Webinar: Debunking the Myths Around RSA SecurID Software Tokens

RSA SecurID Product Management
RSA SecurID software authenticators provide the strength of RSA SecurID two-factor authentication combined with increased end-user convenience and efficient deployment and recovery.

- Enable rapid electronic deployment to a distributed workforce, eliminating the delays, costs and international requirements associated with delivering hardware tokens around the world
- Can be easily redeployed if users leave the organization
- Reduce Help Desk costs caused by lost or forgotten tokens
Two Components of a Software Token

Application/Token Container

- OS-specific application downloaded from RSA.com or app stores
- Must be installed first on a user’s device before provisioning occurs

Customer Token Record (Seed Record)

- Purchased from RSA (SID 820)
- Provisioned by admin to the user’s device
PIN-Pad or Fob Style Usage

- Two methods of usage
- Determined by the administrator prior to provisioning

<table>
<thead>
<tr>
<th>User Experience</th>
<th>6.1</th>
<th>7.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN pad only</td>
<td>PIN pad or Fob style</td>
<td></td>
</tr>
</tbody>
</table>

**PIN Pad Style**

1. Enter PIN in iPhone device.
2. Application displays passcode.
3. Enter passcode in VPN client.

**Fob Style**

1. Enter PIN in VPN client.
2. Obtain token code from SecurID application.
3. Enter token code after PIN in VPN client.
Myth #1: Software Tokens aren’t as secure as hardware tokens
Security Through Copy Protection

• After the token is imported, the token record is protected by a set of system attributes, referred to as “device biometrics.”

• When the application needs to open the token database, it queries the system for the “device biometrics” used, and checks for validity.
  – If the user or malware attempt to copy the token database to another physical machine or device, the “device biometrics” will not match, and it will not be possible to read the token record.

• Benefit:
  – Makes it more difficult for the token to be copied to an unauthorized device
Security Through Protecting the ‘Something you Know’

• The software token application does not know the correct PIN
  – The PIN is not stored in permanent media on the mobile app
  – The user must enter a valid PIN to generate a valid passcode

• When deployed in PIN Pad style, the PIN is entered into the software token application itself.
  – Better protection against PC keyloggers because the PIN is not entered into the user’s PC when authenticating.
The Advantage of Time Based Authenticators...

...versus event based authentication

• Time-based tokens are a better defense against MITM attacks since the tokencode has a small window of validity

• Time-based tokens are less susceptible to phishing attacks since the user (attacker) cannot generate multiple tokencodes for later use

• Event based tokens have a unknown battery life dependant on use. Time-based tokens have set expiration date for planning and replacement. i.e. you won’t know that your event based token’s battery until it fails to produce a tokencode

• Event based tokens are more likely to lose synchronization with server. RSA SecurID Software tokens rely on the mobile device which has a reliable time source.
Myth #2: RSA SecurID Software Token use is restricted to mobile phones only
RSA SecurID Software Authenticators

Mobile Phones and Tablets

RSA SecurID Ready Authenticators

Desktop Tokens

RSA SecurID Mobile SDK

VMware View

Citrix Receiver
Myth #3: Software Token is lost when a user leaves the company
Security Through the Re-Generation of Token Records

• When a RSA SecurID Software Token app user leaves the company the token can be...
  – Unassigned to that user account
  – Assigned to a new user
  – RSA Authentication Manager generates a new software token record at deployment time, allowing a previously used token to be redeployed preserving your investment in the software token.
  – Fast redeployment, lower TCO

• An iOS Software token can be unassigned and reassigned to a Android device when users change mobile devices
  – The software token investment can carry forward as BYOD evolves
Myth #4: Rely on mobile connectivity in order to operate
Security Through Application Contained OTP Generation

• The RSA SecurID Software Token does not require server connectivity to generate the OTP
  – The software application will use the host device to determine current time value
  – Local time, Time Zone and daylight saving time must all be set correctly

• In PIN Pad style
  – The valid passcode will only display when the correct PIN is entered
  – The PIN is never entered into the app you are authenticating against
Myth #5: Provisioning is very difficult
Software Token Provisioning
Seamless and Secure Provisioning of Software Tokens

- Support for two secure token provisioning methods
  - File-Based Provisioning
    - A token file (.SDTID) is generated by AM/SAE
    - File must be delivered to device for import
    - Supported in RSA Authentication Manager 6.x, and 7.1
  - Dynamic Seed Provisioning
    - Provisioning using a protocol (CT-KIP) over HTTPS
    - No seed records exchanged over the wire
    - Supported in RSA Authentication Manager 7.1 (Enterprise License)
Security Through File-Based Provisioning

- A token file (.SDTID) is generated by AM/SAE
  - XML representation of token including seed record
  - Password protection recommended
- File must be delivered to user’s device for import
  - Example: Delivery as an email attachment
    - Most platforms support SDTID email attachments
Security Through Device Binding

• An additional extension attribute can be added to the software token seed record before the SDTID file is generated to bind the software token to a device class (iOS, Android, BB) or a specific device (iPad w/ unique Device ID).

• This device specific attribute is referred to as Device ID

• Benefit:
  – Helps to prevent unauthorized users from importing a token record to an unauthorized device.
Security by Adding Password to Provisioning Process

- RSA recommends a password to be assigned at the time a SDTID file is generated and sent out of band to a user.
- User will be prompted to enter the password to begin the provisioning process.

**Benefit**
- Makes it more difficult for an unauthorized user to import the file into an unauthorized device.

- Applies to File-Based Provisioning only.
Security Through Dynamic Seed Provisioning

- CT-KIP protocol (RFC 4758)
- Provides “over-the-wire” provisioning process for software authenticators
- Instead of generating an .XML file and sending it to a user to import on his device, Dynamic Seed Provisioning generates a one-time URL and activation code, speeding the on-boarding process and providing additional security

- **Benefit:**
  - Reduces the risk that someone may inappropriately access the token record and attempt to provision it to an unauthorized device
  - Speeds deployment and creates an easier user experience
  - Reduces the risk of a replay attack. The activation code can only be used once, so even if a fraudster were to acquire them after provisioning, it would be useless

- Available in RSA Authentication Manager 7.1 only.
Striking a Balance Between Ease of Use and Security

• Extend Self-Service Functionality
  – RSA Deployment Manager (RSA Authentication Manager 6.1)
  – RSA Credential Manager (RSA Authentication Manager 7.1)

• RSA Authentication Manager 8.0 Enhancements
  – Web tier allows CT-KIP Server to be hosted in the DMZ without exposing AM server to external traffic
  – Software tokens can be provisioned via the dashboard
  – Software token security settings can be configured by profile for a particular device type.
    • Users can request software tokens by profile via the self-service console
    – Enhanced search filter for bulk distribution

• RSA Professional Services offers many services that can help build a provisioning infrastructure
THANK YOU