

# WHAT'S NEW IN ITRA

*February 11, 2016*

This latest ITRA release has enabled installation on Microsoft Windows 8.1 and 10.



*February 20, 2015*

This latest ITRA release introduces two new Safenet usb token authenticators to Fiscal Service Public Key enabled (PKE) applications. The Safenet iKey 4000 usb token, and the eToken 5100 now join the iKey 2032 as acceptable personal hardware crypto modules for the protection of Fiscal Service CA issued credentials.

Both the iKey 4000 (Cert #943) and the eToken 5100 (Cert #1883) are FIPS 140-2 Level 3 crypto module validated.

In order to use the new authenticators in addition to supporting the current iKey 2032, it is necessary to replace the current smartcard middleware Safenet Authentication Client (SAC) 8.0 SP 2 with a newer version of the middleware, SAC 8.2.<sup>1</sup> The only processing that has changed with the introduction of new generations of smart tokens is a TRA and end user no longer must use the same usb slot, when swapping TRA token for end user token during certificate generation. With this release it is possible to use a different usb slot than the TRA's (TRA is no longer required to pull his/her token) when the end user's token is inserted.

TRA functionality is only apparent to Level 3 certificate generation, for Level 1 certificate generation a TRA is not required and certificate generation has not changed.

This document is meant to introduce existing users of ITRA to some of the new features delivered in the ITRA Self-Contained (ITRA-SC) release. Note that this document is not intended to be an exhaustive list of changes, but is merely intended to be a short summary of noticeable changes to which ITRA users may want to be aware.

## 1 ITRA-SC START POINT



ITRA certificate generation software can no longer be accessed from a browser. The web based version of ITRA requiring the java plug-in has been terminated as of September 30, 2014. Therefore past ITRA links in browsers will only provide a limited access to ITRA resources.

The start points for ITRA-SC are found within the start menu and desktop icons or shortcuts. When ITRA-SC is launched a new application window will open with options for the Self Service and TRA-Assisted operations.

## 2 SUPPORTED OPERATING SYSTEMS

The ITRA-SC supports Windows 7, 8, and 10 (32 and 64 bit) operating systems. The installer will automatically detect the operating system during installation and will quit installation on a Windows XP machine.

## 3 JAVA 1.7 VERSION

---

<sup>1</sup> Note: iKey 2032s and iKey 4000s will continue to work with Safenet Authentication Client 8.0. It is only with the introduction of eToken 5100s that the new smartcard middleware SAC 8.2 is required.

In this release the ITRA Java version has not changed.

ITRA-SC comes with its own version of Java 1.7 and thus is not dependent on the Java being installed on the client operating system or the Java plug-in enabled for the client browser.

The change from browser based java applet to self-contained java application comes as java vulnerabilities are more prevalent within web browsers. US CERT (Computer Emergency Readiness Team) offered the following recommendation on February 20, 2013:

<http://www.us-cert.gov/ncas/alerts/TA13-051A>

### **Alert (TA13-051A) - Oracle Java Multiple Vulnerabilities**

*Both Java applets delivered via web browsers and stand-alone Java applications are affected, however web browsers using the Java plug-in are at particularly high risk.*

### ***Disable Java in web browsers***

*These and previous Java vulnerabilities have been widely targeted by attackers, and new Java vulnerabilities are likely to be discovered. To defend against this and future Java vulnerabilities, consider disabling Java in web browsers until adequate updates have been installed. As with any software, unnecessary features should be disabled or removed as appropriate for your environment.*

In response to the vulnerabilities expressed in the US CERT alert, ITRA is now offered as a stand-alone or self-contained java application. The Self-Contained version of ITRA will not conflict with the agency's implementation of its Java Plug-in. The agency can manage or disable their clients Java plug-in as it sees fit without compromising the functionality of ITRA-SC.

## 4 SMART CARD MIDDLEWARE

This release of ITRA-SC uses the Safenet Authentication Client 8.2 as the installed smartcard middleware. The Safenet Authentication Client 8.2 is necessary for the introduction of the eToken 5100 version of the Safenet usb crypto module. Therefore, the installation process will NOT allow a Windows administrator to keep past versions of the Safenet middleware on the user's desktop. In case when a particular earlier version of Safenet's Authentication Client is required by the end user's agency, the prior ITRA-SC installer could be used, with understanding that the agency will not be able to use eToken 5100 security tokens.

## 5 DOCUMENTATION

The "ITRA SC User Guide" document, dated Dec. 31, 2014, Section 5 has been modified to reflect changes in the TRA assisted create/recovery of credentials procedures.