



## RSA SecurID Ready Implementation Guide

Last Modified: August 6, 2013

### Partner Information

---

Product Information	
Partner Name	Secure Access Technologies
Web Site	<a href="http://www.secureaccesstechnologies.com">www.secureaccesstechnologies.com</a>
Product Name	SAT Token
Version & Platform	3.9.0 for iOS
Product Description	SAT Token enables a smart phone user to provide secure access to any application (iOS, cloud...) that requires password, RSA SecurID or PKI.

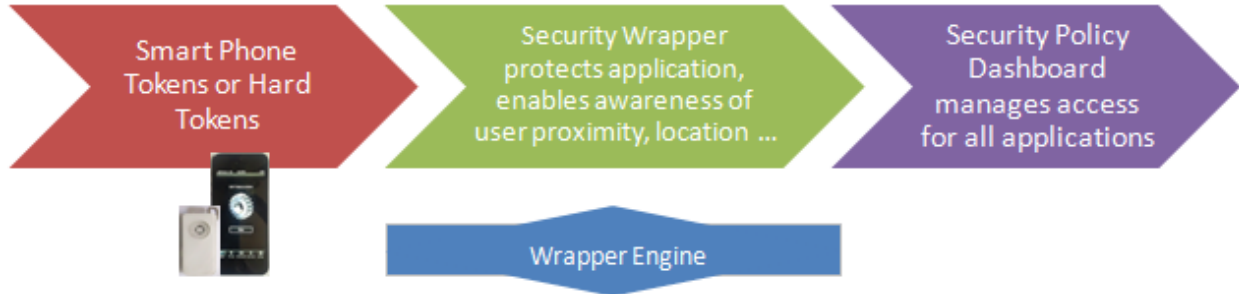


## Solution Summary

SAT Token collaborates with SAT Security Layer, SAT Policy Console and SAT Wrapper Engine to mobilize any application that requires password, RSA SecurID or PKI in minutes.

No more typing of passwords, OTP tokens or swiping of smart cards. SAT provides one-key sign on to any application as long as the user stays near the terminal.

When the user leaves proximity of the terminal, SAT automatically locks the application.



RSA Software Token Supported Features	
Windows Automation	No
SID800 Automation	No
OS X Automation	No
iOS Automation	Yes
Android Automation	No
File-based Provisioning	Yes
CT-KIP Provisioning	No
CTF Provisioning	No

## Partner Product Configuration

---

### ***Before You Begin***

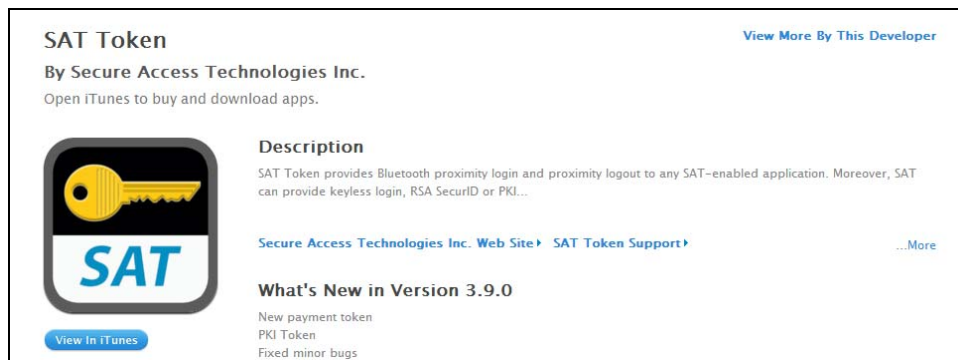
This section provides instructions for configuring SAT Token with RSA SecurID Authentication and RSA Software Token Automation. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

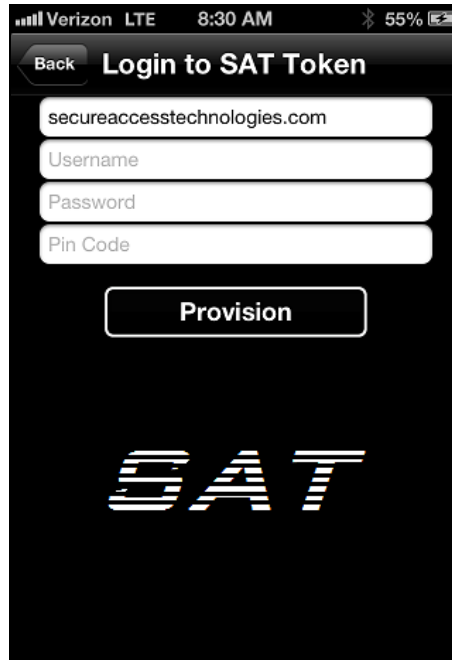
All SAT Token components must be installed and working prior to the integration. Perform the necessary steps before proceeding.

### **SAT Configuration**

1. Download the SAT Token from the Apple Store to iPhone.



2. Sign up for an account using SAT Token.



### Import the RSA SecurID Seed File

To configure the SAT Token for SecurID, please follow these steps:

1. Request an RSA SecurID Soft Token be sent via email (.sdtid format) from your RSA Authentication Manager administrator.
2. Receive the RSA SecurID Soft Token on the iOS device.
3. Import the seed file to SAT Token.

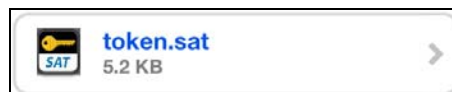
---

 **Note: To import a PKI Certificate and RSA SecurID token, use the following converter:**

<http://www.SecureAccessTechnologies.com/SATConsole/SATTokenConverter.php>

---

4. Using the clients email, select the **.sat** or **.sdtid** file in the email.



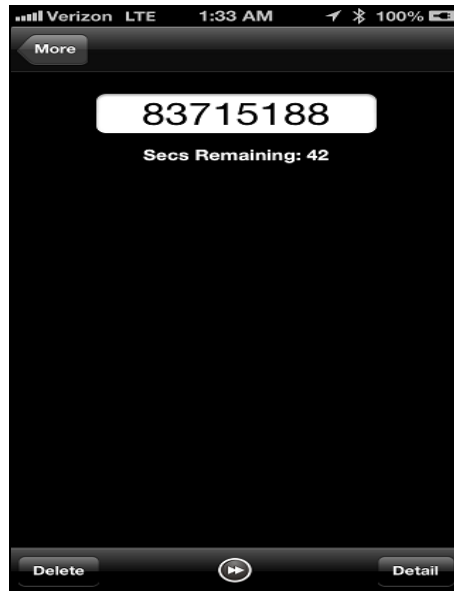
- When prompted to import the SAT Token (.sat file extension) or the RSA SecurID soft token (.stdid file extension) select **Open in SAT Token**.



- Select **OK** to acknowledge the import of the seed record file.



- Once the seed record is imported, the SAT token will display an RSA SecurID One Time Passcode (OTP) to indicate that is installed correctly.

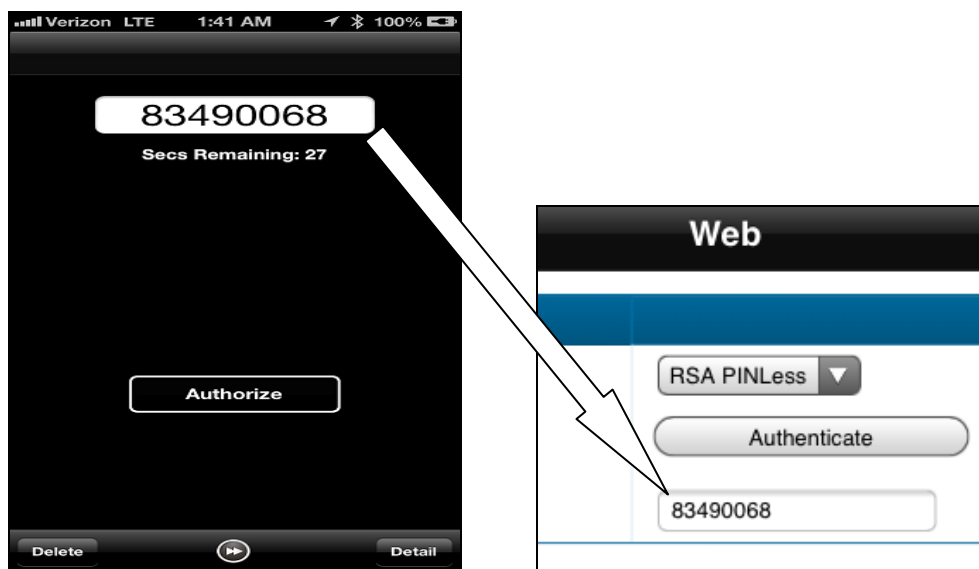


- When the SAT wrapped target application requests the RSA SecurID token, select **Authorize** and the RSA SecurID token is sent via Bluetooth to the iPad and used to authorize the transaction.

 **Note: SAT supports RSA SecurID PINLESS, Fob and PINPad Style Seed records.**

The RSA SecurID token will generally only show after a request is received from an authorized application that uses the SAT SDK.

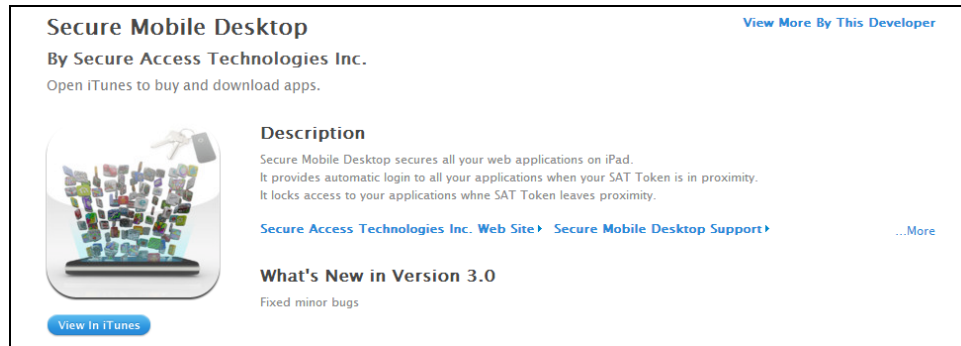
If you are using a PINPad or Fob style token you will be prompted for your PIN before SAT displays the tokencode.



## iPAD Web Application Support


To configure your iPad if your application has a web interface:

1. Download the Secure Mobile Desktop.



2. Contact SAT [support@secureaccesstechnologies.com] to obtain the SAT/SecurID API.
3. Add the SAT/SecurID API to your web application login page.

---

 **Note: For all iOS applications supporting SecurID OTP, contact Secure Access Technologies and submit a request for wrapping your target application.**

---


## Screens

---

Software Token PIN Prompt:

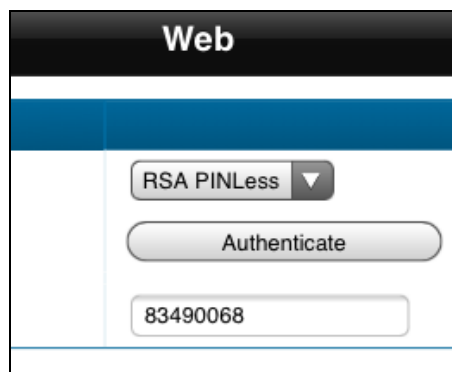


---

 **Note:** Modification of PIN's (System or User-Defined) must be managed from the iOS application or iOS web application interface on the paired iPad.

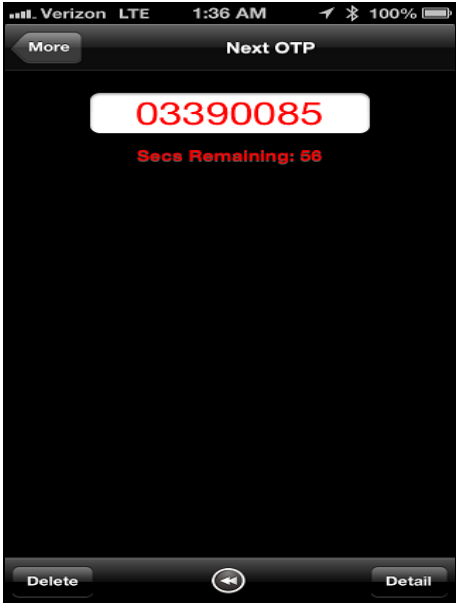
---

Wrapped iOS Login screen:

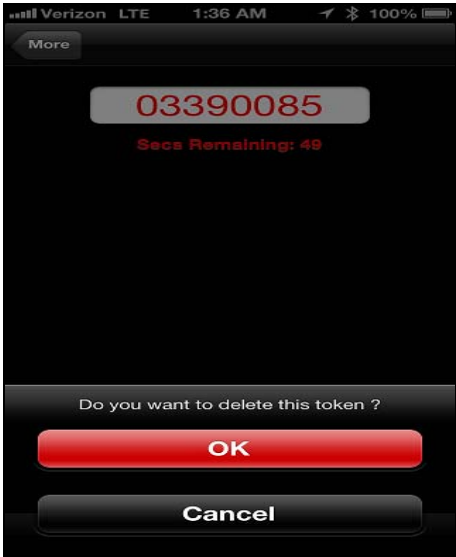




Next Tokencode:



Delete Token:



Token Details:



## Certification Checklist for RSA Authentication Manager

Date Tested: August 6, 2013

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	8.0	Virtual Appliance
SAT Token	3.9.0	iOS
Secure Mobile Desktop	3.0	iOS

## Certification Checklist for RSA Authentication Manager

RSA Software Token Automation – RSA Native Protocol					
	Windows	OS X	Android	iOS	Other
<b>PINless Token</b>					
Next Tokencode Mode	N/A	N/A	N/A	✓	N/A
<b>PINpad-style Token</b>					
Deny Alphabetic PIN	N/A	N/A	N/A	✓	N/A
Next Tokencode Mode	N/A	N/A	N/A	✓	N/A
<b>Fob-style Token</b>					
16-Character Passcode	N/A	N/A	N/A	✓	N/A
Alphanumeric PIN	N/A	N/A	N/A	✓	N/A
Next Tokencode Mode	N/A	N/A	N/A	✓	N/A
<b>Other</b>					
Password-Protected Token	N/A	N/A	N/A	✓	N/A
System-Generated PIN	N/A	N/A	N/A	✓	N/A

DRP / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

## Appendix

Software Token SDK Integration Details			
	Android	iOS	Other
<b>RSA Software Token SDK</b>			
RSA Software Token SDK Version	N/A	1.5	N/A
<b>RSA Software Token Data</b>			
Display Token Serial Number	N/A	✓	N/A
Display Token Expiration Date	N/A	✓	N/A
Number of Tokens Supported	N/A	1	N/A
<b>Provisioning</b>			
File-Based	N/A	✓	N/A
CT-KIP	N/A	✗	N/A
CTF	N/A	✗	N/A

DRP / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration