



Bureau of the Fiscal Service

Integrated Trusted Registration Application

ITRA

Troubleshooting Guide

Document Version 10.0 – 07/12/13

Change Table

Version	Date	Change Description	Section/Page
V1.0	05/12/06	Initial Version	All
V2.0	06/16/06	Release 3.0 – Updated to reflect changes added in ITRA v3.0 CR39	Section 3, 4
V3.0	09/26/06	Release 4.0 - Updated to reflect changes added in ITRA v4.0 CR42	Section 1, 3, 4 (new), 5
V4.0	02/01/07	Release 4.0.6 – Updated to reflect changes added in ITRA v4.0.6 CR71	Section 2.2.1
V5.0	05/11/07	Release 4.1 – Updated to reflect changes added in ITRA v4.1 CR85 – password PIN CR83 – exp cred error msg	All Section 3.3
V6.0	06/11/07	Release 4.01.1 – Updated to reflect changes added in ITRA v4.01.1 CR99	Section 4
V7.0	06/28/07	Release 4.01.2 – Updated to reflect changes added to ITRA v4.01.2 CR96	All
V7.1	09/26/07	Release 4.02.2 – Updated to reflect changes added to ITRA v.4.02.2 CR103	Section 4.2
V7.2	05/02/08	Release 5.0 – Updated screenshots to mask DN details	Section 2.2.1
V8	01/28/11	Release 5.01.4 – Update for Windows 7	Sections 6.8 and 6.10
V8.1	03/14/11	Rel 5.01.5 Updated for Java 64-bit and known issues in Windows 7	Added Section 3
V9.0	05/15/12	Rel 5.01.8 Updated for Rudimentary OID	All
V10.0	06/30/13	ITRA-SC	Sections 3 and 7

TABLE OF CONTENTS

1.	INTRODUCTION TO ITRA.....	5
2.	INTRODUCTION TO DOCUMENT AND ERROR NAVIGATION	6
2.1.	Document Summary	6
2.2.	Error Navigation.....	6
2.2.1.	Fatal Errors	6
2.2.2.	Non Fatal Errors.....	10
3.	ITRA WEB & ITRA-SC	11
3.1.	Legacy FMS PKI Installer (JAVA Applet – Browser)	11
3.2.	ITRA-SC – Java App (Stand-alone).....	14
3.3.	Known Issues with Windows 7	14
4.	ERRORS DURING LOG IN / CHANGE PIN.....	16
4.1.	Workstation Configuration Errors.....	16
4.2.	PKI Connectivity Errors.....	17
4.3.	User Login Process Errors.....	18
5.	CREDENTIAL STATUS NOTIFICATION AND UPDATE ERRORS	21
5.1.	Credential Status Notification issues.....	21
5.2.	Credential Update errors	22
6.	ITRA - APPLICATION ERRORS	26
6.1.	Lost Connection to CA.....	26
6.2.	Wrong Data for Processing	27
6.2.1.	TRA Assisted Mode	27
6.2.2.	Self-Service Create/Recover (Level 1).....	30
6.3.	Creation Limit Error (TRA Assisted).....	32
7.	GENERAL TROUBLESHOOTING	33
7.1.	SPS Tools and Notes	33
7.2.	Administrative Rights During Installation	33
7.3.	Directory Rights	33
7.4.	Web Site Does Not Appear	33
7.5.	Web Site Validation Warning	33
7.6.	Applet Does Not Start	34
7.7.	Java Code Signature Warning	34
7.8.	Token Not Visible or Token Service Not Started	34
7.8.1.	If using Datakey CIP Utilities	34

7.8.2.	If using Safenet Authentication Client.....	35
7.9.	SSL Connection Failure	35
7.10.	Cannot (Fully) Uninstall or Re-Install Datakey CIP	35
7.11.	Turn On Debugging for ITRA Web	35
7.12.	Turn On Debugging for ITRA Self-Contained	36

1. Introduction to ITRA

The Integrated Trusted Registration Agent (ITRA) is a system for creating and recovering PKI credentials. The client component of this system (the ITRA Client) is a PKI-token enabled Java thin-client. The client workstation requires only that an approved token reader and driver be installed, along with an appropriately installed Java runtime environment. The technology for such a client was developed, deployed, and proven as part of the Secure Payment System (SPS) project. This technology is expanded and re-used as the foundation for the ITRA Client, without dependencies on SPS. The ITRA Client is extensible to include new features that facilitate user enrollment and management.

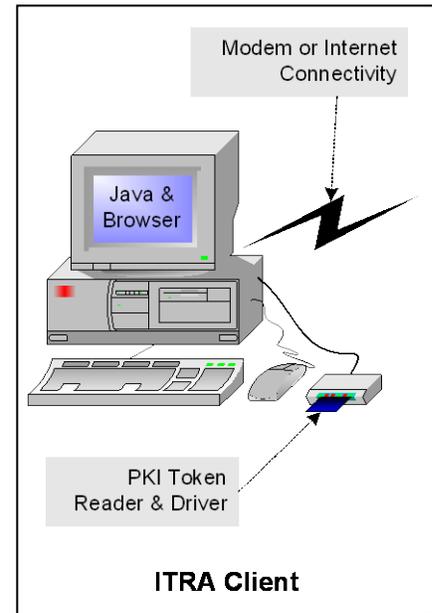
Currently, the ITRA provides two modes of operation:

1. **“TRA Assisted”** use of ITRA, for which TRA intervention is needed, and applies specifically to creation and recovery of high assurance Level-3 users’ credentials;
2. **“Self Service”** use of ITRA, which is available for all other ITRA functions, for which a TRA does not need to intervene. This specifically applies to creation and recovery of Level-1 users’ credentials. Both Level-1 and Level-3 users can use Self Service mode for PIN changes and certain credential management/update operations.

There is also a distinction made between:

1. **Level-1/Low-Assurance Credentials** that do not require in-person proofing to obtain, and have a streamlined acquisition process. TCIS and DebtCheck are examples of applications only requiring Level-1 credentials for access.
2. **Level-3/High-Assurance Credentials** that require in-person proofing and a rigorous vetting process to obtain. SPS and ASAP are examples of applications requiring Level-3 credentials for access.

This document describes the error messages that may be received while running ITRA in either mode of operation, their possible solutions, and general troubleshooting.



2. Introduction to Document and Error Navigation

2.1. Document Summary

This document is intended to help ITRA users with errors that they may receive when using ITRA. The ITRA errors are separated into three categories – log in errors, credential notification and update errors, and application errors. Errors are marked accordingly if they only apply to one set of users (Self Service users or TRA Assisted users). If the user is not able to find the correct error, he/she may use the index, which includes words that should help the user locate his/her problem. Each category will include a summary of the errors it contains, and then proceed with a more complete description and suggested actions, if possible.

A general troubleshooting guide has been provided in this document to help with common problems when accessing the ITRA application.

The user may call the Help Desk if his/her problem is not resolved.

2.2. Error Navigation

2.2.1. Fatal Errors

All fatal errors found in ITRA will follow the same format and will be similar to the following screens. Please note that this is only an example and the actual errors found in the application may not exactly match the details of the error in this section's examples.

The initial screen that appears will be similar to Figure 1. The text in the error message will include the following information:

- ERROR: the name of the error received
- REASON: the reason the error has been received
- SUGGESTION (if available): A possible action to resolve the problem encountered
- Buttons (not on all screens): Exit, Show Details, Hide Details, Save to File

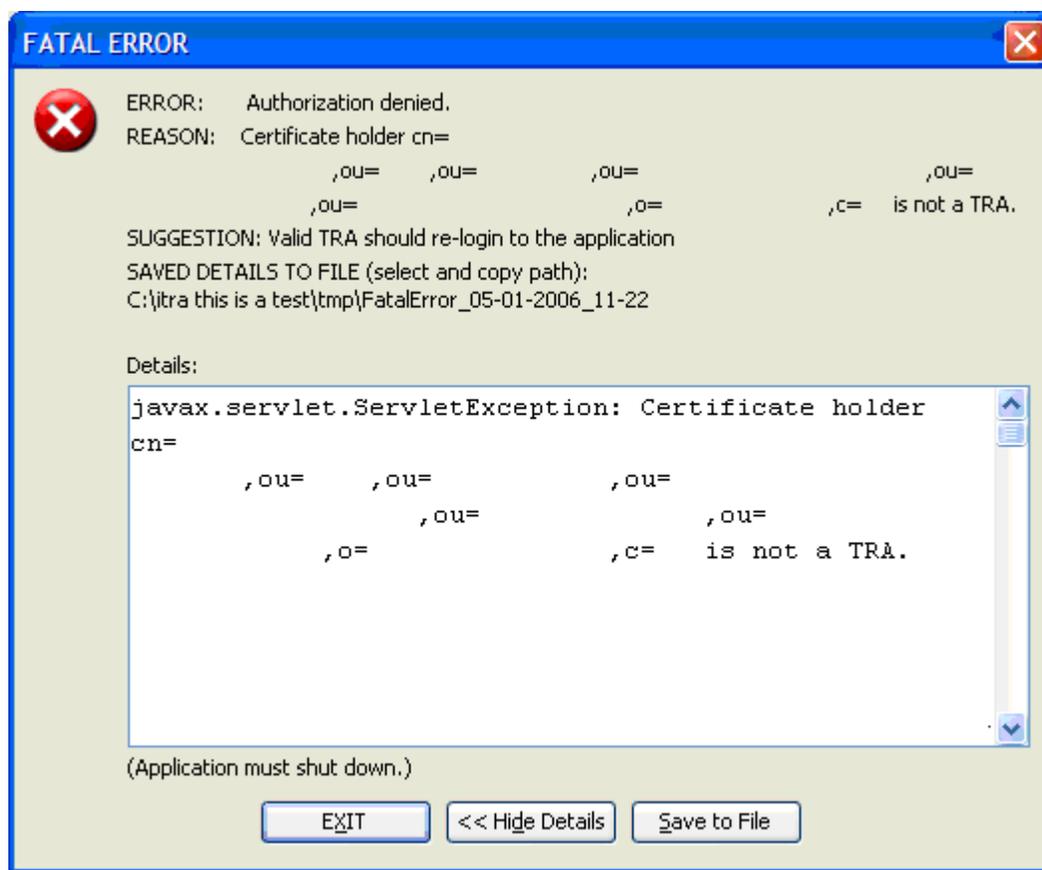


Figure 3

This saved text file will include the following information:

```

FATAL ERROR
DATE AND TIME: [date, time, and local zone]
ERROR: [ERROR as on Fatal Error screen]
REASON: [REASON as on Fatal Error screen]
SUGGESTION: [SUGGESTION as on Fatal Error screen]

-----
[Complete Details text]
-----
[System Environment Information]
-----
[Loader Configuration Information]
-----
[Complete System Properties]

```

If the file cannot be saved, a figure similar to Figure 4 will appear. The user may select the text in the “Details” section and manually save it in a text file.

2.2.2. Non Fatal Errors

The non fatal errors that may appear in ITRA are application errors. Different screens and options will appear, depending on the cause of the error. The detailed information included in the error description in this document will explain the options available.

3. ITRA Web & ITRA-SC

This Section is concerned with ITRA as it evolved from web/java applet-based (ITRA Web) to standalone java application (ITRA-SC). The web/applet model needed to take into consideration the agency's standards for its java plug-in. When an update was pushed out, it was also necessary to update the corresponding Java Cryptographic Extensions (JCE). The FMS PKI Installer had to review the client's Windows OS, client smartcard middleware, browser version, java plug-in version and OS environment (64 or 32-bit).

Since ITRA-SC is self-contained it does not concern itself with Windows OS environment (64 or 32-bit), whether the JCE needs to be reapplied or the version of the Java plug-in standardized by the agency. Standardizing an ITRA-SC client environment is intended to make troubleshooting less an ordeal by reducing variability.

The ITRA functions have not changed and therefore the errors encountered are common to both the Legacy Installer and ITRA-SC.

3.1. Legacy FMS PKI Installer (JAVA Applet – Browser)

The disk for the former FMS PKI Installer was designed for multiple operating systems and supports different middleware for each. As a result, the software that is installed when running the FMS PKI Installer will vary with the operating system being used.

The table below shows possible installation scenarios for the FMS PKI installation. The installer will detect whether any of the software in the **Programs on Machine Prior to Install** column is currently installed. The **Expected Outcome** column shows which software the FMS PKI installation will install for each scenario. The following files will always be installed during a full install and are not included in the Expected Outcome column:

- FMS PKI with the high crypto JAR files and certificates
- ITRA Program Files and ITRA Documentation
- TWAI PKI with Entrust Applet certificate

DataKey CIP Utilities is not compatible with Windows 7 so scenarios for DataKey CIP Utilities on a Windows 7 machine are not included. SafeNet Authentication Client is compatible with both Windows XP and Windows 7 and will be installed in the absence of middleware in both cases.

Operating System	Programs on Machine Prior to Install		Expected Outcome
	Middleware Installed	Java Runtime Environment (JRE) Installed	
Windows XP	No Middleware	No JRE	<ol style="list-style-type: none"> 1. 32-bit SafeNet Authentication Client and iKey drivers installed 2. Java version 1.6.0_27 installed 3. cacerts, trusted.certs, and java.security files are installed

			4. local_policy.jar installed
Windows XP	No Middleware	Version prior to 1.6.0_27	<ol style="list-style-type: none"> 1. 32-bit SafeNet Authentication Client and iKey drivers installed 2. Java version 1.6.0_27 installed 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows XP	No Middleware	1.6.0_27	<ol style="list-style-type: none"> 1. 32-bit SafeNet Authentication Client and iKey drivers installed 2. No Java software is installed (already present) 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows XP	DataKey CIP Utilities	No JRE	<ol style="list-style-type: none"> 1. No middleware is installed (already present) 2. Java version 1.6.0_27 installed 3. cacerts, trusted.certs, and java.security files are installed 4. local_policy.jar installed
Windows XP	DataKey CIP Utilities	Version prior to 1.6.0_27	<ol style="list-style-type: none"> 1. No middleware is installed (already present) 2. Java version 1.6.0_27 installed 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows XP	DataKey CIP Utilities	1.6.0_27	<ol style="list-style-type: none"> 1. No middleware is installed (already present) 2. No Java software is installed (already present) 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows XP	SafeNet Authentication Client	No JRE	<ol style="list-style-type: none"> 1. No middleware is installed (already present) 2. Java version 1.6.0_27 installed 3. cacerts, trusted.certs, and java.security files are installed 4. local_policy.jar installed
Windows XP	SafeNet Authentication Client	Version prior to 1.6.0_27	<ol style="list-style-type: none"> 1. No middleware is installed (already present) 2. Java version 1.6.0_27 installed 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows XP	SafeNet Authentication Client	1.6.0_27	<ol style="list-style-type: none"> 1. No middleware is installed (already present) 2. No Java software is installed (already present) 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows 7 32-bit	No Middleware	No JRE	<ol style="list-style-type: none"> 1. 32-bit SafeNet Authentication Client and iKey drivers installed 2. Java version 1.6.0_27 installed

			<ol style="list-style-type: none"> 3. cacerts, trusted.certs, and java.security files are installed 4. local_policy.jar installed
Windows 7 32-bit	No Middleware	Version prior to 1.6.0_27	<ol style="list-style-type: none"> 1. 32-bit SafeNet Authentication Client and iKey drivers installed 2. Java version 1.6.0_27 installed 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows 7 32-bit	No Middleware	1.6.0_27	<ol style="list-style-type: none"> 1. 32-bit SafeNet Authentication Client and iKey drivers installed 2. No Java software installed (already present) 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows 7 32-bit	SafeNet Authentication Client	No JRE	<ol style="list-style-type: none"> 1. No middleware installed (already present) 2. Java version 1.6.0_27 installed 3. cacerts, trusted.certs, and java.security files are installed 4. local_policy.jar installed
Windows 7 32-bit	SafeNet Authentication Client	Version prior to 1.6.0_27	<ol style="list-style-type: none"> 1. No middleware installed (already present) 2. Java version 1.6.0_27 installed 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows 7 32-bit	SafeNet Authentication Client	1.6.0_27	<ol style="list-style-type: none"> 1. No middleware is installed (already present) 2. No Java software is installed (already present) 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows 7 64-bit	No Middleware	No JRE	<ol style="list-style-type: none"> 1. 64-bit SafeNet Authentication Client and iKey drivers installed 2. 32 bit Java version 1.6.0_27 installed in 32-bit version of IE 7 or 8 3. cacerts, trusted.certs, and java.security files are installed 4. local_policy.jar installed
Windows 7 64-bit	No Middleware	Version prior to 1.6.0_27	<ol style="list-style-type: none"> 1. 64-bit SafeNet Authentication Client and iKey drivers installed 2. 32-bit Java version 1.6.0_27 installed in 32-bit version of IE 7 or 8 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows 7 64-bit	No Middleware	1.6.0_27	<ol style="list-style-type: none"> 1. 64-bit SafeNet Authentication Client and iKey drivers installed 2. No Java software is installed (already present)

			<ol style="list-style-type: none"> 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows 7 64-bit	SafeNet Authentication Client	No JRE	<ol style="list-style-type: none"> 1. No middleware is installed (already present) 2. 32-bit Java version 1.6.0_27 installed in 32-bit version of IE 7 or 8 3. cacerts, trusted.certs, and java.security files are installed 4. local_policy.jar installed
Windows 7 64-bit	SafeNet Authentication Client	Version prior to 1.6.0_27	<ol style="list-style-type: none"> 1. No middleware is installed (already present) 2. 32-bit Java version 1.6.0_27 installed in 32-bit version of IE 7 or 8 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up
Windows 7 64-bit	SafeNet Authentication Client	1.6.0_27	<ol style="list-style-type: none"> 1. No middleware is installed (already present) 2. No Java software is installed (already present) 3. cacerts, trusted.certs, and java.security files are updated 4. local_policy.jar is backed up

3.2. ITRA-SC – Java App (Stand-alone)

The ITRA-SC client is designed to be portable across different Windows operating systems, bit versions, without altering the enablement of the agency's version of the Java plug-in.

3.3. Known Issues with Windows 7

The following known issues exist in Windows 7:

Known Issue	ITRA-Web components are not all 64-bit compatible. Java Plug-in must be 32-bits and run in a 32-bit IE browser.
Components affected:	JRE 1.6.0_27 plug-in – 32-bit, the Entrust Java Toolkit FMS uses in building its java components is not 64-bit compatible.
Severity:	None.
Resolution:	The users should install ITRA-SC (self-contained), which is immune to browser/Java plugin incompatibilities.

Known Issue	IE8 reopens ITRA
--------------------	------------------

Components affected:	ITRA (Web browser version) when using IE8+
Severity:	Low
Resolution:	<p>IE8 will automatically reopen the browser window after a credential has been modified. None of the previously entered information is retained. The user will have to manually close the browser window.</p> <p><u>Attention:</u> The best solution is to install ITRA-SC (self-contained), which is immune to browser/Java plugin incompatibilities.</p>

Known Issue	ActiveX control needs to be accepted
Components affected:	ITRA (Web browser version)
Severity:	None
Resolution:	<p>If an ActiveX dialog saying “This website wants to run the following add-on: ‘Java™ SE Runtime Environment 6 Update 22’ from ‘Sun Microsystems, Inc.’ If you trust the website and the add-on and want to allow it to run click here.” appears, the user will need to click it, and click “Run Add-on.”</p> <p><u>Attention:</u> The best solution is to install ITRA-SC (self-contained), which is immune to browser/Java plugin incompatibilities.</p>

4. Errors during Log in / Change PIN

The errors encountered by the user during log in / change PIN are split into the following categories:

- Workstation configuration
- PKI Connectivity
- User login process
- Credential Status Notification and Update (optional feature) – see Section “Credential Status Notification and Update Errors”

If the user is unsure of which type of error he/she has received, he/she may search the index for the words of the error or the reason in order to expedite the search.

4.1. Workstation Configuration Errors

FATAL ERROR
ERROR: The application cannot be started.
REASON: Java high-cryptography security policy jar files are missing
SUGGESTION: Close your browser and install correct high-cryptography security policy jar files. Call helpdesk if you need help.
Description: The user has attempted to access the ITRA Web Application when his/her Java installation was not properly configured for ITRA. To install the necessary files, the user can refer to the ITRA Desktop Installation Document. This document describes the procedure for configuring Java. The user may call the Help Desk if there are any questions.
Attention: The best solution is to install ITRA-SC (self-contained), which is immune to browser/Java plugin incompatibilities.

FATAL ERROR
ERROR: The application cannot be started.
REASON: Java plugin has insufficient security level.
SUGGESTION: Close your browser and install correct java policy file. Call helpdesk if you need help.

Description: The user has attempted to access the ITRA Application when his/her Java installation was not properly configured for ITRA. To install the necessary files, the user can refer to the ITRA Desktop Installation Document. This document describes the procedure for configuring Java. The user may call the Help Desk if there are any questions.

Attention: The best solution is to install ITRA-SC (self-contained), which is immune to browser/Java plugin incompatibilities.

4.2. PKI Connectivity Errors

FATAL ERROR

ERROR: Cannot log into PKI

REASON: LDAP is not available.

SUGGESTION: Save the error details to the file and send the file to help desk. Close the ITRA and call the help desk.

Description: The user tried to access the ITRA application and the action failed because LDAP was not available. Please click the “Show Details” button and then save the error details to a file using the “Save to File” button. The location of the file will be shown in the error message. Please reference this file when calling the Help Desk for more information.

FATAL ERROR

ERROR: Cannot log into PKI.

REASON: PKI environmental issues - CRLs either missing or invalid.

SUGGESTION: Save the error details to the file and send the file to help desk. Close the ITRA and call the help desk.

Description: The user tried to access the ITRA application and the action failed because of a problem in the system environment. Please click the “Show Details” button and then save the error details to a file using the “Save to File” button. The location of the file will be shown in the error message. Please reference this file when calling the Help Desk for more information.

4.3. User Login Process Errors

FATAL ERROR
ERROR: Cannot Log into PKI.
REASON: Error reading or communicating with token: Error Code#-1 No active token slots found
Description: The user attempted to log in to the ITRA Application when there was no token connected to the workstation. In order to access the ITRA Application, the user must first connect a token, then access the ITRA to log in again.

FATAL ERROR
ERROR: Login cancelled by user.
Description: The user attempted to log in to the ITRA Application. During the log in process, the user clicked the “Cancel” button. This cancels the log in process and exits the ITRA Application. To log in again the user must re-start the ITRA.
NOTE: This does not include pressing the “Cancel” button on the “PKI Token Selection Dialog” screen; this action will produce a different error.

FATAL ERROR
ERROR: Cannot Log into PKI.
REASON: Bad PIN. Maximum login attempts exceeded.
Description: The user attempted to log in to the ITRA Application and entered an incorrect PIN three times. The user may attempt to log in to the ITRA Application again by accessing the ITRA and entering the PIN again. If the error is received again, the user may call the Help Desk.

FATAL ERROR (TRA ASSISTED USERS ONLY)
ERROR: Authorization denied.
REASON: User is not a TRA.
SUGGESTION: Valid TRA should re-login to the application.

Description: The current user's token is not a TRA and therefore is not permitted to log into the TRA Assisted system. In order to access TRA-Assisted ITRA, a valid TRA token must be used.

Error details include error code 11005.

FATAL ERROR (TRA ASSISTED USERS ONLY)

ERROR: Authorization denied.

REASON: Found no valid OIDs. The authorization level is insufficient for this application.

Description: The current user's token is assigned a TRA role, but the user's credential includes a Level 1 OID, and therefore is not permitted to log into the TRA Assisted system as a TRA. In order to access TRA-Assisted ITRA as a valid TRA, the TRA credentials must be recovered with only Level 3 OID. A DACD ticket must be issued.

Error details include error code 11006.

FATAL ERROR

ERROR: Cannot Log into PKI.

REASON: Problem with Smartcard Credential Certificate: The CA certificate is not valid: Could not find certificates due to a Directory communication error.

Description: The current user's certificate on his/her token has expired or the certificate was created from an incompatible PKI. The user must contact his/her Help Desk for more information.

FATAL ERROR

ERROR: Cannot Log into PKI.

REASON: Your certificate has expired.

Description: The current user's certificate on his/her token has expired. The user must contact his/her Help Desk for more information.

FATAL ERROR
ERROR: Cannot Log into PKI.
REASON: User possibly deactivated by administrator. Contact Help Desk. (USER_VALIDITY).
Description: This user has been revoked or deactivated in the PKI. This issue should be investigated with DACD.

FATAL ERROR
ERROR: Cannot Log into PKI.
REASON: Smartcard connection error.
Description: At the “PKI Token Selection Dialog” screen, the user selected “Cancel” instead of selecting a token. To access ITRA, the user must access ITRA again and select the token he/she wishes to use to log into the application.

5. Credential Status Notification and Update Errors

Included in this section are notification messages and errors that are encountered while using the ITRA Self-Service Credential Update process or during regular login process (the key management option must be turned on). These errors are separated into the following categories:

- Credential Status Notification issues
- Credential Update errors

If the user is unsure of which type of error he/she has received, he/she may search the index for the words of the error or the reason in order to expedite the search.

5.1. Credential Status Notification issues

USER CREDENTIAL STATUS
Notification Dialog with LOGIN NOTIFICATION: Token contains credentials that have been managed outside of ITRA. The credential status information might be inaccurate. Options (buttons) vary
1. Option Update (if present and enabled): The dialog will close and the user will perform all pending changes, such as PIN change and/or credential updates that are listed in Notification dialog.
2. Option Skip Update or OK (if present and enabled): The dialog will close and the user will skip all pending updates and attempt to continue.
3. Option Save to File: saves all error-related information to the file on user's computer. The user remains on the screen.
4. Option Exit (if present): The dialog will close and the user will receive a Fatal Error dialog with "User cancelled operation" message. The ITRA will exit.
Description: The user's token was written and/or managed using an application other than ITRA, such as Entrust Service Provider (ESP), True Pass, or other third-party tools. Some versions of those tools might create a V2 credential, for which credential status cannot be obtained by ITRA, and therefore, cannot be accurately displayed to the user.

USER CREDENTIAL STATUS

No Notification Dialog or No expected DN Change pending notification.

Options (buttons) vary

Description: DN changes are not pending, or DACD changed the DN but did not keep the old entry in the directory (LDAP). ITRA requires the old DN entry in order to identify the pending DN change.

A DACD ticket must be issued: when changing DN the old entry must be kept in directory.

5.2. Credential Update errors**NON FATAL ERROR**

Error Dialog with exception details (not fatal): Credential management cannot be performed: OIDs mismatch.

Options (buttons)

1. Option OK: The error dialog will close and the user will continue to access the application.

2. Option Save to File: saves all error-related information to the file on user's computer.

Description: The credential update ticket was retrieved, but the authorization to perform the update is denied for one of the following reasons:

A) The Verification and Encryption OIDs in the credential update ticket are different.

B) The level of Verification and Encryption OIDs in the credential update ticket is higher than in the current user certificate.

DACD ticket must be issued: credential update ticket must not have mismatched OIDs and must not elevate OIDs level for the current user certificate.

Error details include error code 11016.

NON FATAL ERROR

Error Dialog with exception details (not fatal): Key management is not possible at this time: The credentials appear to be in 24-hour waiting period.

Options (buttons)

1. Option OK: The error dialog will close and the user will continue to access the application.

2. Option Save to File: saves all error-related information to the file on user's computer.

Description: The credential update ticket was retrieved, but the user token contains an Options object with CertificatePublicationPending timestamp, which was written by some tool during the last credential management action: create/recover/credential update.

The only option the user has is to wait for the 24-hour period to expire.

NON FATAL ERROR

Error Dialog with exception details (not fatal): The certificate keys are not set for automatic update.

Options (buttons)

1. Option OK: The error dialog will close and the user will continue to access the application.

2. Option Save to File: saves all error-related information to the file on user's computer.

Description: The credential update ticket was retrieved, but the key expiry policy is set by specific date, instead of lifetime percentage. This key expiry setting prevents keys from being updated automatically.

Usually, this key expiry policy is set with the purpose to prevent users from updating their credentials via self-service, so no action is required. If this key expiry policy is set by mistake, then the DACD ticket must be issued: key update policy must be set using lifetime percentages and the user must be recovered.

NON FATAL ERROR

Error Dialog with exception details (not fatal): An error occurred during certificate management.

Options (buttons)

1. Option OK: The error dialog will close and the user will continue to access the application.

2. Option Save to File: saves all error-related information to the file on user's computer.

Description: The credential update ticket was retrieved, but the credential management could not be completed. The reason of failure must be investigated. The error message and/or error details might include an error code, so saving those details to a file and passing the file to a helpdesk will help in the failure investigation.

WARNING

Warning Message: Token contains credentials that have been managed outside of ITRA. ITRA does not support credential management for such tokens at this time.

Options (buttons)

1. Option OK: The error dialog will close and the user will continue to access the application.

Description: This token contains V2 credentials and these are not supported by the current release of ITRA. These tokens must be managed outside of ITRA. If needed, this credential could be recovered by ITRA.

NON FATAL ERROR

Error Dialog with exception details (not fatal): Entrust PKIX-CMP Error code (-1648).

Options (buttons)

1. Option OK: The error dialog will close and the user will continue to access the application.

2. Option Save to File: saves all error-related information to the file on user's computer.

Description: The user's security token contains old signing certificate. Possible scenarios:

A. User credentials were recovered to the new security token, but later old token was used to update credentials.

B. User attempted to perform automated credential update, but communication to the CA was timed-out and user's new signing certificate was immediately revoked.

In both scenarios, user must completely recover the credentials.

NON FATAL ERROR

Error Dialog with exception details (not fatal): Entrust PKIX-CMP Error code (-1647).

Options (buttons)

1. Option OK: The error dialog will close and the user will continue to access the application.

2. Option Save to File: saves all error-related information to the file on user's computer.

Description: The user's security token contains old encryption certificate. Possible scenario: User credentials were recovered to the new security token, but later old token was used to update credentials.

In such case, user must completely recover the credentials.

6. ITRA - Application Errors

Included in this section are errors that are encountered while using the ITRA application. These errors are separated into the following categories:

- Lost connection to CA
- Wrong data for processing
- Creation Limit (TRA Assisted only)

If the user is unsure of which type of error he/she has received, he/she may search the index for the words of the error or the reason in order to expedite the search.

6.1. Lost Connection to CA

FATAL ERROR
ERROR: Create credential failed.
REASON: CA was not available.
SUGGESTION: Save error details to file and call helpdesk.
Description: The user (TRA or Self-Service Level 1 user) tried to create a certificate and the action failed because the CA was not available. Please click the “Show Details” button and then save the error details to a file using the “Save to File” button. The location of the file will be shown in the error message. Please reference this file when calling the Help Desk for more information.

NON FATAL ERROR (SELF-SERVICE USERS ONLY)
Error Dialog with exception details (not fatal): Ticket request contains bad reference ID. Options (buttons)
1. Option OK: The error dialog will close and the user will be returned to the empty entry screen for self-service Level 1 users.
2. Option Save to File: saves all error-related information to the file on user’s computer.
Description: The self-service Level 1 user entered all information on the main self-service screen and continued, but the authorization for the certificate could not be retrieved because the CA was not available. Error details include error code 11011.

6.2. Wrong Data for Processing

6.2.1. TRA Assisted Mode

NON FATAL ERROR
<p>ITRA: Key Recovery Error</p> <p>The key should be created, not recovered.</p> <p>Options (buttons)</p>
<p>1. Option Create: ITRA will perform one-time create and display created credential. After that, the only choice will be to exit the ITRA.</p>
<p>2. Option Exit (or closing the dialog): exit the ITRA and Close the ITRA.</p>
<p>Description: The user has attempted to recover a certificate with data that is not valid for recovery. The user may click the “Create” button to try to create the certificate with the entered data. Only one create will be permitted (with that data), then the ITRA application will exit. If the user does not wish to try to create the certificate, he/she may click the “Exit” button to exit ITRA.</p>

NON FATAL ERROR
<p>ITRA: Create Error</p> <p>The key should be recovered, not created.</p> <p>Options (buttons):</p>
<p>1. Option Recover: ITRA will perform one-time key recovery and display created credential. After that, the multiple creates will continue.</p>
<p>2. Option Skip: application checks the session (time and number of creates < 5, including the current step) and takes user to the “Create new credential” screen.</p>
<p>3. Option Exit (or closing the dialog): exit the ITRA and Close the ITRA.</p>
<p>Description: The user has attempted to create a certificate with data that is not valid for creation. The user may click the “Recover” button to attempt to recover the certificate with the entered data. This will only recover one certificate, and then continue with the create certificate process. The user may click the “Skip” button to discard the entered data and continue to create certificates with other data. The user may click the “Exit” button to discard the entered data and exit the ITRA Application.</p>

NON FATAL ERROR

Error Dialog with exception details (not fatal):

The reference number is either bad, expired, or already used.

Option OK (or closing the dialog): the application checks the session (time) and takes user to the “Enter End User codes” (manually, no file decryption) screen.

Description: The user has attempted to create or recover a certificate with a reference number that is invalid. If the user was trying to create a certificate, he/she may click the “OK” button to be taken to the “Enter End User codes” create screen; if the user was trying to recover a certificate, clicking the “OK” button will take him/her to the “Enter End User Codes” (manual entry with no file decryption) recovery screen.

NON FATAL ERROR

Error Dialog with exception details (not fatal):

The authorization code does not match the reference number.

Option OK (or closing the dialog): the application checks the session (time) and takes user to the “Enter End User codes” (manually, no file decryption) screen.

Description: The user has attempted to create or recover a certificate with a reference number that is valid, but the authorization code does not match the reference number. If the user was trying to create a certificate, he/she may click the “OK” button to be taken to the “Enter End User codes” create screen; if the user was trying to recover a certificate, clicking the “OK” button will take him/her to the “Enter End User Codes” (manual entry with no file decryption) recovery screen.

NON FATAL ERROR

Error Dialog with exception details (not fatal):

Authorization expired. The codes must be re-issued.

Option OK (or closing the dialog): the application checks the session (time) and takes user to the “Enter End User codes” (manually, no file decryption) screen.

Description: The user has attempted to create or recover a certificate with a reference number and authorization code that have expired. If the user was trying to create a certificate, he/she may click the “OK” button to be taken to the “Enter End User codes” create screen; if the user was trying to recover a certificate, clicking the “OK” button will take him/her to the “Enter End User Codes” (manual entry with no file decryption) recovery screen.

FATAL ERROR

ERROR: Create credential failed. PKIX-CMP Error code -1685.

REASON: Credential has been upgraded to V2 and cannot be managed by ITRA.

SUGGESTION: Save error details to file and call helpdesk.

Description: ITRA creates credentials in the traditional Entrust “V1” format, which assumes a single verification certificate and a single encryption certificate. Entrust now has a new credential “V2” format, and an associated management mode, that is supported by only certain of their products. At this time, ITRA will not create or manage credentials that have been migrated to “V2” format. At this time, users with V2 credentials must use the credential management application that created or converted them to V2. Please save the error details to a file using the “Save to File” button. The location of the file will be shown in the error message. Please reference this file when calling the Help Desk for more information.

Error details include error code 1685.

6.2.2. Self-Service Create/Recover (Level 1)

NON FATAL ERROR
Error Dialog with exception details (not fatal): Ticket request contains bad reference ID. Options (buttons)
1. Option OK: The error dialog will close and the user will be returned to the empty entry screen for self-service Level 1 users.
2. Option Save to File: saves all error-related information to the file on user's computer.
<p>Description: The self-service Level 1 user entered invalid reference number.</p> <p>A) In the case of simple typo, the user can re-type the reference number.</p> <p>B) If the user typed reference number exactly as it was delivered to him or her, then the problem might be that the user's credentials were added to a wrong group by issuing authority. DACD ticket must be issued: only Level 1 group users may use Self-Service mode of ITRA.</p> <p>Error details include error code 11011.</p>

NON FATAL ERROR
Error Dialog with exception details (not fatal): Found no valid OIDs. The authorization level is insufficient for this application. Options (buttons)
1. Option OK: The error dialog will close and the user will be returned to the empty entry screen for self-service Level 1 users.
2. Option Save to File: saves all error-related information to the file on user's computer.
<p>Description: The reference number refers to the credentials issued for correct Level 1 group, but with no valid OIDs.</p> <p>A) In the case of simple typo, the user can re-type the reference number.</p> <p>B) If the user typed reference number exactly as it was delivered to him or her, then the problem might be that the user's credentials were added to a correct group by issuing authority, but without Level 1 OIDs. DACD ticket must be issued.</p> <p>Error details include error code 11006.</p>

NON FATAL ERROR
Error Dialog with exception details (not fatal): Failed to validate certificate. Options (buttons)
1. Option OK: The error dialog will close and the user will be returned to the empty entry screen for self-service Level 1 users.
2. Option Save to File: saves all error-related information to the file on user's computer.
Description: The reference number refers to the expired credentials. A) In the case of simple typo, the user can re-type the reference number. B) If the user typed reference number exactly as it was delivered to him or her, then the activation codes must be re-issued by issuing authority. DACD ticket must be issued. Error details include error code 11007.

NON FATAL ERROR
Error Dialog with exception details (not fatal): Found invalid OIDs. The authorization level is insufficient for this application. Options (buttons)
1. Option OK: The error dialog will close and the user will be returned to the empty entry screen for self-service Level 1 users.
2. Option Save to File: saves all error-related information to the file on user's computer.
Description: The reference number refers to the credentials issued for correct Level 1 group, but with OIDs appropriate for higher level assurance credentials. A) In the case of simple typo, the user can re-type the reference number. B) If the user typed reference number exactly as it was delivered to him or her, then the problem might be that the user's credentials were added to a correct group by issuing authority, but contain Level 3 OIDs. DACD ticket must be issued. Error details include error code 11013.

FATAL ERROR
ERROR: Create credential failed.
REASON: The authorization code does not match the reference number.
SUGGESTION: Save error details to file and call helpdesk.

Description: The Self-Service Level 1 user tried to create or recover a certificate with a reference number that is valid, but the authorization code does not match the reference number. Please save the error details to a file using the “Save to File” button. The location of the file will be shown in the error message. Please reference this file when calling the Help Desk for more information.

FATAL ERROR

ERROR: Create credential failed. PKIX-CMP Error code -1685.

REASON: Credential has been upgraded to V2 and cannot be managed by ITRA.

SUGGESTION: Save error details to file and call helpdesk.

Description: ITRA creates credentials in the traditional Entrust “V1” format, which assumes a single verification certificate and a single encryption certificate. Entrust now has a new credential “V2” format, and an associated management mode, that is supported by only certain of their products. At this time, ITRA will not create or manage credentials that have been migrated to “V2” format. At this time, users with V2 credentials must use the credential management application that created or converted them to V2. Please save the error details to a file using the “Save to File” button. The location of the file will be shown in the error message. Please reference this file when calling the Help Desk for more information.

Error details include error code 1685.

6.3. Creation Limit Error (TRA Assisted)

FATAL ERROR

ERROR: Exit Session

REASON: You have reached your creation limit for the session.

Description: The TRA user tried to create a certificate after already creating five certificates. The ITRA Application must shut down. In order to create or recover more certificates, the TRA user must log in again.

7. General Troubleshooting

7.1. SPS Tools and Notes

The SPS and FMS PKI Setup installations are very similar. Many of the tools and technical notes for SPS are also valid for the FMS PKI Setup.

7.2. Administrative Rights During Installation

The ITRA PKI Setup installation requires that the installer have full administrative rights to the local workstation. Experience has shown that performing an installation using an account that has less than full rights to the workstation can sometimes lead to a non-functional installation.

7.3. Directory Rights

If the directory rights are not set properly in the ITRA directory structure, the ITRA can fail with a number of error indications, usually while downloading its signed code.

The TRA user must have full rights to this directory structure. The default installation attempts to give such access to all users. If this does not work, or is inappropriate for the environment, the rights can be set manually. This is performed by right clicking on the ITRA directory (chosen during installation, default is C:\ITRA-SC), selecting “properties”, going into the “Security” tab and giving full rights to the TRA users.

7.4. Web Site Does Not Appear

This usually means that the workstation does not have Internet access. If the user must use a proxy to access the Internet, ensure that the proxy is configured in the.

7.5. Web Site Validation Warning

If a warning message appears when accessing the web site that indicates the site might not be trusted, you need to install the ITRA PKI CA certificate in your browser.

The following certificate files are provided on the ITRA installation CD:

```
\javacfg\prep\fmsroot-prep.crt  
\javacfg\prod\fmsroot-prod.crt
```

By default, the installer will add these to the IE certificate store during installation. To add them manually, double-click on the files, select “Install” and follow the prompts.

For browsers other than IE, follow the instructions for adding certificates appropriate to that browser.

Attention: The best solution is to install ITRA-SC (self-contained), which is immune to browser/Java plugin incompatibilities.

7.6. Applet Does Not Start

Ensure the Java Plug-in is installed and that Java is enabled in the browser.

Attention: The best solution is to install ITRA-SC (self-contained), which is immune to browser/Java plugin incompatibilities.

7.7. Java Code Signature Warning

If you receive a warning similar to the one below:



It is most likely that the ITRA Java policy and keystore files are not being found by the Java Plug-in. Refer to the FMS PKI Setup Desktop Installation document covering Java policy and keystore files to ensure that Java is properly configured.

Attention: The best solution is to install ITRA-SC (self-contained), which is immune to browser/Java plugin incompatibilities.

7.8. Token Not Visible or Token Service Not Started

7.8.1. If using Datakey CIP Utilities

The PKI token might not be visible in the Datakey CIP utilities, or you may get a “Token Service Not Started” error. This usually indicates a Windows (mis)configuration problem with Microsoft’s “Smart Card” server that prevents the token driver from loading.

Some environments put security templates on their workstations that turn off the Smart Card Service. As a result, this service shows as “disabled” in the Services control panel. If this is the case, change the state to “automatic” and start the service. Additionally, you will need to ensure that the “Datakey Token Service” is also set to “automatic” and started.

On some occasions, the Smart Card service cannot start because it does not have rights to an obscure registry key. The account “LOCAL SERVICE” must have read rights to all of the registry keys at and below the following entry:

```
HKLM\SOFTWARE\Microsoft\Cryptography\Calais
```

7.8.2. If using Safenet Authentication Client

The PKI token might not be visible in the Safenet Authentication Client, or you may get a “Token Service Not Started” error. This usually indicates a Windows (mis)configuration problem with Microsoft’s “Smart Card” server that prevents the token driver from loading.

Some environments put security templates on their workstations that turn off the Smart Card Service. As a result, this service shows as “disabled” in the Services control panel. If this is the case, change the state to “automatic” and start the service. Additionally, you will need to ensure that the “SACSrv” is also set to “automatic” and started.

On some occasions, the Smart Card service cannot start because it does not have rights to an obscure registry key. The account “LOCAL SERVICE” must have read rights to all of the registry keys at and below the following entry:

```
HKLM\SOFTWARE\Microsoft\Cryptography\Calais
```

It may also be helpful to install the BSec Utilities for SAC 8.0 for troubleshooting purposes. The installer for this is located within the “install” folder on the ITRA-SC Installer CD.

7.9. SSL Connection Failure

This usually occurs because the workstation uses a web-proxy to access the Internet, but the ITRA has not been configured to use one. Follow the instructions in the ITRA-SC Installation document for configuring/repairing the ITRA-SC client to use a web-proxy.

7.10. Cannot (Fully) Uninstall or Re-Install Datakey CIP

On occasion it is desirable to re-install Datakey CIP in order to try to resolve an installation problem. Unfortunately, there are occasions when CIP will not uninstall fully, after having attempted to remove it in the “Add/Remove Programs” applet in the control panel.

The Fiscal IT Service Desk could provide a Datakey CIP Cleanup tool that can help uninstall Datakey CIP.

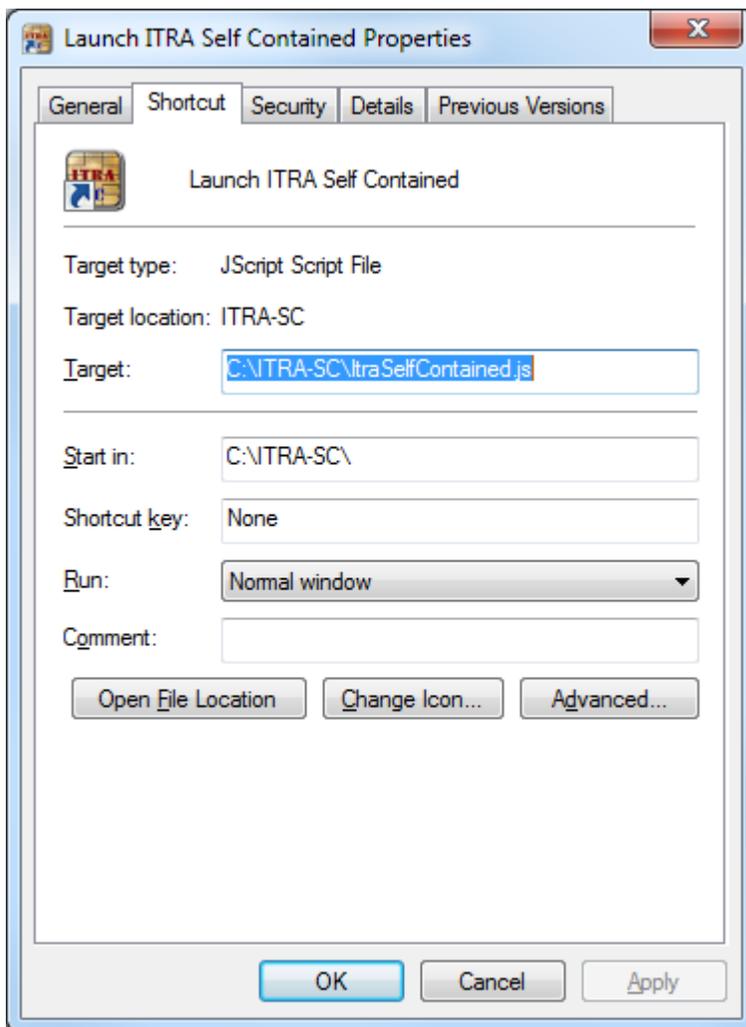
7.11. Turn On Debugging for ITRA Web

Turn on debugging for ITRA Web by setting the system property “-Dloader.debug=true” option in the Java Plug-in control panel applet. Setting this to “true” or “on” will cause the ITRA loader to output debugging information to the Java console and trace logs. The Java console can be made visible in the Java Plug-in control panel. The trace log is located in the user’s home directory:

```
C:\Documents and Settings\username\Application  
Data\Sun\Java\Deployment\log\plugin###.log
```

7.12. Turn On Debugging for ITRA Self-Contained

Turn on debugging for ITRA-SC (Self-Contained) by modifying the “Launch ITRA Self Contained” shortcut Properties. The Properties could be opened either from Desktop shortcut, or from Windows menu Start>All Programs>ITRA>ITRA – Self Contained (ITRA-SC). Right-click on the “Launch ITRA Self Contained” shortcut and select Properties.



In the field “Target:” append the following text:

```
-d "-Dloader.debug=true"
```

Warning: the text above must be appended, so that the original text “C:[...]ItraSelfContained.js” is preserved and should look similar to the following:

```
C:\ITRA-SC\ItraSelfContained.js -d "-Dloader.debug=true"
```

This setting will make an empty Java window to appear, but the output of the debug log will be stored in the ITRA-SC logs directory:

```
C:\ITRA-SC\logs\jre_log.out
```

Index

Administrative Rights During Installation	33	Found no valid OIDs. The authorization level is insufficient for this application.....	30
Applet Does Not Start	33	Ticket request contains bad reference ID.	26, 29
Cannot (Fully) Uninstall or Re-Install Datakey CIP	35	The application cannot be started.....	16
Directory Rights	33	TRA ASSISTED	
ERROR		Authorization denied.	18, 19
Cannot log into PKI	17	Authorization expired. The codes must be re-issued.	28
Cannot log into PKI.	17	Create credential failed.	29
Cannot Log into PKI.	18	Create Error	27
Cannot Log into PKI.	19	Exit Session	32
Cannot Log into PKI.	19	Key Recovery Error	27
Cannot Log into PKI.	20	The authorization code does not match the reference number.	28
Cannot Log into PKI.	20	The key should be created, not recovered.	27
Create credential failed.	26	The key should be recovered, not created.	27
CREDENTIAL UPDATE		The reference number is either bad, expired, or already used.	28
Could not perform certificate management.	24, 25	ERROR CODE	
OIDs mismatch.....	22	11005	19
The certificate keys are not set for automatic update.	23	11006.....	19, 30
The credentials appear to be in 24-hour waiting period.....	23	11007.....	30
Login cancelled by user.	18	11011.....	26, 29
SELF SERVICE		11013.....	31
Create credential failed.....	31	11016.....	22
Failed to validate certificate.	30	1647	25
Found invalid OIDs. The authorization level is insufficient for this application.	31	1648	25

1685.....	29, 32	Found no valid OIDs. The authorization level is insufficient for this application.....	19
Java Code Signature Warning.....	34	User is not a TRA.	18
REASON		You have reached your creation limit for the session.....	32
Bad PIN. Maximum login attempts exceeded.	18	REASON: User possibly deactivated by administrator. Contact Help Desk. (USER_VALIDITY).	20
CA was not available.....	26	REASON: Your certificate has expired.	19
Error reading or communicating with token: Error Code#-1 No active token slots found.....	18	SPS Tools and Notes	33
Java high-cryptography security policy jar files are missing	16	SSL Connection Failure.....	35
Java plugin has insufficient security level.	16	STATUS	
LDAP is not available.	17	CREDENTIAL	
PKI environmental issues - CRLs either missing or invalid.....	17	No expected DN Change Notification.....	22
Problem with Smartcard Credential Certificate: The CA certificate is not valid: Could not find certificates due to a Directory communication error.	19	Token contains credentials that have been managed outside of ITRA.	21
SELF SERVICE		Token Not Visible or Token Service Not Started.....	34
Credential has been upgraded to V2 and cannot be managed by ITRA.	31	Turn On Debugging	35
The authorization code does not match the reference number.....	31	WARNING	
Smartcard connection error.	20	V2 Credentials not supported.....	24
TRA ASSISTED		Web Site Does Not Appear.....	33
Credential has been upgraded to V2 and cannot be managed by ITRA.	29	Web Site Validation Warning	33
