Attribute Certificate Generation

Key Management and Generation

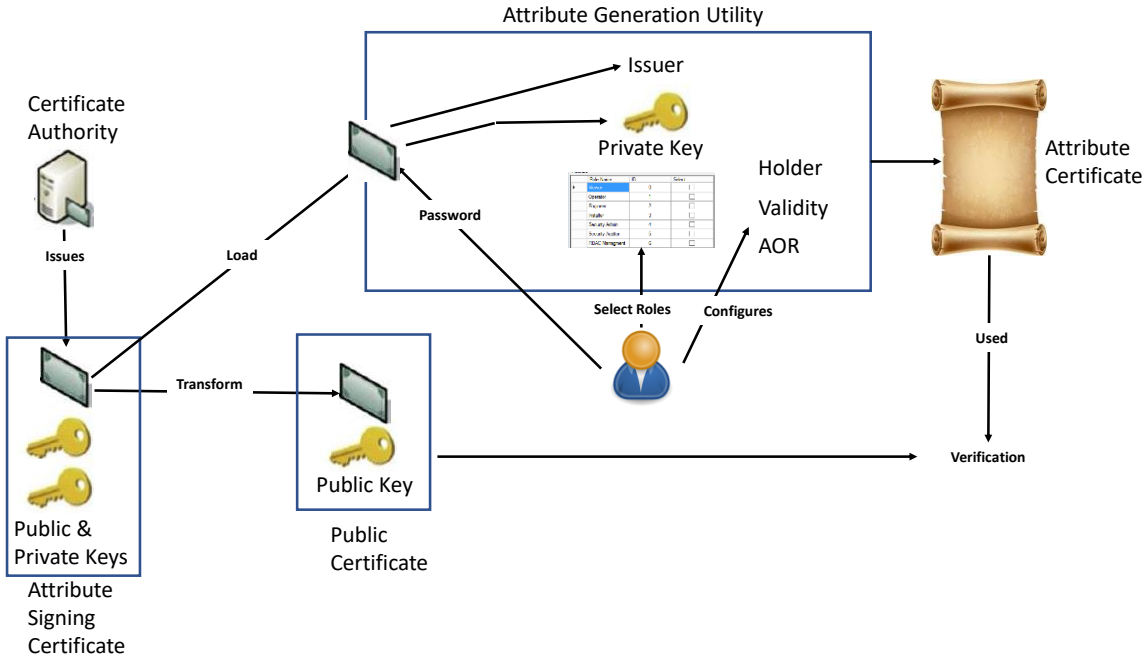
PCItek, LLC & Outside the Box Consulting Services, LLC

PCItek, LLC
P.O. Box 315
Shell Knob, Missouri 65747

Email: sales@pcitek.com
Phone: 903-477-7176

1 Attribute Certificate Generation

The PCItek CENtARI IEC 62351-8 RBAC Certificate Generator, or Attribute Generation Utility (AGU) was created to support secure setup of Role Based Access Controls (RBAC). This utility allows users to create IEC 62351-8 Attribute Certificates.



The general process is to designate a certificate as the Attribute Signing Certificate. This certificate would be an X.509 Identity certificate issued by a Certificate Authority (CA). The user loads the Signing Certificate and must know the password to extract the Private Key in order to sign the Attribute Certificate (AC). The user then enters additional information and creates an AC.

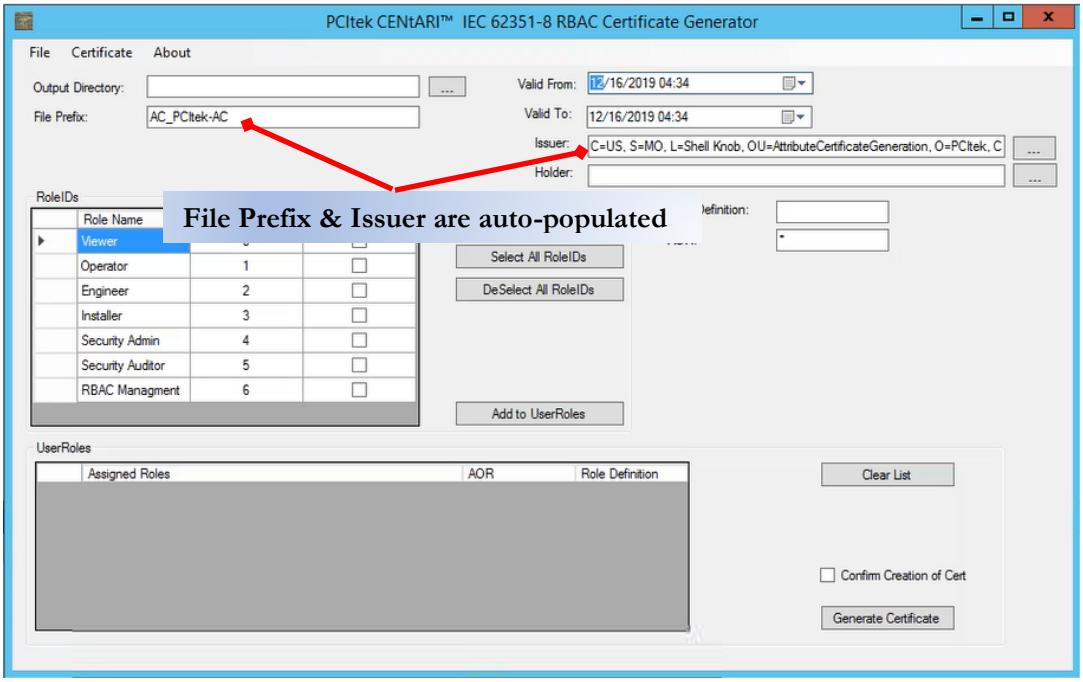
In order to utilize the AC, the end application will need to verify the signature of the AC using the Public Attribute Signing Certificate (e.g. it does not contain the Private key).

1.1 Steps for using the AGU:

The Certificate Authority (CA) should have already issued the Attribute Signing Certificate including both the Public and Private Keys.

1. Users must load that certificate into the AGU.
    a. From the top left menu, select the Certificate dropdown
    b. Select Load Certificate Signing Certificate
    c. Browse for the Attribute Signing Certificate
    d. Double-click the certificate (for the example below, PCItek-AC.pfx was used)

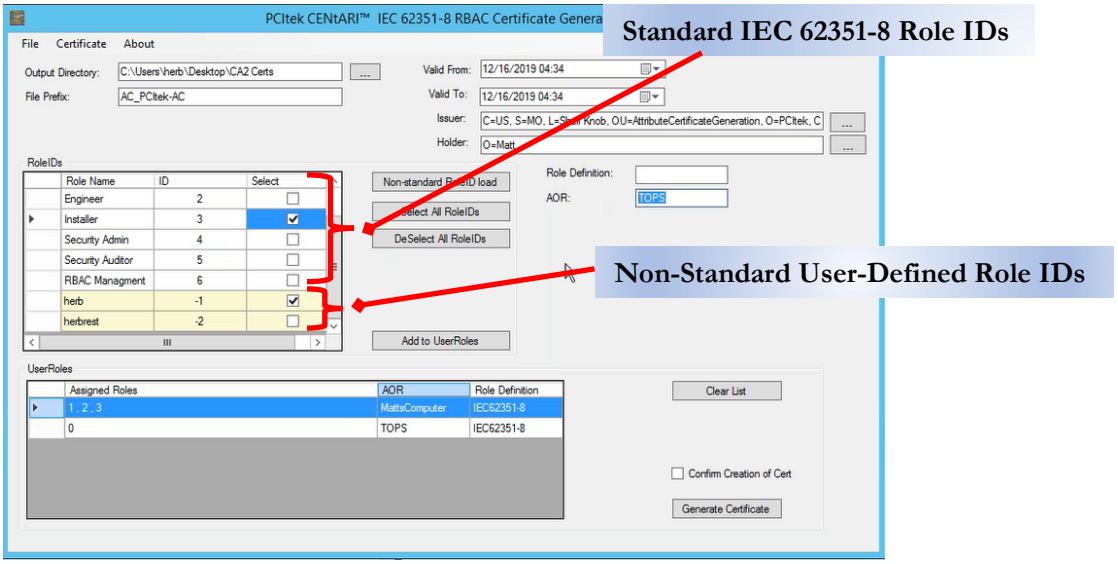
e. The AGU extracts Issuer and the Private Key of the Attribute Signing Certificate by entering the password required to extract the private key. Without entering the proper Key, you cannot move past this step. The File Prefix and the Issuer are auto-populated.



2. Enter a value in the Holder field. You must use valid Relative Distinguished Names (RDN). For example, O=Name, where O is Owner and Name is the name of the user to whom you are assigning access. The … button for Holder, or Issuer value, provides help in creating the RDNs.
3. Specify the Output Directory for the Attribute Certificate in the Output Directory field.
4. Select the Role IDs to be assigned to the user by checking the boxes next to the right of the Role Names.
    a. You may select Standard Role IDs that are already defined in the AGU. If only standard Role IDs are selected, then the Role Definition field can be left blank since the utility defaults to a Role Definition of “IEC62351-8” to represent that the Role IDs comply with the IEC62351-8 standard.

b. You may also load Non-standard Role IDs using the “Non-standard Role ID Load”

   i. All non-standard Role IDs that are added will show with a negative ID number.

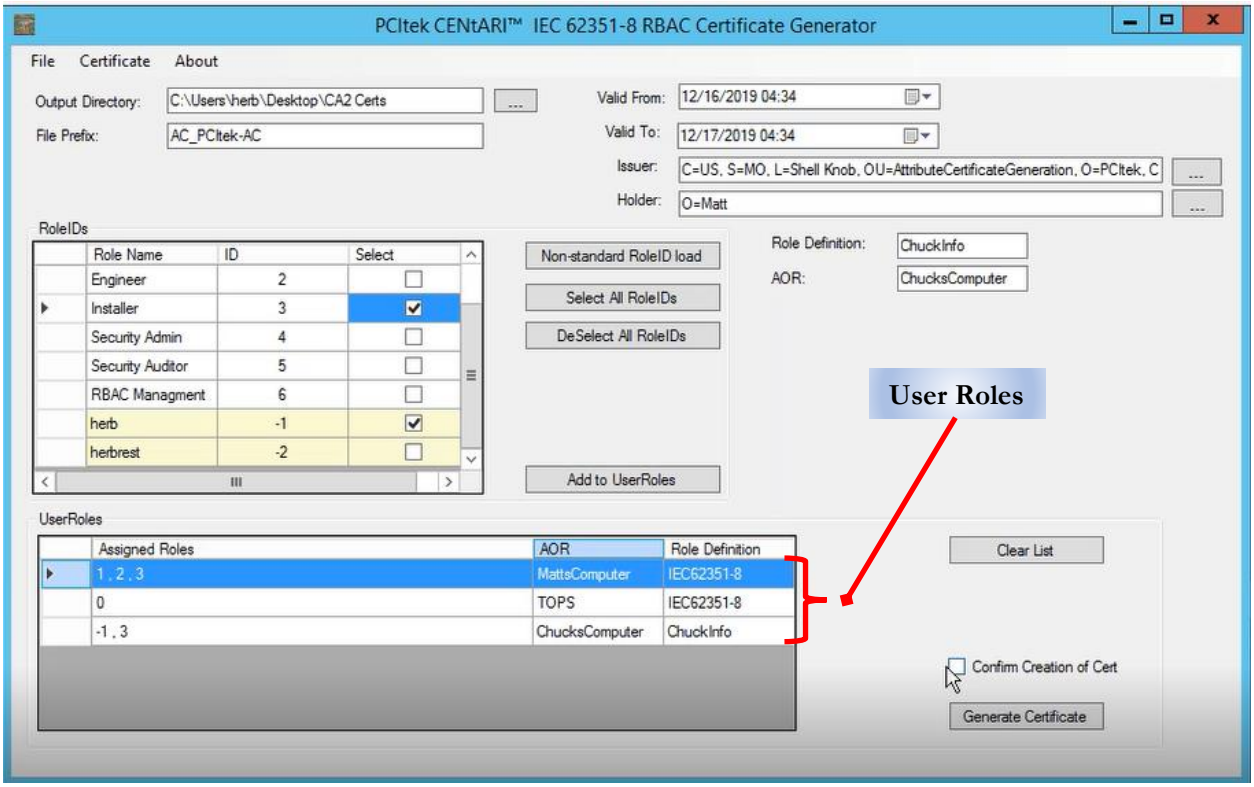


The non-standard roles are loaded by creating a Comma Separated Variable (CSV) file that has two (2) columns. The first column of the CSV is a negative number (indicating custom RoleID). The second column of the CSV is the name of the Role.

   ii. If any non-standard Role IDs are selected, then the Role Definition field should be filled in with a descriptive custom value. In the current release, if left blank, the utility defaults to a Role Definition of “IEC62351-8” and will not error.

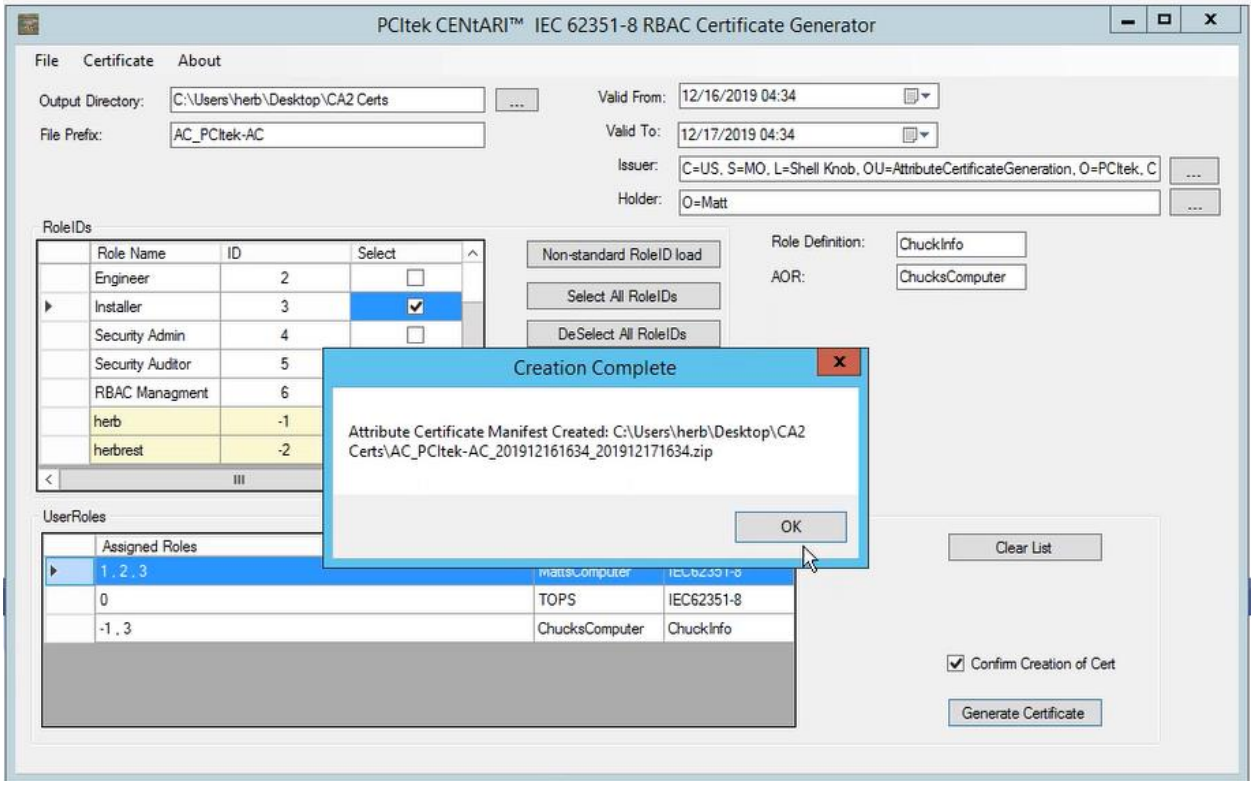
5. Add a description in AOR (Area of Responsibility)

6. Once Role IDs are selected, click “Add to User Roles”, which will add a line for that user to the User Roles chart.

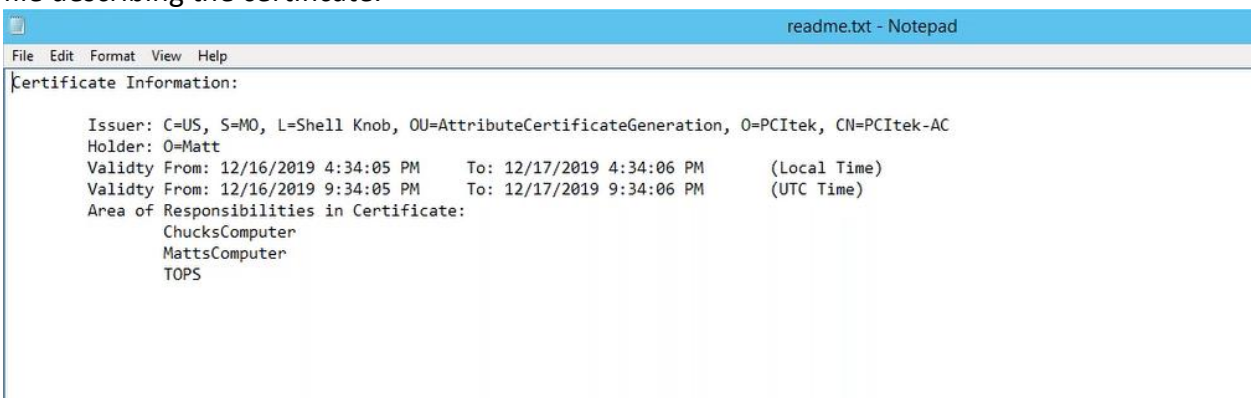


7. If desired, you may enter multiple User Roles to be included in the same Attribute Certificate.
8. Update the “Valid From” and “Valid To” date/time fields to set desired validity dates and times. Note that times will be converted to UTC when the certificate is created.
9. Before generating the certificate, consider whether you want a confirmation notification.

10. Click the “Generate Certificate” button.



11. Check the Output Directory you defined to find the generated certificate and a readme file describing the certificate.



Feedback is welcome. Please send to:

Email: sales@pcitek.com Phone: 903-477-7176

While this application is available as freeware, free support for this application is not implied or intended.