

plusID

Using plusID with RSA SecurID® One-Time Passwords:

Commissioning plusID Personal Biometric Tokens as RSA SecurID Tokens

Introduction

RSA – the Security Company of EMC – is a pioneer in the development of “one-time password” technology (OTP). Privaris has taken the security of RSA’s SecurID OTP to the next level by integrating it into the plusID personal biometric token for a three-factor authentication solution. plusID protects the OTP behind a biometric verification and adds the convenience of automatically transferring the OTP via Bluetooth or USB. Certified interoperability with RSA’s SecurID® technology enables plusID products to be used across the complete range of RSA enabled applications in the enterprise and is an important addition to the plusID family.

RSA’s traditional implementation of OTP technology is a single-function key-fob called SecurID with an LCD that displays a 6-digit password which changes every 30-60 seconds. Users must type the displayed password when prompted in order to logon to a computer, application, VPN, web site, etc. That password must match the one simultaneously generated by the RSA Authentication Server software on the back end. This approach significantly reduces the potential for unauthorized access by reducing the ability for passwords to be reused or stolen.

The plusID personal biometric token provides the added security of requiring a biometric verification before generating a SecurID OTP password. plusID works **without making any changes to existing security systems**, giving organizations the ability to **easily move to three-factor authentication**:

1. Something you have – the RSA SecurID one-time password (OTP) generated on the plusID token
2. Something you know – the PIN that is required to generate the OTP, and
3. Something you are – your fingerprint

Not only more secure, plusID makes SecurID more convenient by automatically transferring the OTP to the host computer via USB or Bluetooth, when connected. When no connection is possible (e.g., at a public PC or kiosk) plusID displays the SecurID OTP number on its LCD display, a standard feature on the plusID 75 and 90 models.

RSA has over 19 million SecurID tokens in use today, giving them a huge footprint in the enterprise market. Now plusID can be commissioned as a SecurID token, adding the security of biometric verification, the convenience of automatic transfer of the OTP, and the efficiency of issuing a single credential in place of multiple cards, fobs and passwords. It’s a winning combination.

Support for RSA SecurID furthers Privaris’ goal of making plusID the universal identity credential – capable of working with all major installed security environments – without any changes to legacy systems.

System requirements for using SecurID with plusID personal biometric tokens

1. plusID model 75 or 90 with firmware Version 2.2 or later

SecurID is supported on plusID models 75 and 90 (both come standard with built-in LCDs) with firmware Version 2.2 or later. plusID units running earlier firmware versions will need to be upgraded to Version 2.2 to activate SecurID capability. The easiest way to upgrade firmware is to connect each plusID to a computer running Version 2.2 of the plusID Manager software which will automatically prompt an upgrade.

2. plusID Manager Software Version 2.2 or later

3. RSA SecurID infrastructure

This may include for, example, the RSA Token Provider software Version 4.0 or later. RSA SecurID software applications and infrastructure are provided by RSA.

4. SecurID one-time password (OTP) Seed Token Records (seeds)

These are purchased from RSA or through RSA resellers and loaded onto plusID units by means of the RSA token provisioning software. Multiple OTP seeds can be placed on a single plusID.

5. The Privaris RSA SecurID Support Package (*required on computers where the automatic transfer of the one-time password via USB or Bluetooth is desired.*)

Key questions when preparing for deployment

Have the plusID units been upgraded to firmware Version 2.2?

RSA SecurID is only supported in Version 2.2 or higher of the plusID firmware and plusID Manager Software.

Is the plusID Manager software already installed and confirmed to be working properly?

Be sure that enrollment and management of plusID units is working before starting to implement RSA SecurID.

Does someone involved in the process have Administrative rights on the PC running plusID Manager? Can that person install additional software on this machine? Are there domain policy restrictions related to installation of software?

Admin rights are required in order to load software such as Version 2.2 of the plusID Manager and required RSA software.

If planning to load plusID Manager Software, can MS SQL be installed on the computer?

plusID Manager uses MS SQL (plusID Manager Professional) or MS SQL Compact Framework (plusID Manager Basic)

Does the computer have a CD Drive?

Needed in order to load the software from the plusID Manager installation CD

Are there restrictions on the USB ports on this machine? For example, can you read and write to a memory stick/mass storage device?

In order to upgrade plusID units to the latest firmware, the PC needs to be able to read and write to a mass storage device. Some enterprises restrict this capability.

Depositing RSA SecurID one-time password “seeds” onto a plusID

RSA SecurID seed token records (seeds) are deposited on plusID personal biometric tokens using RSA software. (The plusID Manager application is not used in the process.) RSA Seed Token Records can be deposited on plusID units before or after user enrollment

Step 1: Verify the RSA server version

If you are using a pre-7.1 version, you need to request your RSA 6 digit software Seed Token Records directly from RSA.

If you have RSA 7.1 or later version software you can order the current version RSA software Seed Token Records through your standard RSA purchasing channel.

Step 2: Convert seed records

Once you receive the seed files from RSA (they will be in an xml format), you will need to process the seeds with the “RSA Seed Converter Wizard.” This application converts the file from an xml format to an “sdtid” file format. The seeds are now ready to be loaded to plusID units.

Note: when you use the wizard to create the .sdtid seeds, they must be designated “token code only” – that is, without a PIN. This is a radio button selection in the wizard.

Step 3: Load seeds onto plusID

The seed records can be loaded onto plusID units using any authorized PC that is running RSA Token Provider 4.0 or later, and the Privaris RSA SecurID Support Package, which allows plusID to communicate with the RSA software application.

- i. Connect the plusID unit to the PC via USB
- ii. Run Token Provider 4.0, or other approved RSA software application
- iii. Select Privaris devices as the destination
- iv. Browse to find the seed record you wish to load, select it and click OK. Only one can be loaded at a time. Repeat the process if you plan to load more than one seed on a plusID.
- v. Select the button on the front of the plusID with which you want to associate the RSA function

Using plusID as an RSA SecurID token

Once a valid RSA seed has been loaded onto a plusID personal biometric token, a SecurID one-time password will be automatically generated with each successful biometric authentication. plusID can be used as a SecurID token in two modes: stand-alone mode and connected mode.

Stand-alone mode: refers to reading the one-time password off of the plusID's display and typing it into the application requesting the password, in the same manner in which you would use an RSA SecurID token.

Connected mode: refers to the automatic transfer of the one-time password when a plusID is connected to a PC via USB, or wirelessly via Bluetooth. To use plusID RSA SecurID capability in connected mode, the Privaris RSA SecurID Support Package is required on the PC with which the plusID will be communicating.