

# Citrix HSD & RSA SoftToken Configuration (Ver-1.2)

## Contents

1) Installation of "DigiCert SHA2 Extended Validation Server CA" certificate.....	2
2) RSA PIN Configuration Guide (only for the first time RSA logins) .....	6

## 1) Installation of "DigiCert SHA2 Extended Validation Server CA" certificate

Please click on the below link

<https://www.digicert.com/digicert-root-certificates.htm>

Click anywhere on the webpage and press CTRL + F keys to search and enter “DigiCert SHA2 Extended Validation Server CA” as shown below:

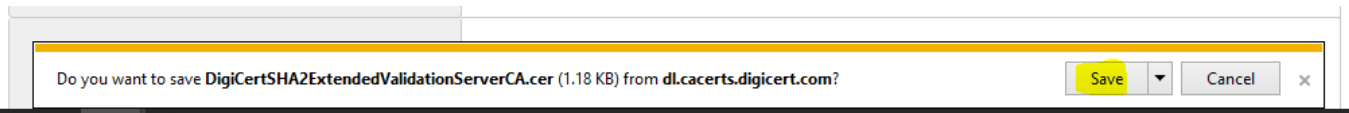
The screenshot shows the DigiCert Root Certificates webpage. A search bar in the top right corner contains the text "DigiCert SHA2 Extended Validation Server CA" and shows "1/1" results. The main content area displays a table of certificates. The fourth certificate, "DigiCert SHA2 Extended Validation Server CA", is highlighted in orange. It lists the issuer as "DigiCert High Assurance EV Root CA", valid until "22/Oct/2028", and provides serial number, SHA1 fingerprint, and SHA256 fingerprint. Links for "Download PEM" and "Download DER/CRT" are provided for each certificate.

Certificate Name	Details
DigiCert Private Server CA	Valid until: 01/Aug/2020 Serial #: 0775EAB2D01E43042ECF147549A180B8 SHA1 Fingerprint: 771FF8A19D15526890BD8934755A73FB23C72788 SHA256 Fingerprint: F8992645B66820D57F53F0D8410325DEA450BD13F02221613075D6AB69C8C8C1
DigiCert SHA2 Assured ID CA	Issuer: DigiCert Assured ID Root CA Valid until: 05/Nov/2028 Serial #: 04AE79606666901AB9C57FA66C58DC0D SHA1 Fingerprint: E12D2E8D47B64F469F518802DFB099C0D86D3C6A SHA256 Fingerprint: A542BCA09C5E4579C619774AE59082BCED0FB6D261C5A7A5A0F6217C10279EA7C
DigiCert SHA2 Assured ID Code Signing CA	Issuer: DigiCert Assured ID Root CA Valid until: 22/Oct/2028 Serial #: 040918185F058B66755343B56F955008 SHA1 Fingerprint: 82C1588E85AF2201CE7915EB538B492F605B80C6 SHA256 Fingerprint: 510447068D237B91B89B781337E6D62656C69F0FCFFBEBE43741367948127B62
<b>DigiCert SHA2 Extended Validation Server CA</b>	Issuer: DigiCert High Assurance EV Root CA Valid until: 22/Oct/2028 Serial #: 0079A944B08C11952092615FE2681083 SHA1 Fingerprint: 7E2F3A4F8FEBFA8A5730AEC029696637E986F3F SHA256 Fingerprint: 403E062A2653059113285BAF80A0D4AE422C84BC9F7BFA001F094B0C5B87FEF1A

Now, make sure that you identified the “DigiCert SHA2 Extended Validation Server CA” certificate and Click on “Download DER/CRT” link as shown below and download the certificate:

This is a close-up of the certificate entry for "DigiCert SHA2 Extended Validation Server CA". The "Download PEM" link is in blue, and the "Download DER/CRT" link is highlighted with a yellow background.

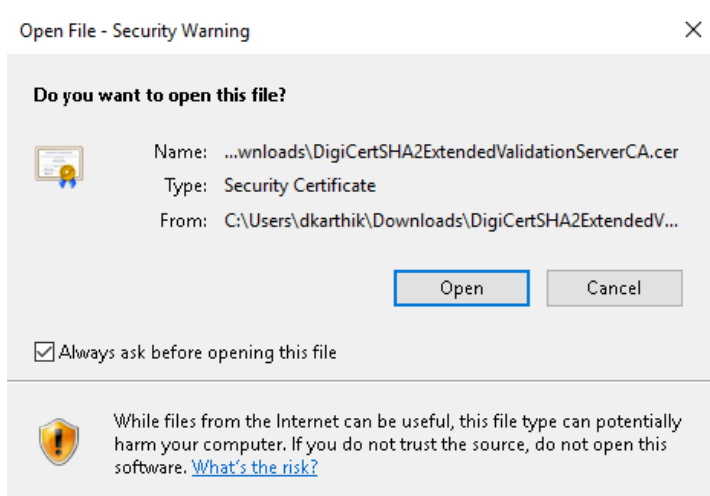
Click on “Save”:



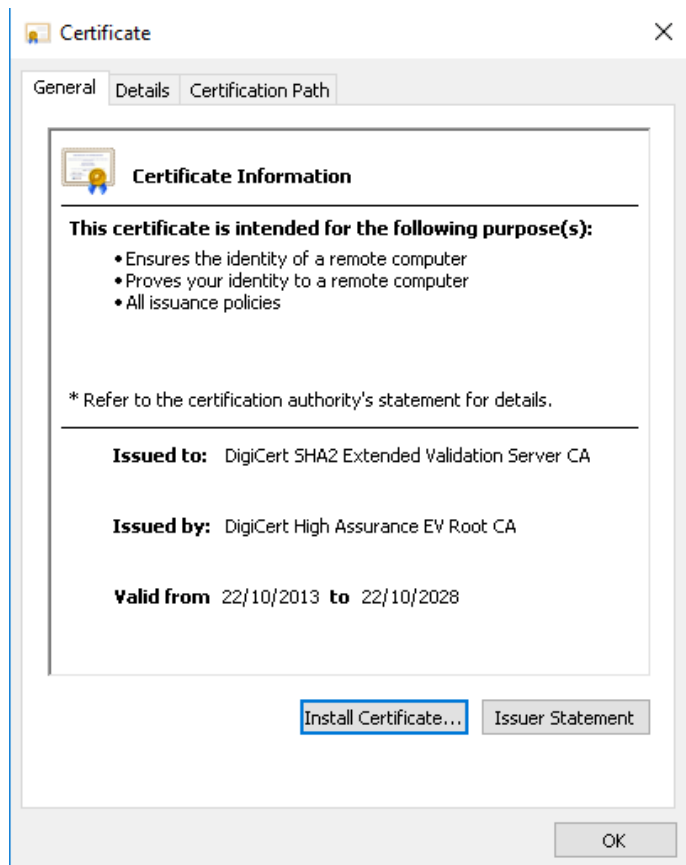
Click on “Open”:



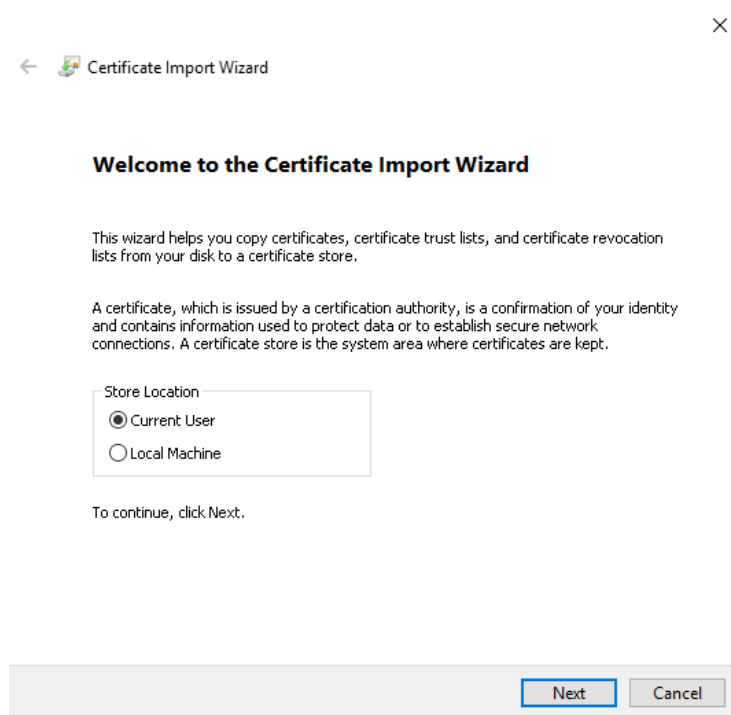
Click on “Open” again:



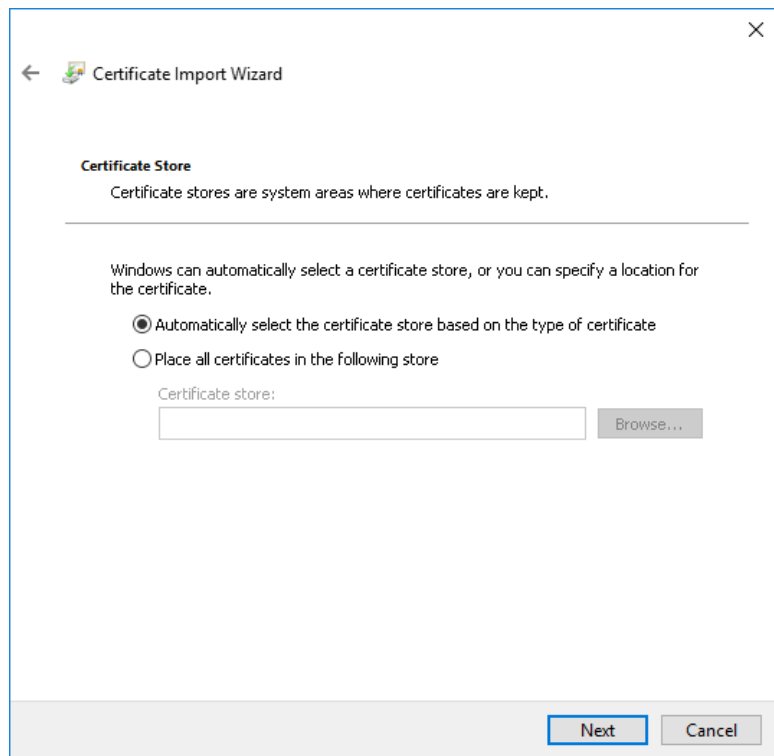
Click on “Install Certificate”:



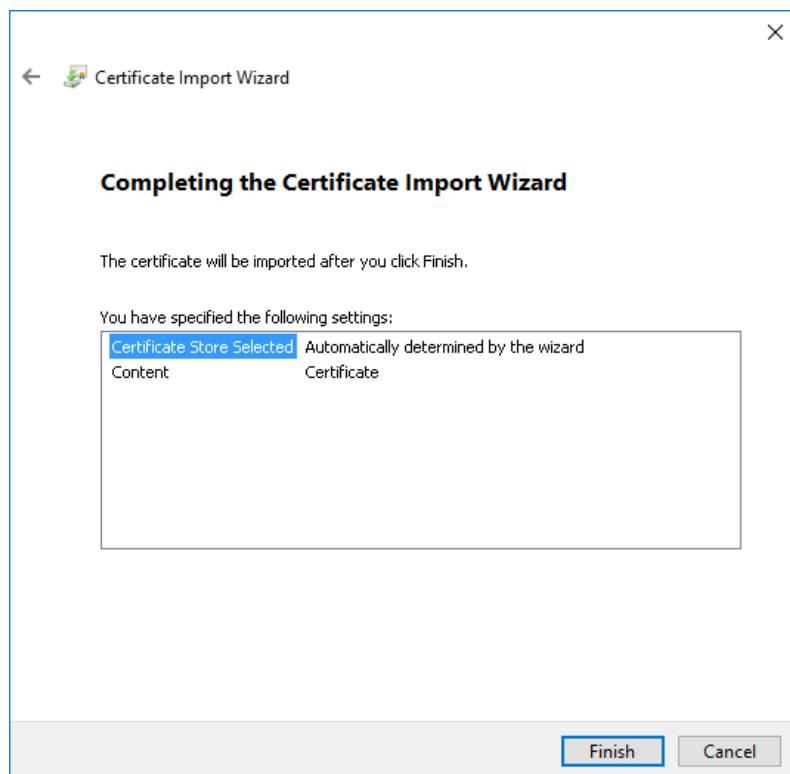
Click on “Next” and make sure “Current User” is chosen:



Click on “Next” and make sure “Automatically Select the certificate...” is chosen:



Click on “Finish” to import the certificate:

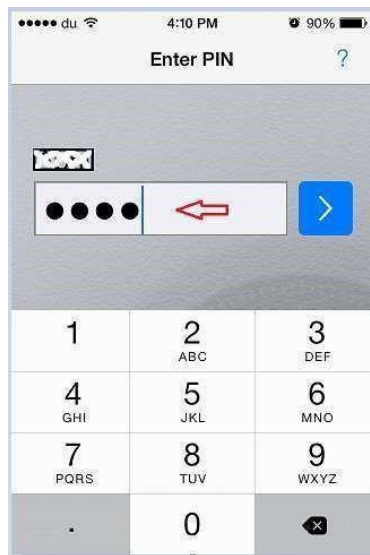


1. Please restart your machine. Login to the machine

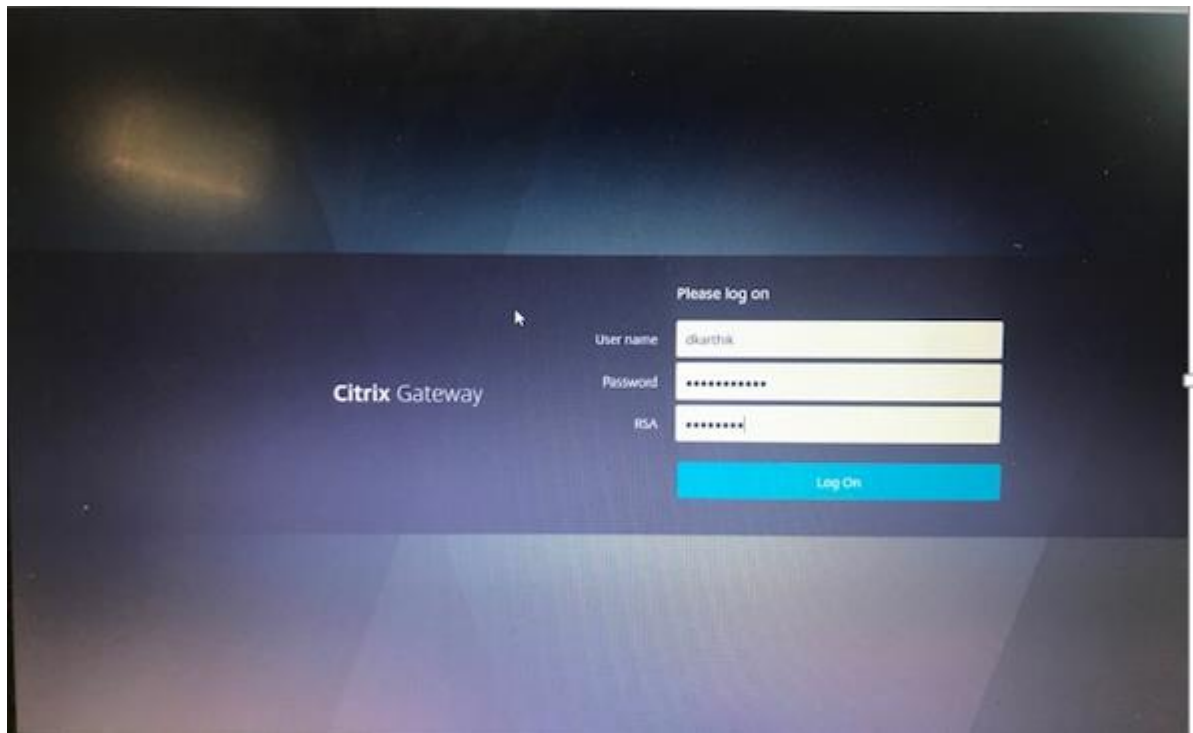
## 2) RSA PIN Configuration Guide (only for the first time RSA logins)

1. Open RSA Secure ID app on the mobile device (applicable to users who are provided with Soft Token) and type 0000 in the enter PIN screen. A passcode will be displayed.

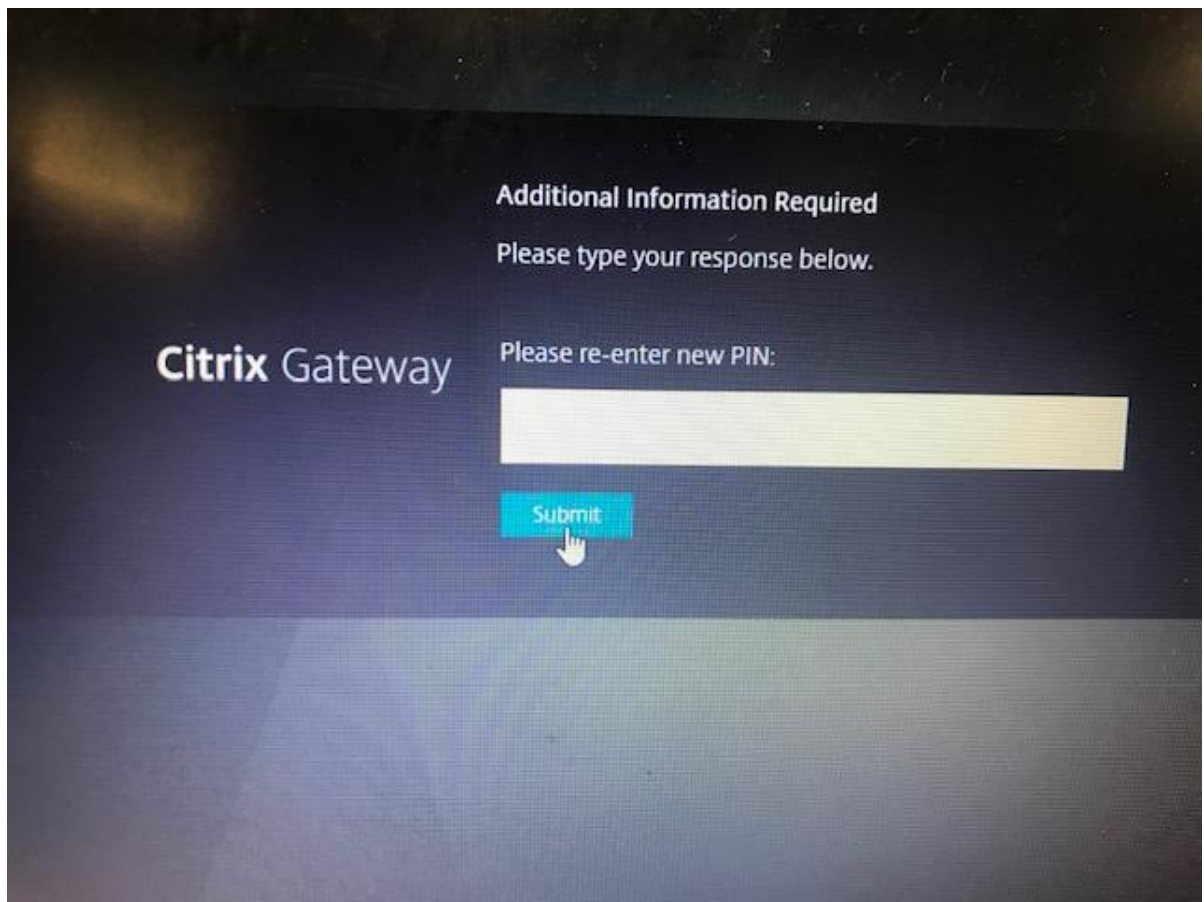
For users who are assigned with physical token, please enter the dynamic number displayed in the device and go to step 4.



1. Open the URL – <https://ctxgw.rakbank.ae> from Internet explorer or Chrome browser.



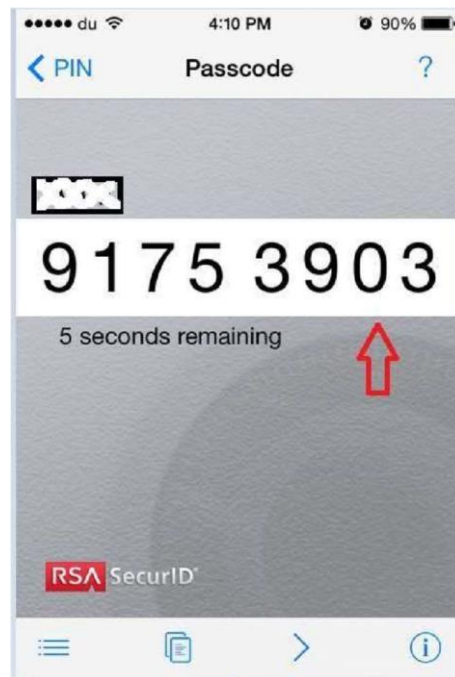
2. Key in your windows user id for 'User name', Windows password for 'password' and enter the dynamic passcode displayed in Step 1 of 'RSA'
  
3. Set a new PIN as shown below:



For users who are assigned with physical token, please go to step:6.

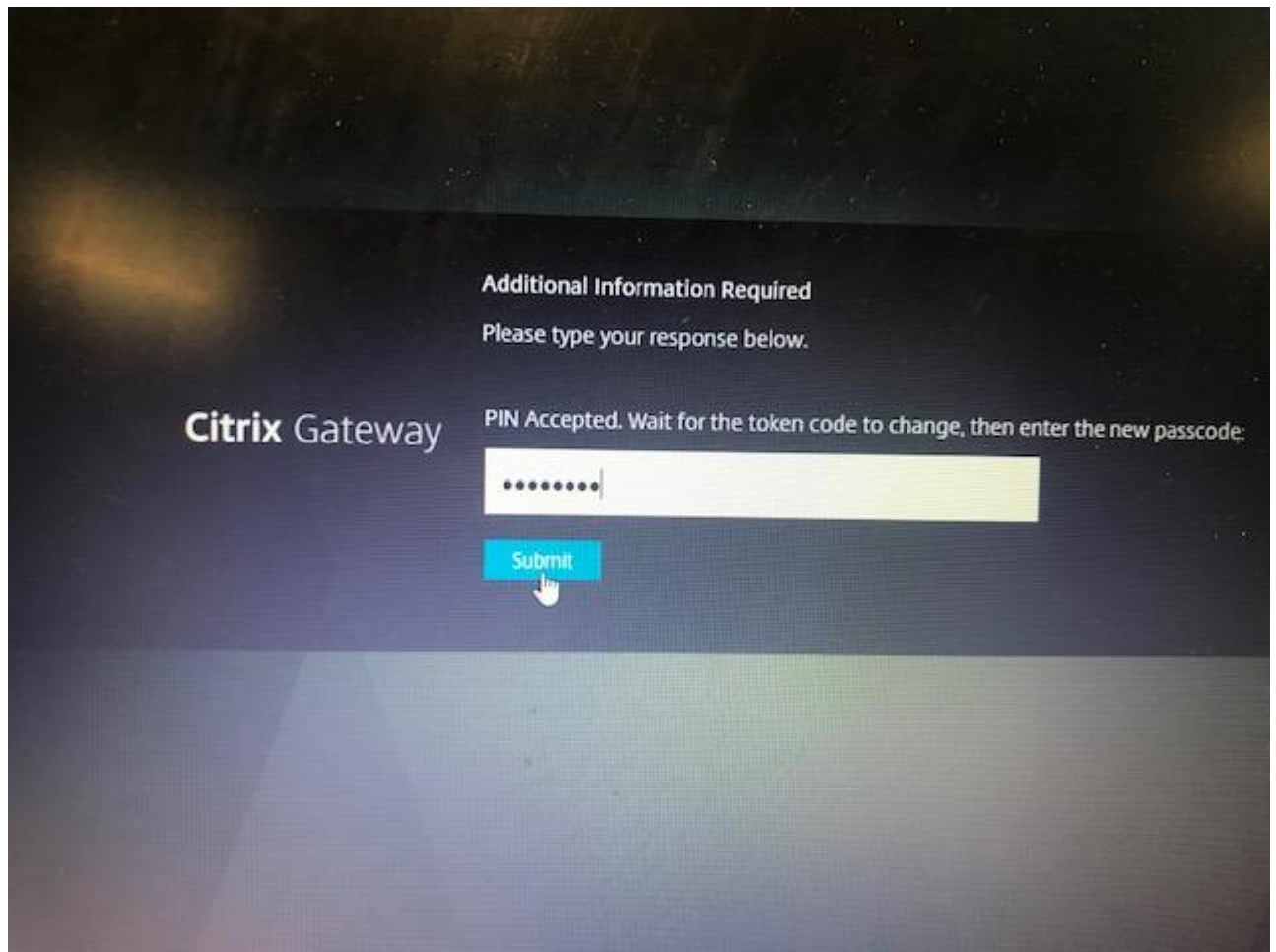
4. Close and reopen the RSA Secure ID app again on your mobile device with the newly created PIN.





5. Now note down this eight digit token and enter the same on the below screen:

For users who are assigned with physical token, enter the 4 digit pin followed by the 8 digit token (together on the same text box) and click on submit.



6. Now click on “Desktops” tab and you will see the assigned HSD /Application on your screen, now click on the icon to launch.

---END OF DOCUMENT---