

**RSA SECURID<sup>®</sup> ACCESS**

**Standard Agent  
Implementation Guide**

**VMware Horizon View Client 6.2**

Daniel R. Pintal, RSA Partner Engineering  
Last Modified: August 9<sup>th</sup>, 2016

**RSA**  
**READY**

## Solution Summary

---

VMware Horizon View delivers end-to-end desktop control and manageability while providing a familiar user experience. VMware Horizon View is an enterprise-class connection broker that provides secure connectivity between remote clients and centralized virtual desktops.

Working in conjunction with VMware vCenter, VMware Horizon View provides optimized management and control of desktop operating systems running on VMware ESX.

By default, VMware Horizon View authenticates users using Microsoft Active Directory credentials (username, password, and domain name). As an option, VMware Horizon View can be configured so that users are first required to authenticate using RSA SecurID. VMware Horizon View authentication works in conjunction with RSA Authentication Manager. Two-factor authentication provides enhanced security for access to virtual desktops and is a standard feature of VMware Horizon View.

<b>RSA SecurID Access Supported Features</b>	
<b>VMware Horizon View Client 6.2</b>	
<b>RSA SecurID Authentication via Native RSA SecurID Protocol</b>	Yes
<b>RSA SecurID Authentication via RADIUS Protocol</b>	No
<b>On-Demand Authentication via Native SecurID Protocol</b>	Yes
<b>On-Demand Authentication via RADIUS Protocol</b>	No
<b>RSA Authentication Manager Replica Support</b>	Yes
<b>Secondary RADIUS Server Support</b>	No

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

## Partner Product Configuration

---

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

This section provides instructions for configuring the VMware Horizon View Client to provision RSA Authentication Manager resources. 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 VMware Horizon View Client components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### ***Provisioning***

#### **Windows**

The VMware Horizon View Windows Desktop and Web client provides support for RSA SecurID authentication and requires the user to enter the RSA token code or passcode manually.

#### **Mobile Clients**

The VMware Horizon View Mobile client provides support for RSA SecurID authentication and either manually entering the RSA token or passcode or through token automation. Token automation requires the user or administrator to provision an RSA Software token from the RSA Authentication Manager by one of the three supported methods of provisioning; SDTID, CT-KIP or CTF.

---

**!> Note: For more details related to provisioning and importing of RSA Software Tokens please reference the RSA Authentication Manager Administrators guide and the VMware Horizon View Client guides.**

---

### ***VMware Horizon View Configuration***

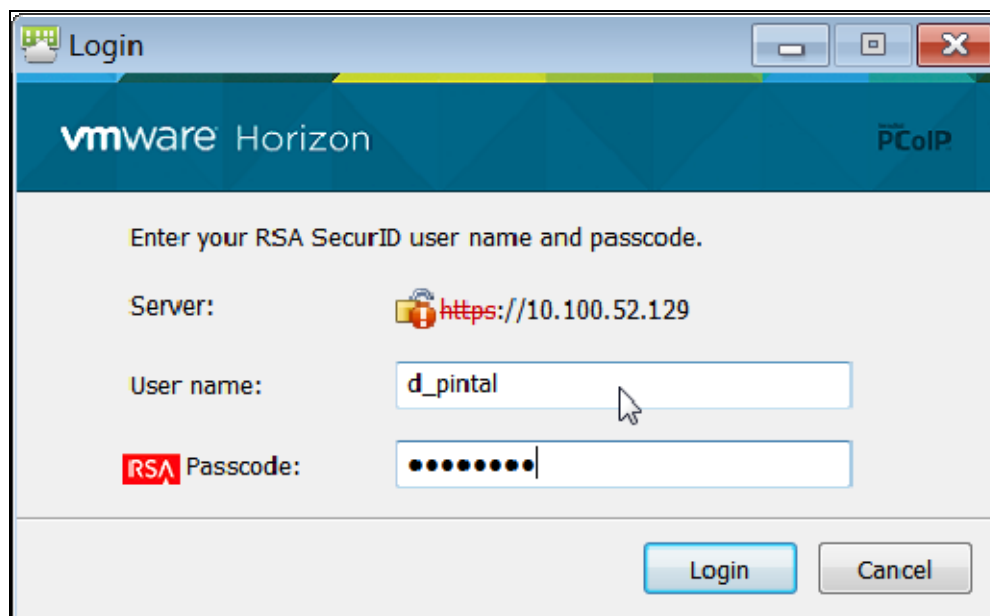
No modification to the client is required, RSA SecurID authentication is implemented using the process outlined within the **VMware\_Horizon\_View\_6\_2\_RSA\_SecurID\_Access\_8.2\_Standard\_Agent** implementation guide. VMware Horizon View Agents adhere to the authentication policy configured within the VMware Horizon View Connection server.

## Screens

---


### Windows and MAC Desktop

Login screen:




vmware Horizon PCoIP

Enter your RSA SecurID user name and passcode.

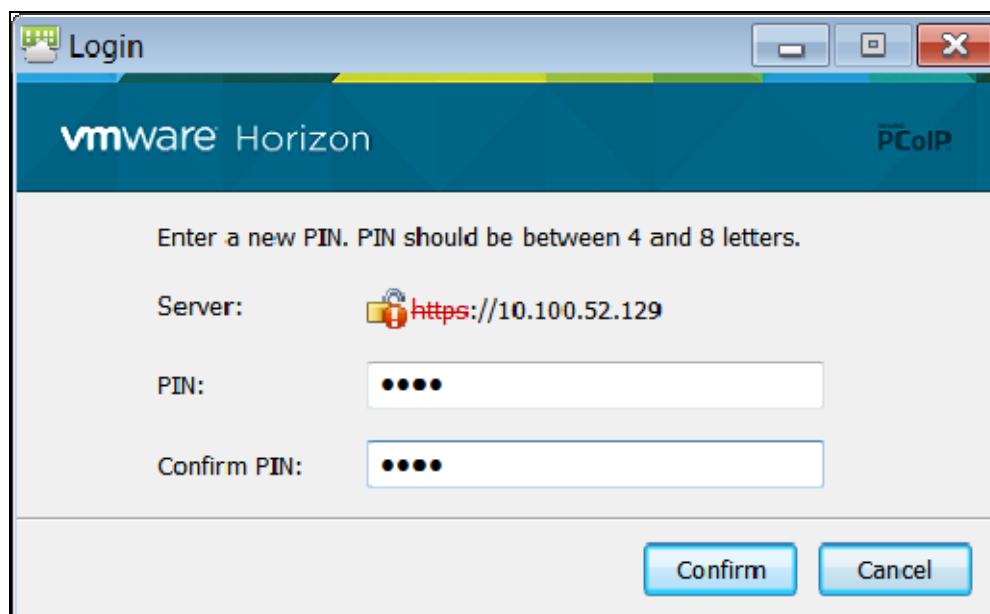
Server:  https://10.100.52.129

User name: d\_pintal

 Passcode: ●●●●●●●●●●


Login Cancel

User-defined New PIN:



vmware Horizon PCoIP

Enter a new PIN. PIN should be between 4 and 8 letters.

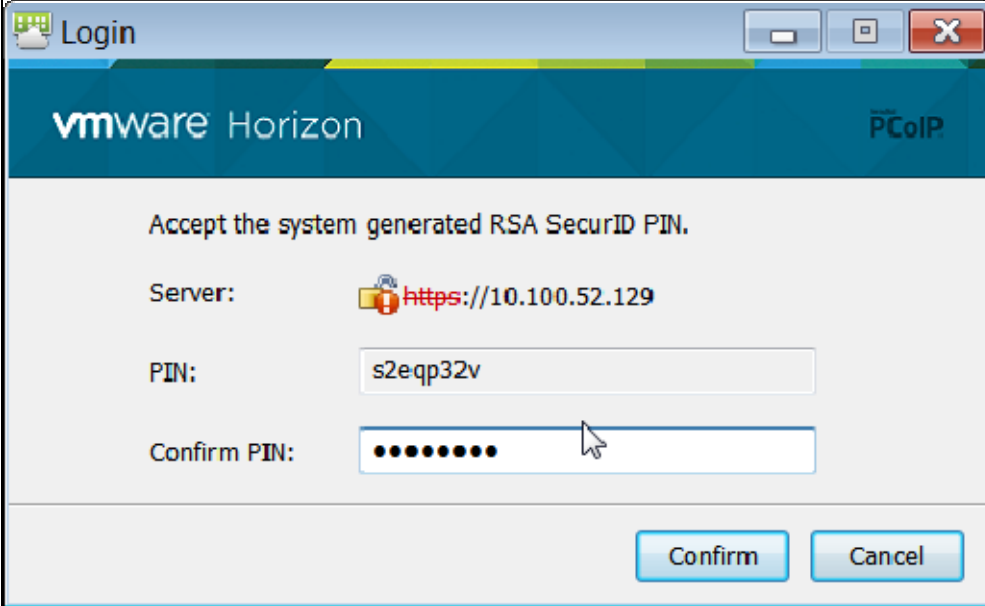
Server:  https://10.100.52.129

PIN: ●●●●


Confirm PIN: ●●●●

Confirm Cancel

System-generated New PIN:

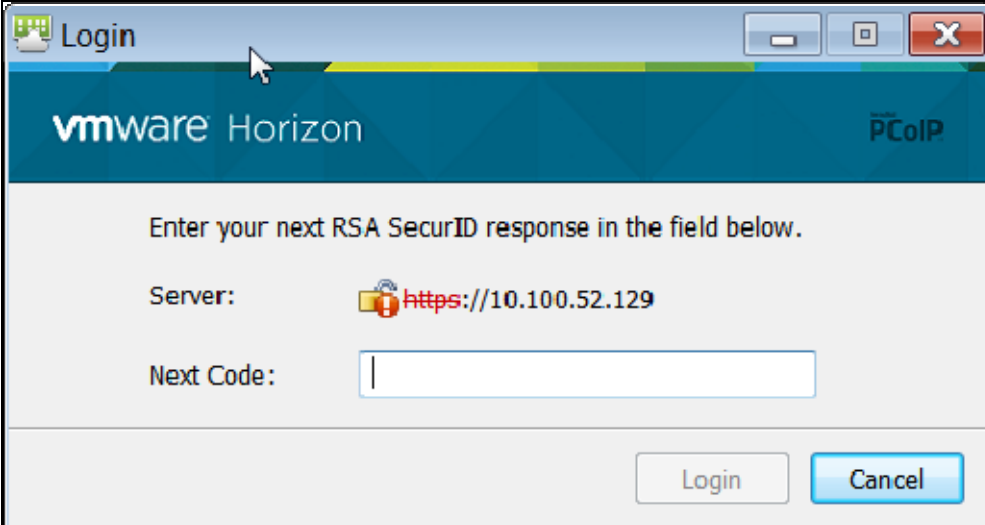


The screenshot shows a 'Login' window for VMware Horizon. The title bar includes the VMware logo and the text 'Login'. The main header is blue with 'vmware Horizon' on the left and 'PCoIP' on the right. The main content area is white and contains the following text and fields:


- Accept the system generated RSA SecurID PIN.
- Server:  <https://10.100.52.129>
- PIN:
- Confirm PIN:

At the bottom right, there are two buttons: 'Confirm' and 'Cancel'.

Next Tokencode:



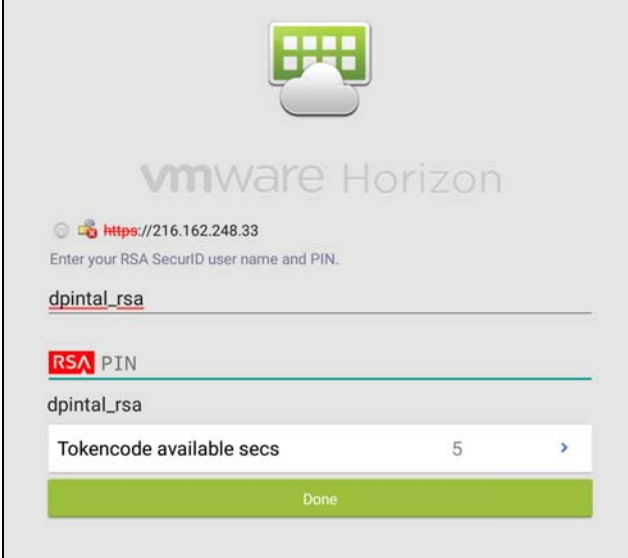
The screenshot shows the same 'Login' window for VMware Horizon. The main content area is white and contains the following text and fields:

- Enter your next RSA SecurID response in the field below.
- Server:  <https://10.100.52.129>
- Next Code:

At the bottom right, there are two buttons: 'Login' and 'Cancel'.

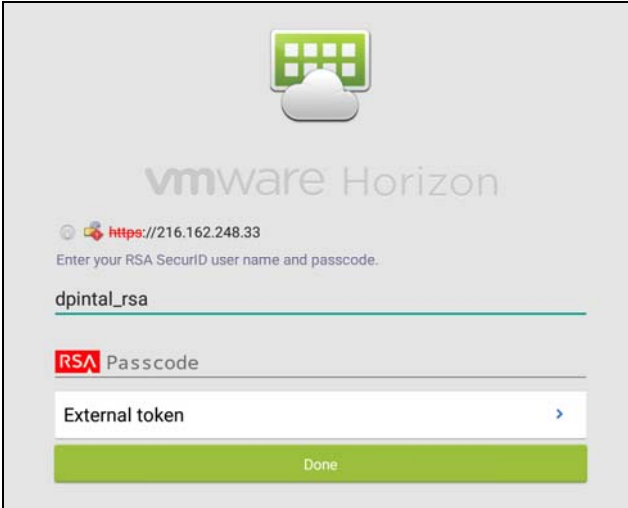
### Mobile (Android)

Software Token PIN Prompt:



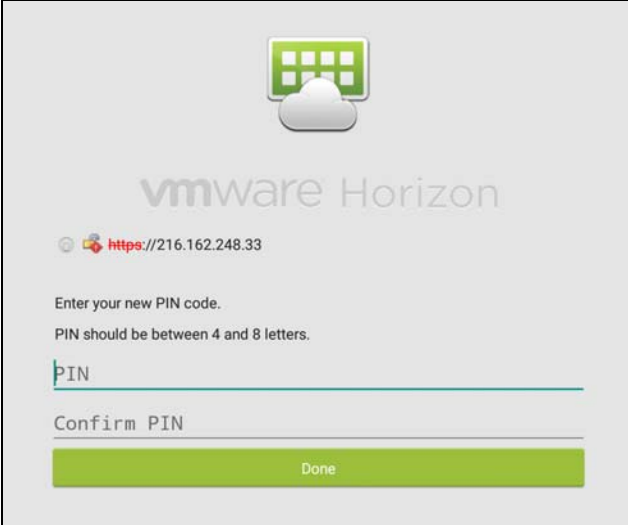
The screenshot shows the VMware Horizon login interface for a Software Token PIN prompt. At the top is the VMware Horizon logo. Below it, the URL <https://216.162.248.33> is displayed. The instruction reads: "Enter your RSA SecurID user name and PIN." The username field contains "dpintal\_rsa". The PIN field is labeled "RSA PIN" and contains "dpintal\_rsa". A "Tokencode available secs" field shows "5" with a right arrow. A green "Done" button is at the bottom.

Login screen:



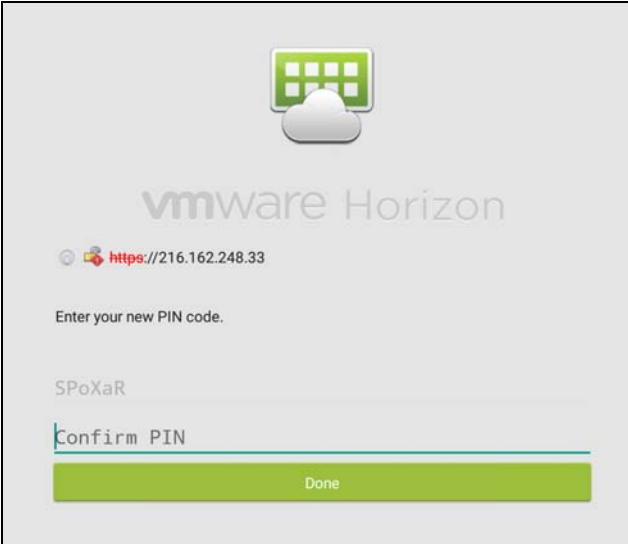
The screenshot shows the VMware Horizon login interface for a standard login screen. At the top is the VMware Horizon logo. Below it, the URL <https://216.162.248.33> is displayed. The instruction reads: "Enter your RSA SecurID user name and passcode." The username field contains "dpintal\_rsa". The passcode field is labeled "RSA Passcode". An "External token" field is present with a right arrow. A green "Done" button is at the bottom.

User-defined New PIN:



The screenshot shows the VMware Horizon PIN creation interface. At the top is the VMware logo. Below it, the text "vmware Horizon" is displayed. A URL "https://216.162.248.33" is shown. The instructions read: "Enter your new PIN code. PIN should be between 4 and 8 letters." There are two input fields: the first is labeled "PIN" and the second is labeled "Confirm PIN". A green "Done" button is at the bottom.

System-generated New PIN:



The screenshot shows the VMware Horizon PIN creation interface. At the top is the VMware logo. Below it, the text "vmware Horizon" is displayed. A URL "https://216.162.248.33" is shown. The instructions read: "Enter your new PIN code." There are two input fields: the first is labeled "SPoXaR" and the second is labeled "Confirm PIN". A green "Done" button is at the bottom.

Next Tokencode:

The screenshot shows the VMware Horizon login interface. At the top is the VMware logo. Below it, the text "vmware Horizon" is displayed. A URL "https://216.162.248.33" is shown with a lock icon. The instruction "Enter your next RSA SecurID response in the field below." is present. A text input field contains "dpintal\_rsa". Below this is an "RSA Passcode" section with a sub-input field labeled "External token" and a right-pointing arrow. At the bottom is a green "Done" button.

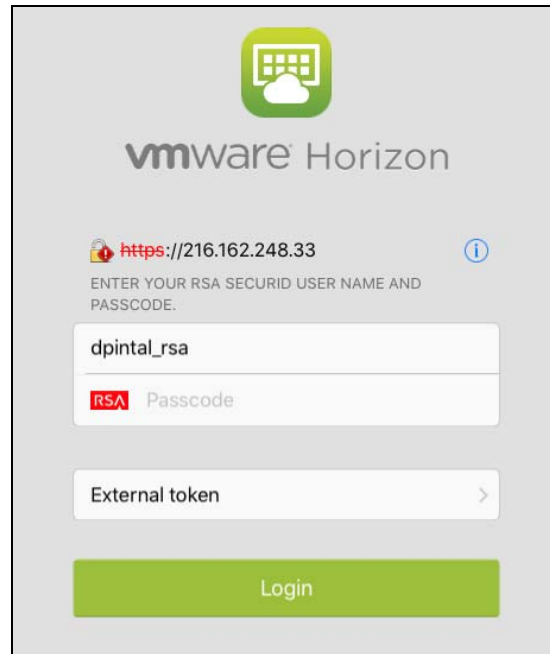
### Mobile (iOS)

Software Token PIN Prompt:



The screenshot shows the VMware Horizon login interface on a mobile device. At the top is the VMware logo. Below it, the text "vmware Horizon" is displayed. A URL "https://216.162.248.33" is shown with a lock icon and an information icon. A text input field contains "gpintal\_rsa". Below this is an "RSA PIN" section with a sub-input field. Below that is a "GPINTAL\_RAA" section with a sub-input field labeled "Tokencode available secs" and a right-pointing arrow showing "10". At the bottom is a green "Login" button.



Login screen:




vmware Horizon

 <https://216.162.248.33> 

ENTER YOUR RSA SECURID USER NAME AND PASSCODE.

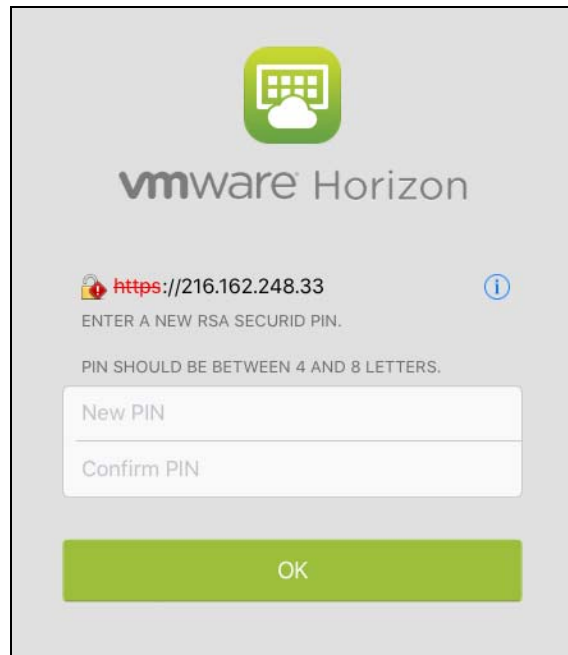
dpintal\_rsa

 Passcode



External token >

Login

User-defined New PIN:



vmware Horizon

 <https://216.162.248.33> 

ENTER A NEW RSA SECURID PIN.

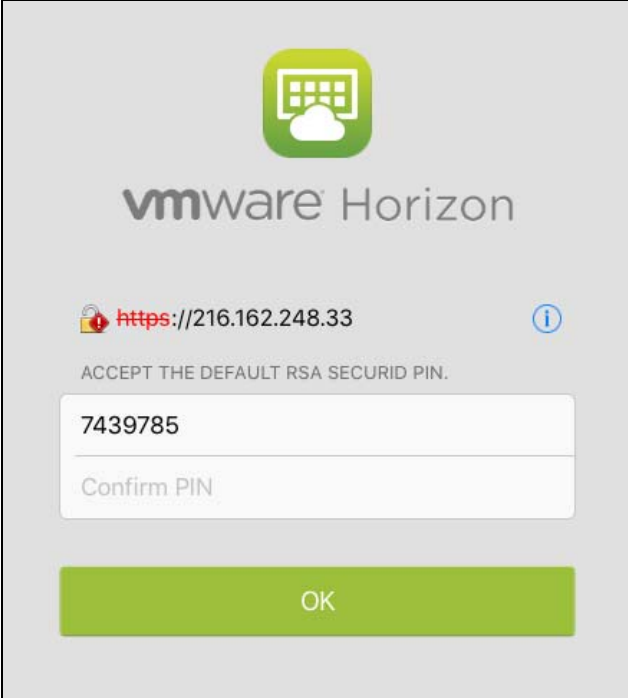
PIN SHOULD BE BETWEEN 4 AND 8 LETTERS.

New PIN

Confirm PIN

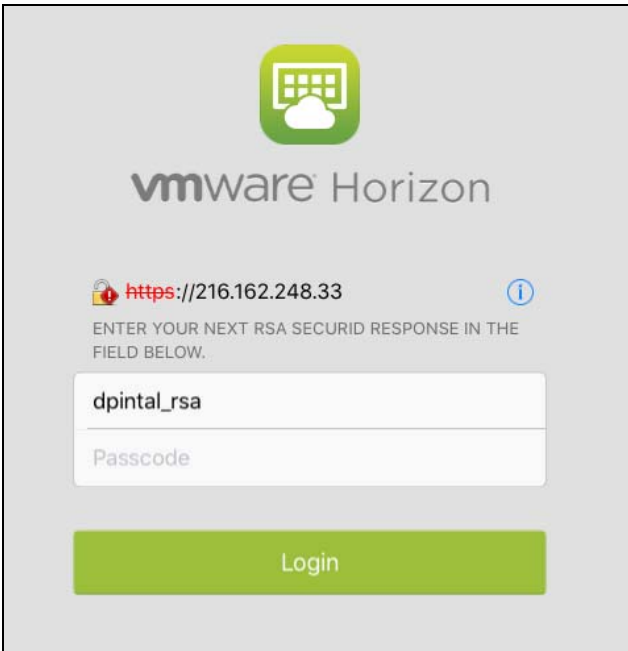
OK

System-generated New PIN:



The screenshot shows the VMware Horizon RSA SecurID PIN entry screen. At the top is the VMware Horizon logo. Below it is the URL <https://216.162.248.33> with a lock icon and an information icon. The text "ACCEPT THE DEFAULT RSA SECURID PIN." is displayed. There are two input fields: the first contains the PIN "7439785" and the second is labeled "Confirm PIN". A green "OK" button is at the bottom.

Next Tokencode:



The screenshot shows the VMware Horizon RSA SecurID Tokencode entry screen. At the top is the VMware Horizon logo. Below it is the URL <https://216.162.248.33> with a lock icon and an information icon. The text "ENTER YOUR NEXT RSA SECURID RESPONSE IN THE FIELD BELOW." is displayed. There are two input fields: the first contains the tokencode "dpintal\_rsa" and the second is labeled "Passcode". A green "Login" button is at the bottom.



## Certification Checklist for RSA SecurID Access

Date Tested: August 9<sup>th</sup>, 2016

Certification Environment		
Product Name	Version Information	Operating System
<b>RSA Authentication Manager</b>	8.2	Virtual Appliance
<b>VMware Horizon View</b>	6.2	Microsoft Windows Server 2012 R2 x64
<b>VMware Horizon View HTML Access</b>	2.4	Microsoft Windows Server 2012 R2 x64
<b>VMware Windows Client</b>	4.01	Microsoft Windows 7 x64
<b>VMware MAC Client</b>	4.1.0	MAC OS X 10.11.6
<b>VMware iOS Mobile Client</b>	4.1	iOS 9.3.3
<b>VMware Android Mobile Client</b>	1.8	Android 6.0.1
<b>VMware Horizon View Agent</b>	6.2	Windows 10

RSA SecurID Authentication – RSA Native Protocol					
	Windows	OS X	Android	iOS	Web Client
<b>New PIN</b>					
Force Authentication After New PIN	✓	✓	✓	✓	✓
System-Generated PIN	✓	✓	✓	✓	✓
User Defined (4-8 Alphanumeric)	✓	✓	✓	✓	✓
User Defined (5-7 Numeric)	✓	✓	✓	✓	✓
Deny 4 and 8 Digit PIN	✓	✓	✓	✓	✓
Deny Alphanumeric PIN	✓	✓	✓	✓	✓
Deny PIN Reuse	✓	✓	✓	✓	✓
<b>Passcode</b>					
16-Digit Passcode	✓	✓	✓	✓	✓
4-Digit Fixed Passcode	✓	✓	✓	✓	✓
<b>Next Tokencode Mode</b>					
Next Tokencode Mode	✓	✓	✓	✓	✓
<b>On-Demand Authentication</b>					
On-Demand Authentication	✓	✓	✓	✓	✓
On-Demand New PIN	✓	✓	✓	✓	✓
<b>Load Balancing / Reliability Testing</b>					
Failover (3-10 Replicas)	✓	✓	✓	✓	✓
No RSA Authentication Manager	✓	✓	✓	✓	✓

✓ = Pass ✗ = Fail N/A = Non-Available Function

## Certification Checklist for RSA SecurID Access

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
<b>PINpad-style Token</b>					
Deny Alphabetic PIN	N/A	N/A	✓	✓	N/A
Next Tokencode Mode	N/A	N/A	✓	✓	N/A
<b>Fob-style Token</b>					
16-Character Passcode	N/A	N/A	✓	✓	N/A
Alphanumeric PIN	N/A	N/A	✓	✓	N/A
Next Tokencode Mode	N/A	N/A	✓	✓	N/A
<b>Other</b>					
Password-Protected Token	N/A	N/A	✓	✓	N/A
System-Generated PIN	N/A	N/A	✓	✓	N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function

## Appendix

RSA Software Token SDK Integration Details			
	Android	iOS	Other
<b>RSA Software Token SDK</b>			
RSA Software Token SDK Version	2.0	2.1	N/A
<b>RSA Software Token Data</b>			
Display Token Serial Number	✓	✓	N/A
Display Token Expiration Date	✓	✓	N/A
Number of Tokens Supported	10	10	N/A
<b>Provisioning</b>			
File-Based	✓	N/A	N/A
CT-KIP	✓	✓	N/A
CTF	✓	✓	N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function