

NCR CFR EPS Bulletin

New Verifone TLS Certificates Available

Summary

Current production Verifone TLS certificates for all Verifone PIN Pad device types will expire on May 13, 2023. This applies to Verifone MX915, MX925, and M400 PIN Pad devices. Due to the pending expiration NCR has new Verifone TLS certificates available to customers. It is strongly recommended that customers who use the Verifone MX915, MX925, or M400 PIN Pad devices to process inside payment card transactions install the new TLS certificate prior to May 13, 2023. If the new TLS certificate is not installed prior to May 13, 2023, the Verifone PIN Pads will stop processing transactions. The new TLS certificate is good for 3 years and will expire on July 13, 2025.

Testing

The new Verifone TLS certificates, which are generic (not customer specific), have gone through testing and are now available for customer lab testing.

Installation

Please reach out to your NCR Account Team for the new Verifone TLS Certificate. Detailed install instructions will be distributed with the TLS certificates and are included following this bulletin.

Support

If any issues occur during installation or testing NCR CFR EPS customers should contact the NCR Help Desk.

NCR Corporation 864 Spring St. NW, Atlanta, GA 30308-1007

©2023 NCR Corporation. All rights reserved. ncr.com

NCR respects [your privacy](#).

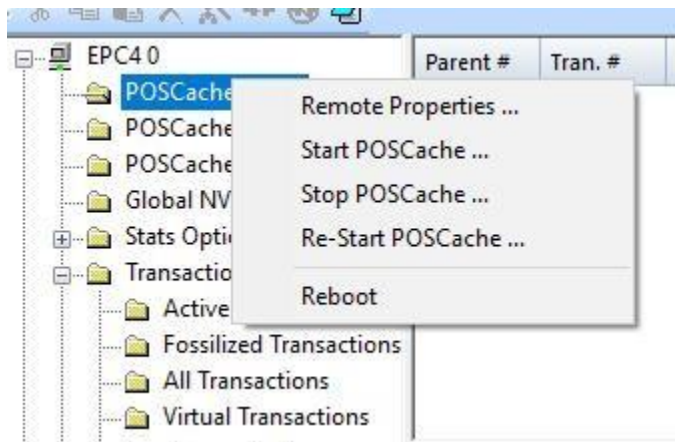


How to Install (or Upgrade) PINpad TLS certificates on EPC

In Epsilon 2.5 and above, we utilize TLS certificates to secure the connection between the PINpad and POSCache. The PINpad certificate is built into the forms and is paired with either a development or production version of the certificate. The PINpad certificate must match the POSCache certificate - so a development POSCache certificate must be paired with the development certificate embedded in the firmware load on the PINpad.

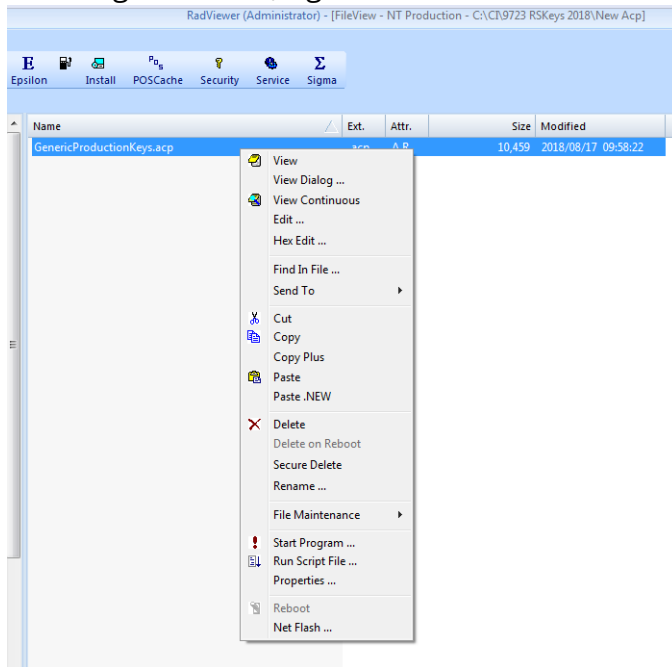
The steps below detail how to install the POSCache certificate on the EPC.

1. Stop POSCache by going to **POSCacheView** and right-click on **POSCache Status**. Select **Stop POSCache**.

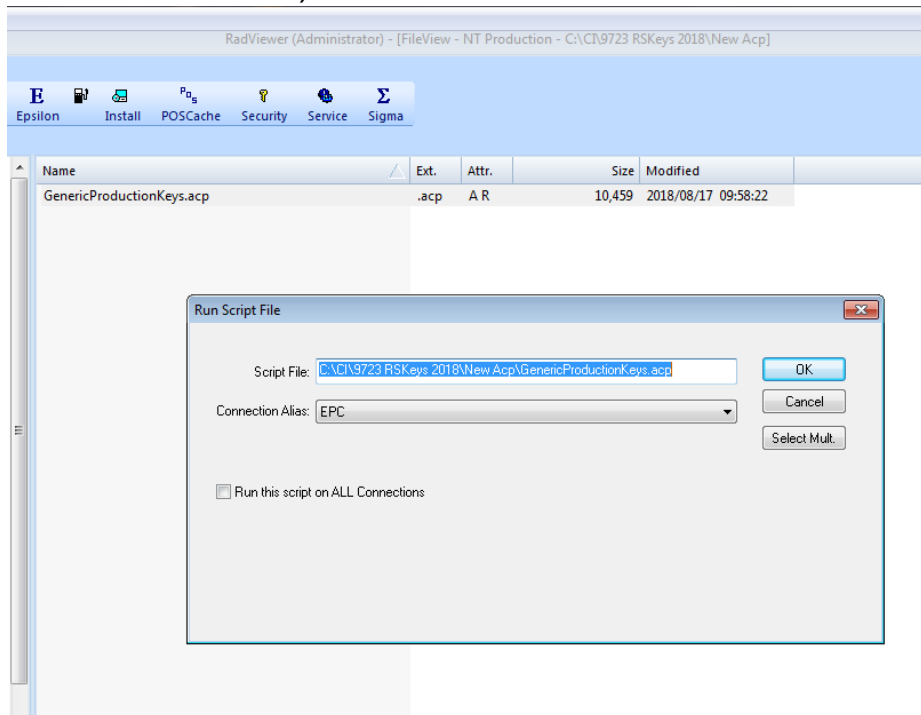


2. Copy the Certificate file (GenericProduction.ACP for Verifone) to the site controller or another system that has Radviewer installed and access to the EPC (or system where POScache is installed).
3. Load Radviewer and enter **FileView**
4. In Radviewer, using **My Local Drive**, browse to the location where the TLS certificate is located.

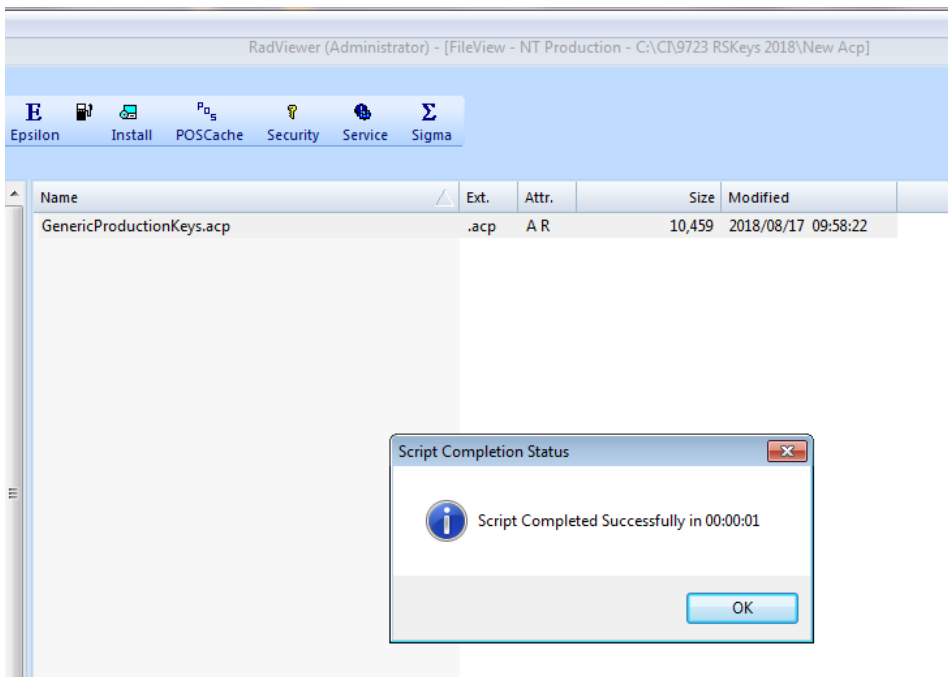
5. In the right window, right-click on the file and select **Run Script File**.



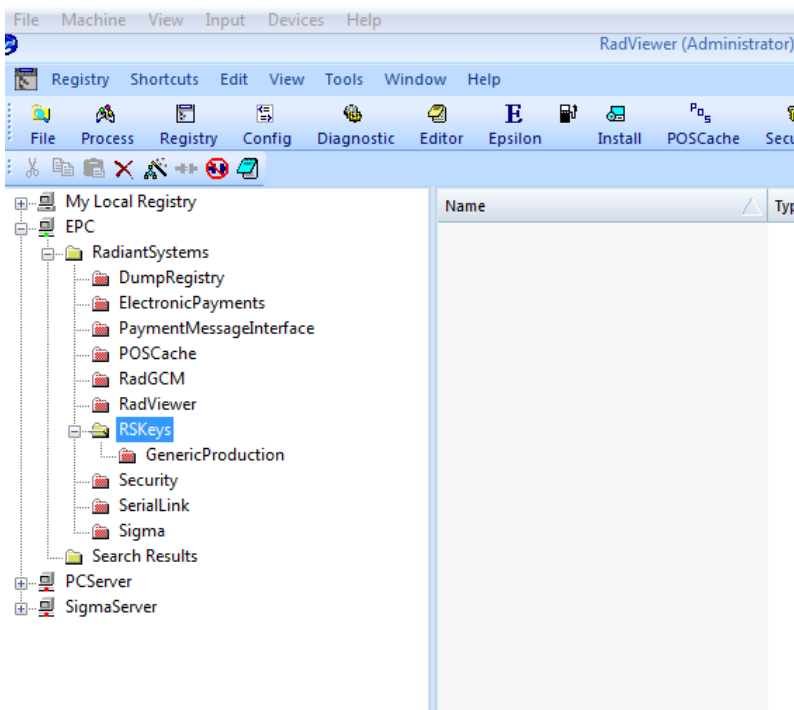
6. You are presented with a destination box. Choose your EPC (or location where POSCache is installed) in **Connection Alias** and hit **OK**.



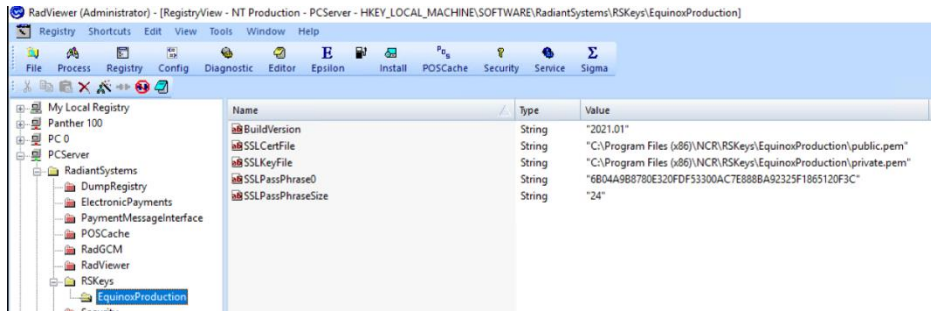
7. The script will complete successfully. If you get any other response, please try again. If it is still failing, please reach out to the NCR Help Desk for support.



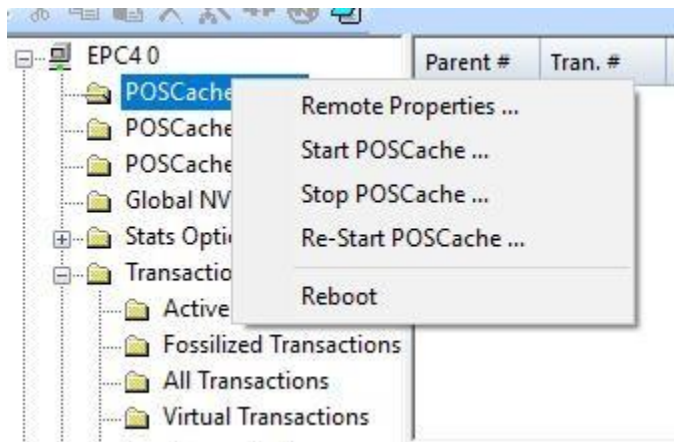
8. To validate it installed (or upgraded) correctly, using **RegistryView**, navigate to the EPC (or wherever you have POSCache installed). Under **RadiantSystems**, look for **RSKeys**. You should see the name of the certificate installed. In this case, we installed GenericProduction.ACP, so that is what is listed.



- Highlight the Key and confirm the following key names are populated. The value of the **BuildVersion** will be set to the date the TLS certificate was generated. For Verifone devices, this should be **2022.7** (prod) or **2018.9** (dev). If it does not match this, please try the steps again. If it still does not match, please reach out to the NCR Help Desk for support.



- Start POSCache by going to **POSCacheView** and right-clicking on **POSCache Status**. Select **Start POSCache**.



- Confirm the PINpad is connected by checking **Global NVP's** in **POSCacheView**. NVP Value should read **UP** for all PINpads. If it does not, please reach out to the NCR Help Desk for support.

