference Number> and <Authorization Code> can be obtained by contacting the Fiscal IT Service Desk @ 304-480-7777 and asking for “your Token’s Activation Codes”</p> <p>Note: The “PIN Rules” displayed on the screen belong to the TRA user’s credential policy. The newly entered <Credential PIN> required format is:</p> <ul style="list-style-type: none"> - 8 Characters <i>minimum</i> - Alpha-Numeric - Must contain 1 Uppercase, 1 Lowercase, 1 Numeric, & 1 Special Character

<i>Step</i>	Instructions	Comments
11.	 <p>Review the information on the screen and click [Continue]</p>	
12.	 <p>Wait for ITRA to finish writing the selected credential to the selected token</p>	<p>While the system recovers the credential, the status message will display information about the specific step that is being performed, in the top left corner of the screen.</p> <p>The examples are:</p> 

Step	Instructions	Comments
13.	 <p>The screenshot shows a dialog box titled "I-TRA Profile Status". The text inside reads: "Profile has been successfully created for [cn=ch ITRA28,ou=...].", "TRA & End User: Please verify the above information in brackets is the correct User and Agency name. If there is a discrepancy, please immediately notify the Fiscal IT Service Desk: 304-480-7777.", "TRA: Please remove End User token and click OK.", and "TRA: For additional Key Recovery actions, re-launch ITRA and begin the process again." There is an "OK" button at the bottom.</p> <p>Review displayed information for accuracy. Remove your token from the system and click [OK]</p>	



Helpful Hint: Some times, TRA might select to recover a certificate, but the authorization codes had been issued for the credentials creation. In such cases, the ITRA will display the “ITRA: Key Recovery Error” message (Figure 5-2). The TRA can select the “Create” option and proceed with credential creation without re-entering authorization codes.

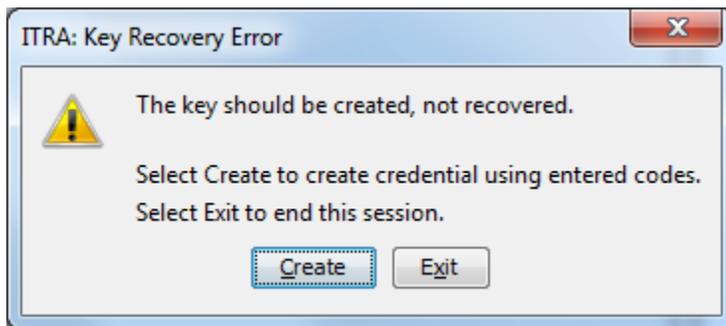


Figure 5-2 TRA Assisted Key Recovery Error: the Authorization Codes are valid for Credentials Creation

Appendix A – Troubleshooting Tips

A-1 General Issues

The following items will cover common errors a user may receive while using ITRA or common actions a user may need to take.

A-1.1 ITRA Maintenance Page

When ITRA application is shut down for maintenance, the users will not be able to access the normal ITRA screen, as shown in Figure 2-2, and instead, the approximated maintenance web page will be displayed (see Figure A-1):

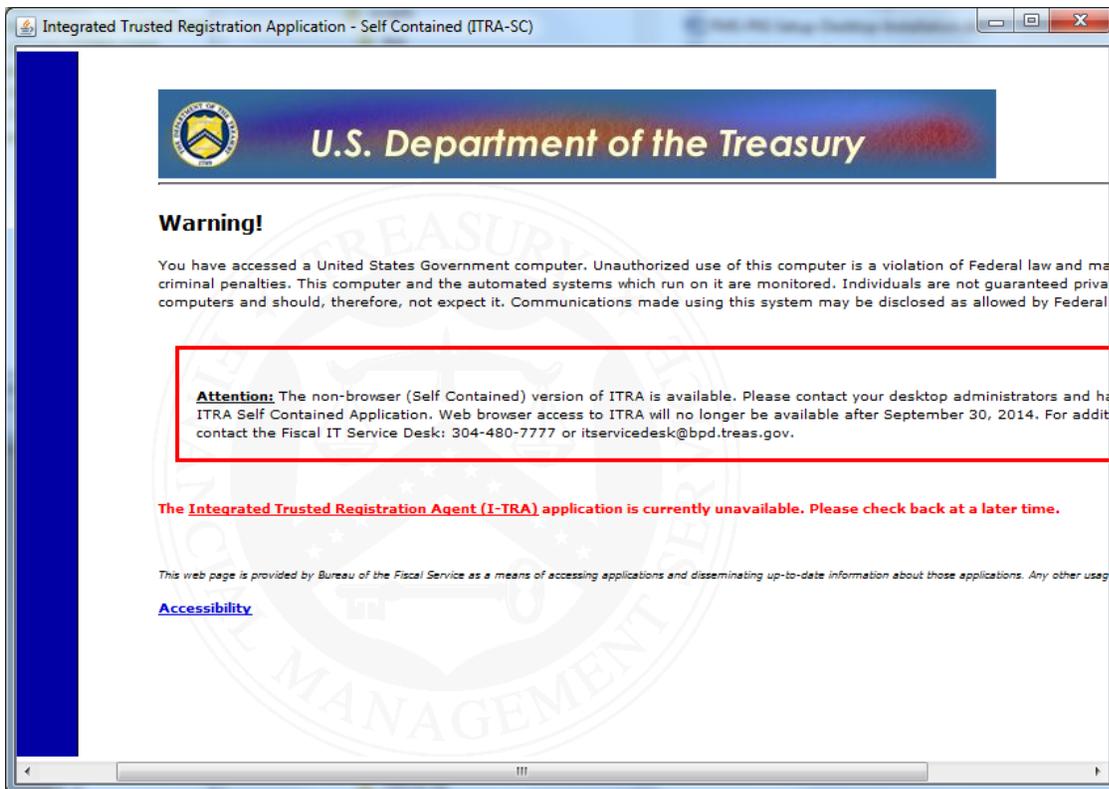


Figure A-1 ITRA Maintenance Page displayed on ITRA Self-Contained main screen

When the ITRA maintenance page is displayed, the users can only wait for ITRA to be started in its normal mode. The users may call the Fiscal IT Service Desk, to inquire when ITRA is planned to become available.

A-1.2 ITRA Cannot Connect to Server

There are many different reasons why ITRA client is unable to connect to ITRA server. The user will receive the Fatal Error (Figure A- 2) that indicates that system is “Unable to start ITRA”.

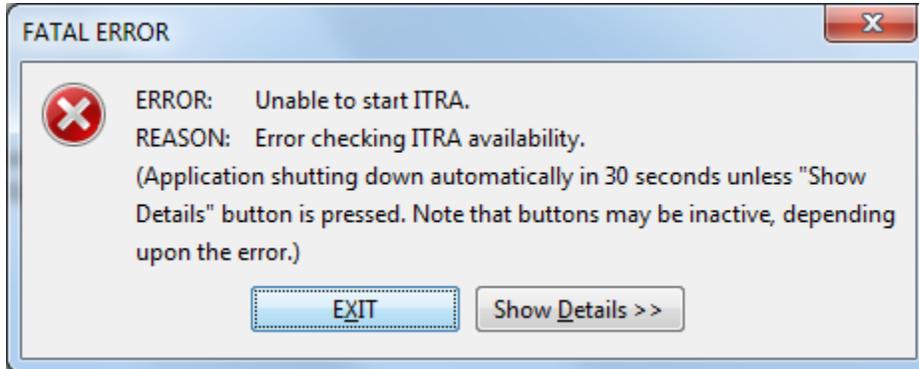


Figure A- 2 Fatal Error message: Unable to start ITRA

It is very important to collect as much information as possible about this error and send all collected information to the Fiscal IT Service Desk. See Section A-5 for instructions on collecting error information.

A-2 Issues with Security Token (iKey)

When ITRA application cannot find any tokens attached to the user’s workstation, it will display a corresponding error message.

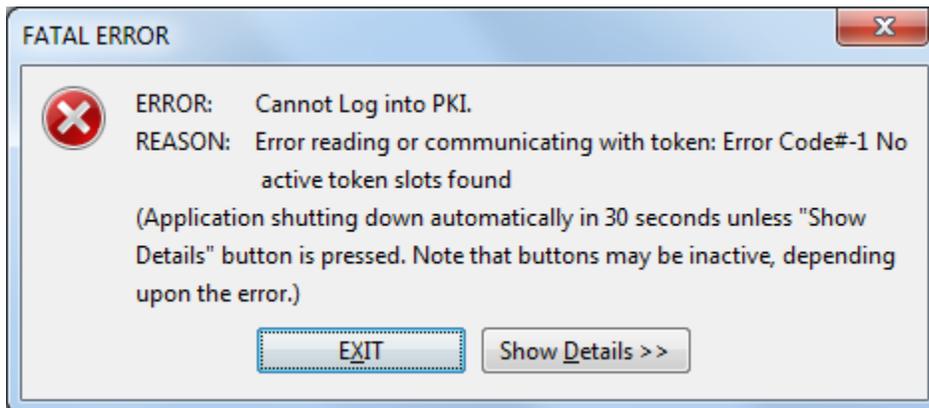


Figure A- 3 ITRA Cannot Find Token (iKey)

Another indication that iKey is not found is a Warning Message as shown on Figure A- 4.



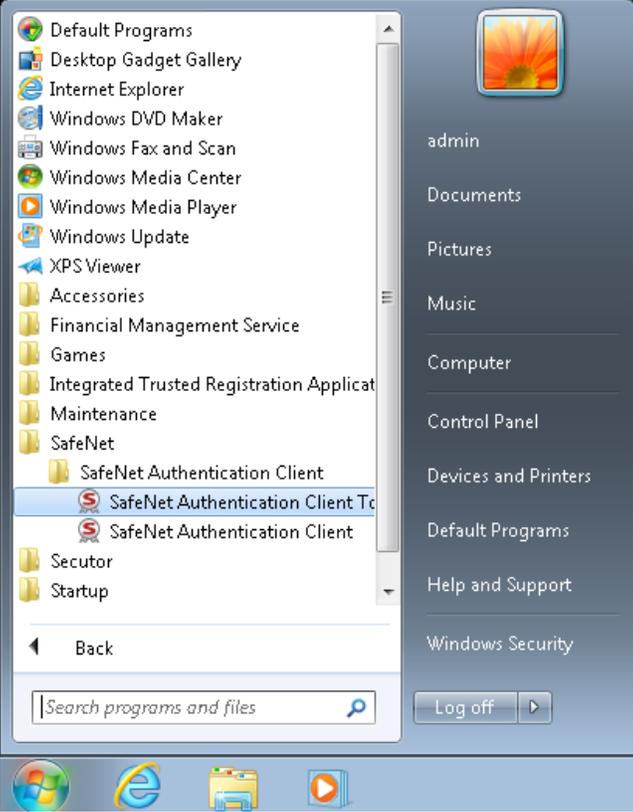
Figure A- 4 Self Service Create/Recovery: Cannot Find Token (iKey or eToken)

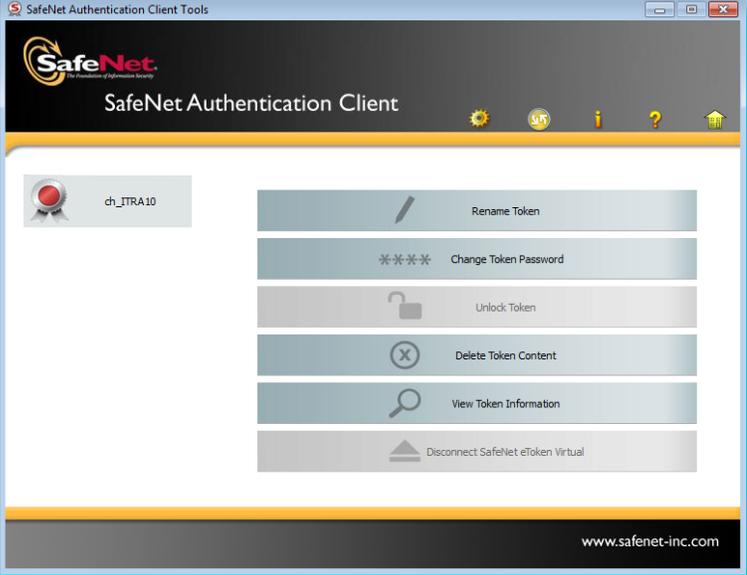
The users may follow the steps below, to attempt to remedy the issue.

A-2.1 View iKey/eToken Contents

Accomplish the following step to view the certificates on a token. Successfully accomplishing this task proves your token is properly inserted in the computer.

Table A-2-1 View Token Contents

Step	Instructions	Comments
1.	Insert <User iKey> into a USB port and wait for a light on the token to illuminate	
2.	 <p>Click Start -> All Programs -> SafeNet -> SafeNet -> SafeNet Authentication Client Tools</p>	

Step	Instructions	Comments
3.	 <p>If you receive a Screen similar to the above, then the inserted iKey is recognized by SafeNet.</p>	<p>Note: if you receive a screen in which the left hand space is blank, then SafeNet is not recognizing the iKey. Attempt to re-insert the offending iKey and refresh the window. If problem persist contact the Fiscal IT Service Desk @ 304-480-7777 for resolution.</p>

If the SafeNet correctly displays the token, then please collect the information as described in Section A-5 and send the detailed information to the Helpdesk. The most probable cause of this problem is incomplete installation of SafeNet, but this should be confirmed by Helpdesk.

A-3 Issues with Login to ITRA

When the token is recognized by SafeNet and ITRA, the login to ITRA might still fail for numerous reasons. This document only lists the two cases that are relatively easy to identify and take appropriate action. For all other errors, users should collect the detailed information (see Section A-5) and contact Fiscal IT Service Desk for additional help.

A-3.1 Your Certificate Has Expired

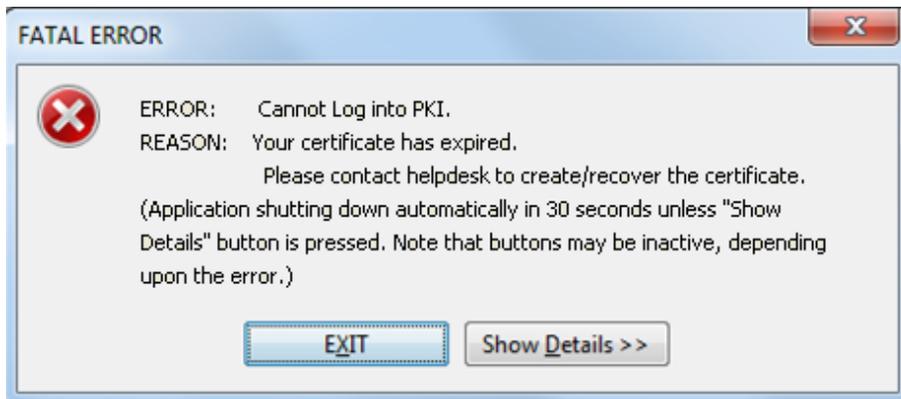


Figure A-5 Login Failed: Expired Certificate

Receiving this error means the PKI credential has expired. The user must contact his/her Help Desk for more information and probably, start Key Recovery process.

A-3.2 TRA Access Fails

A user who can perform TRA role must have a valid token (iKey or eToken) with Level-3/Medium Hardware-Assurance credentials. In addition, a special PKI role “TRA” must be assigned to the TRA credentials in the PKI. If any of these requirements have not been satisfied, access to the “TRA Assisted Create/Recovery” functionality of ITRA will be denied to the user.

If the TRA certificate expired, the TRA user will not be able to login to perform TRA Assisted Create/Recovery actions: see Section A-3.1.

When the TRA certificates are currently valid, there can be denial of access if credentials are not Level-3. The resulting error message is shown on Figure A- 6.

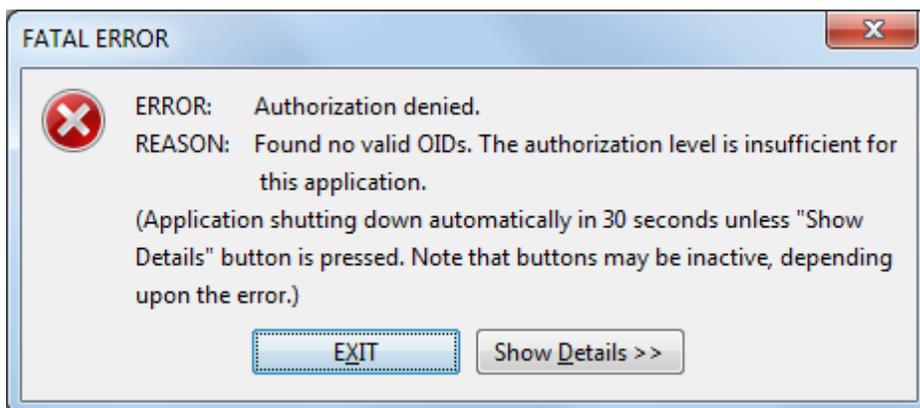


Figure A- 6 TRA Login Failed: credentials must be Level-3

When the TRA certificates are currently valid and are Level-3, the TRA login will fail if the user is not assigned TRA role. The resulting error message is shown on Figure A- 7.

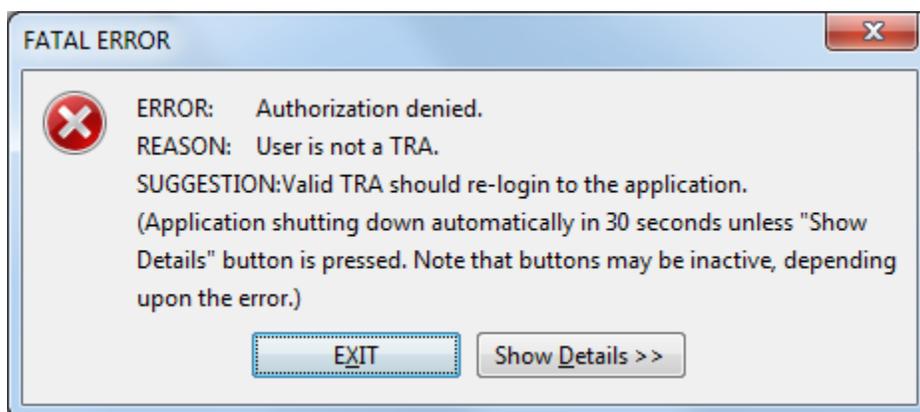


Figure A- 7 TRA Login Failed: User is not a TRA

In all cases, the user should find a TRA who can successfully login to the ITRA and perform TRA Assisted Create and Recover actions. Call the helpdesk if you need help locating such TRA user.

A-4 Issues with Credential Management

There are many different causes that might lead to failure of credential management. This document only lists the two cases that are relatively easy to identify and take appropriate action. For all other errors, users should collect the detailed information (see Section A-5) and contact Fiscal IT Service Desk for additional help.

A-4.1 Bad Reference ID

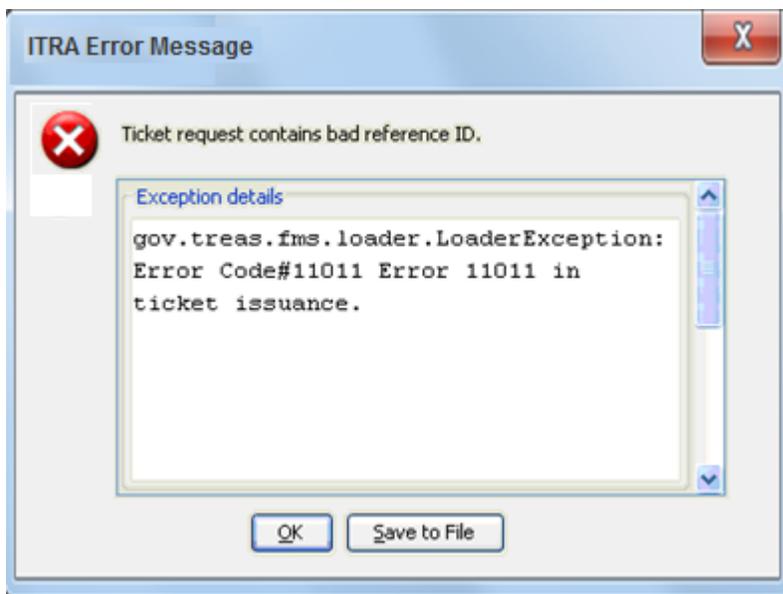


Figure A- 8 Error Message: Bad Reference ID

A bad <*Reference Number*> was entered during one of the following steps:

- Step 5 of Self Service Create Recovery:

- The most probable cause is mis-typed number.
- Another option is using self-service create/recover process for Level-3 credentials. If this is the case – the user must use TRA Assisted create/recover process.

- Step 10 of TRA Assisted Create or Step 10 of TRA Assisted Recovery:

- The most probable cause is mis-typed number.
- Another option is the reference number that is already used.

User should click **[OK]** and attempt the appropriate step again. If the problem persists, please contact the IT Service Desk to confirm the Reference Number.

A-4.2 Authorization Codes Do Not Match

The authorization codes must match, for the credential management to complete successfully. When the reference number and Authorization Code do not match, the credential creation fails with the error shown on Figure A- 9.

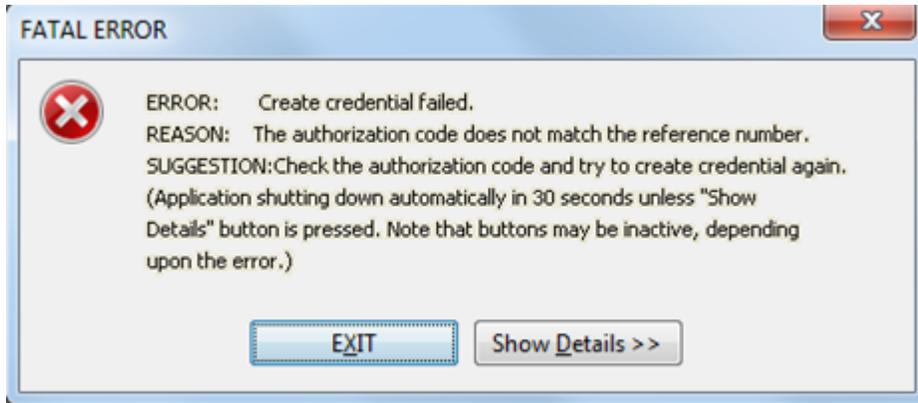


Figure A- 9 Authorization Codes do not match

The <*Authorization Code*> does not match the <*Reference Number*> during **Self Service Create/Recovery** or **TRA Assisted** Tasks. User should capture error message by following directions outlined in Section A-5, and open a ticket with the IT Service Desk

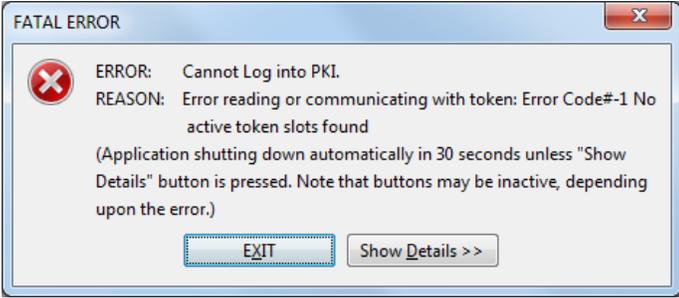
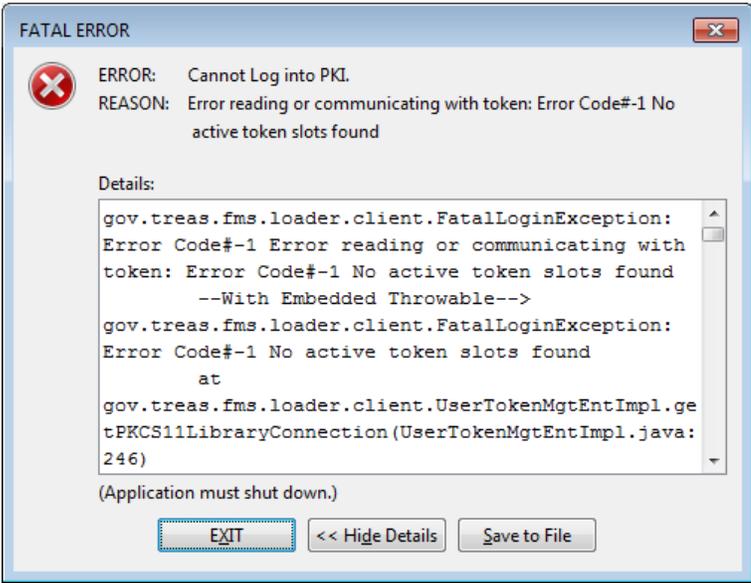
A-5 Collect Information for Helpdesk Ticket

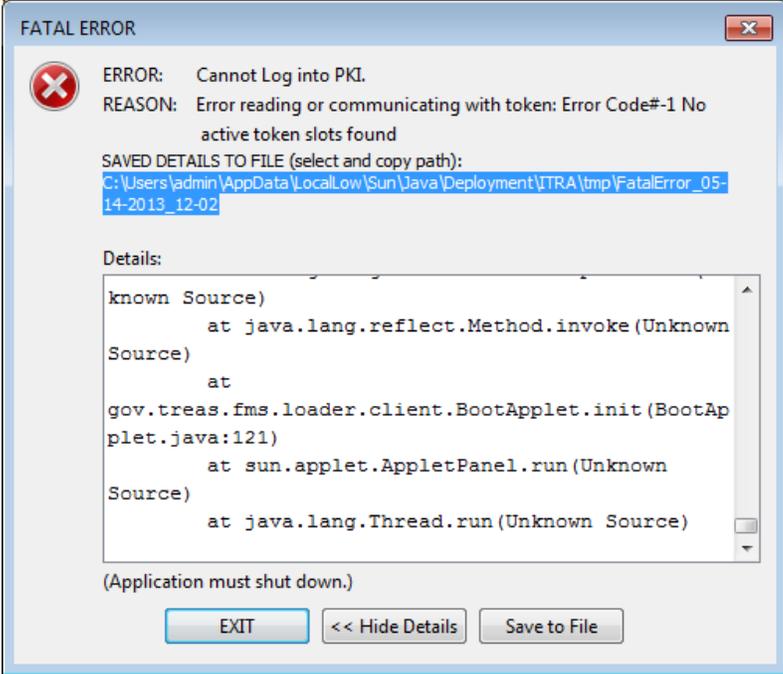
When an ITRA user requests help from the Fiscal IT Service Desk, any details about the error will greatly speed up the problem resolution. That is why the ITRA developers provided several convenient ways to assist ITRA users with collecting important information about ITRA client installation and errors that might occur. Please follow the steps specified below and attach the resulting text files to the email with your service ticket request.

A-5.1 Capture Error Details for Helpdesk Ticket

The following steps should only be accomplished at the direction of the IT Service Desk. The following details how to properly save the error message output the IT Service Desk Personnel will require to resolve the error.

Table A-5-1 Capture Error Details into the file

<i>Step</i>	Instructions	Comments
1.	 <p>Click [Show Details>>]</p>	
2.	 <p>Click [Save to File]</p>	

<i>Step</i>	Instructions	Comments
3.	 <p>The Error is saved to the identified location and file name under the SAVED DETAILS TO FILE line (highlighted above)</p>	<p>The information in this file will need to be sent to the IT service desk: Users should browse to the stored file location and attach file to an email.</p>

A-5.2 Capture ITRA Execution Thumbprint

The following text file could be found in the local ITRA installation directory [ITRA_HOME]:

C:\ [ITRA_HOME]\tmp\ItraExecThumbPrint.txt

The information in this file will need to be sent to the IT service desk: Users should browse to the stored file location and attach file to an email.