



**USAID**  
FROM THE AMERICAN PEOPLE

# Guidelines for Remote Access Soft Tokens for Personal Devices

A Mandatory Reference for ADS Chapter 545

New Edition Date: 11/09/2012  
Responsible Office: M/CIO  
File Name: 545mbm\_110912

## Remote Access Soft Tokens for Personal Devices

RSA Remote Access Soft Tokens can be used on USAID employees' and contractors' personally owned mobile smart devices. An "RSA token" is a device, either physical ("hard") or an application on your mobile device ("soft") that provides you with a passcode to access USAID e-mail, and your USAID desktop when you telework via server-based computing (SBC/Citrix).

Soft tokens are offered as an alternative to the RSA hard token. For a listing of devices that are compatible with the soft token application please visit:

[http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators.htm#!offerings\\_for\\_mobile\\_devices](http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators.htm#!offerings_for_mobile_devices)

To obtain a new soft token, employees will need to turn in their hard token to the M/CIO Help Desk.

### Important Note

Please note, M/CIO is not responsible for technical support of personal devices. Therefore, M/CIO will not be able to:

- Troubleshoot any issues with your personal device.
- Install any application or remove any applications on personal devices

M/CIO also is not responsible for software incompatibilities caused by the installation and usage of the remote access applications software.

### Steps to Obtain a Soft Token on a Personal Device

After ensuring your smart device is compatible via the link above, please follow the instructions below:

**Step 1:** Send an e-mail to your Administrative Management Staff (AMS) Officer or your Mission System Manager (Mission employees) requesting a soft token for use on your personal device.

**Step 2:** The AMS officer initiates a Remedy request and assigns it to the Remote Access Security (RAS) Support team. The request will include your name, your log-on ID and your organization.

- If this is a new request (the employee currently has no token at all), the AMS will select 'AMS\SM-Remote Access Request' from the dropdown menu within Remedy.
- If this is to replace a hard token with a soft token, the AMS will select 'AMS\SM-Remote Access Request-Hard to Soft' from the dropdown menu within Remedy.

**Step 3:** The request is received and processed by the RAS Support Team.

**Step 4:** The RAS Support team e-mails a Soft Token User Agreement to the requesting employee. You will need to read, complete the required information, electronically sign the user agreement, and return it to the RAS Support Team via e-mail to [RAS.SUPPORT@usaid.gov](mailto:RAS.SUPPORT@usaid.gov). The user agreement requires information about the type of device and your e-mail account that is set up on the device (this account is typically an outside e-mail account used for personal e-mail). Additional information about your device may be required; all information must be provided before the request can be fulfilled.

**Step 5:** The Remote Access Security Support Team will then review the required information and send the remote access application installation instructions to you. Follow the instructions, install the application and confirm that the application has been installed by sending an e-mail to the Remote Access Security Support Team at [RAS.SUPPORT@usaid.gov](mailto:RAS.SUPPORT@usaid.gov).

**Step 6:** The Remote Access Security Support Team will then send an e-mail to the personal e-mail account with which your device is linked. The e-mail will contain a link to the token and instructions on how to import the Soft Token.

**Step 7:** Follow the instructions to install the application and import the token. After the token has been imported, contact the CIO Help Desk. The CIO Help Desk activates the token, provides support creating your PIN and provides any support needed to use the remote application.

**Step 8:** Send an e-mail to the Remote Access Security Support Team at [RAS.SUPPORT@usaid.gov](mailto:RAS.SUPPORT@usaid.gov) to confirm that you received and activated your token.

**Step 9:** The Remote Access Security Support team completes the process by sending you the Remote Access Security Notice.