

How to Download Certs Needed for RDP to HRSA Servers

1. Go to [NIH Certificate Chains](#).
2. Under the section called “Certificate Chains”, select “HHS Device Certificate Chain”

Certificate Chains:

Most digital certificates problems are caused by broken certificate chains.

A certificate chain is a string of certificates from the one you are using (e.g., your certificate) to a certificate that is trusted by your computer. The first link of the chain is a self-signed certificate that a Root Certificate Authority (CA) issues to itself. The next link of the chain is a certificate that the Root CA issues to a Subordinate CA. The last link of the chain is an end-entity certificate that a Subordinate CA issued to you, a webserver, or some other person or device. A certificate chain is broken if your computer does not trust the Root CA or cannot find the certificates that link the end-entity to the trusted root.

The following certificate chains are used at NIH as part of the HHS PKI:

[Entrust FPKI Certificate Chain](#)

Used to trust smart cards and some internal NIH web servers.

[Entrust Public TLS certificate chain](#)

Used to trust some public facing web servers and the NIH VPN.

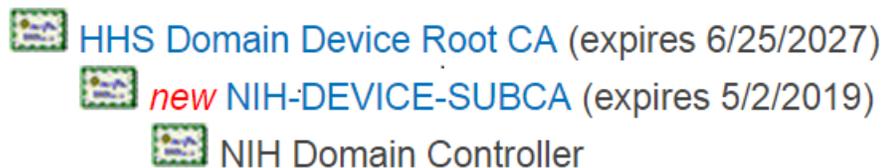
[HHS Device Certificate Chain](#)

Used by your desktop to support smart card login.

3. The page should scroll you down to another section called “HHS Device Certificate Chain”. Click on both the “NIH-DEVICE-SUBCA” and “HHS Domain Device Root CA” links, and save them.

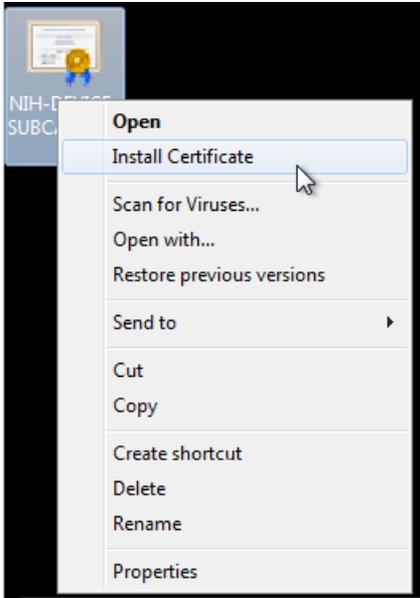
HHS Device Certificate Chain

This certificate chain is the trust path used by NIH desktops and servers to trust NIH domain controllers during smart card logon.



Note: the device PKI certificates must be installed in the Windows Local computer certificate stores.

4. Go to the location that the certificates were saved to, right click on them, and click “install certificate”



5. A wizard will pop up. Without making any changes, click “next” all the way through until the option for “finish” comes up. Click “finish”.
6. A message will pop up saying “the import was successful”. At this point the Certs will have been successfully installed and authenticating to a server over remote desktop using a PIV card will work.