



## 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: <u>sales@pcitek.com</u> 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.

		PCItek CENtAR	I™ IEC 62351-8 RBAC Certifi	cate Generator	_ 🗆 X
File Certificate Output Directory: File Prefix:	About		Valid From: 12/16/201 Valid To: 12/16/201 Issuer: C=US, S= Holder:	9 04:34	reGeneration, O=PCItek, C
RoleIDs Role Nam Viewer Operator Engineer	ne File Prefi	ix & Issuer	are auto-populate Select All RoleIDs DeSelect All RoleIDs	d Vefinition:	
Installer Security A Security A RBAC Ma	Admin 4 Auditor 5 anagment 6		Atta the Pole		
			Add to UserRoles		
Assigned	d Roles		AOR Role Definition	on	Clear List
				Con	firm Creation of Cert rate Certificate

- 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.

2				PCItek CENt	tARI™ IEC 62351-	8 RBAC (	Certificate Genera	Standard IEC 6	0351	Role IDe	
File	Certificate	About	t					Stanuaru IEC 02	-551-0	o Role IDS	
Outp	ut Directory:	C:\Use	rs\herb\Desktop\C	A2 Certs	Valid	From: 12/	16/2019 04:34				
File F	Prefix:	AC_PC	Itek-AC		Val	d To: 12/	16/2019 04:34				
					ls	suer: C=	JS, S=MO, L=Shar Knob.	. OU=AttributeCertificateGeneration, O=PCItek, C			
					н	older: O=	Matt				
Role	IDs										
	Role Name	•	ID	Select	Non-standard	P .eID load	Role Definition				
	Engineer		2		select All	RoleIDs	AOR:	TOPS			
	Installer		3								
L	Security Ad	Imin	4		DeSelect A	II HoleIDs					
L	Security Au	uditor	5		1		N	Non-Standard II	ser_T	efined Role	IDe
L	RBAC Man	agment	6				-0	Non-Standard O	SCI-L	Junica Role	1D5
	herb		-1								
	herbrest		-2		·		_				
<			Ш	>	Add to Us	erRoles					
User	Roles								î.		
	Assigned	Roles			AOR	Role	Definition	Clear List			
►	1.2.3				MattsCompute	r IEC6	351-8				
	0				TOPS	IEC62	351-8				
								Confirm Creation of Cert			
								Generate Certificate			

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.

				PCItek (	ENtAR	™ IEC 62351-8 R	BAC Certif	icate Generator		>		
ile	Certificate	About										
Output	Directory:	:\Users\her	b\Desktop\0	CA2 Certs		Valid From	n: 12/16/201	19 04:34				
File Pre	fix: 7	AC_PCItek-A	.C			Valid To	12/17/201	12/17/2019 04:34				
						Issuer	C=US, S=	MO, L=Shell Knob, OI	 J=AttributeCertificateGener	ation, O=PCltek, C		
						Holder	O=Matt					
RoleID	)s							Dela Defeware				
	Role Name	ID	1.8	Select	^	Non-standard Role	ID load	Hole Definition:	ChuckInfo			
	Engineer		2			Select All Role	IDs	AOR:	ChucksComputer			
•	Installer	_	3			De Calant All Da						
	Security Admin	n or	4		-	Deselect All No	eiDs					
	BBAC Manag	ment	6		=				User Roles			
	herb		-1						User Roles			
	herbrest		-2		~							
<		m			>	Add to UserRo	les					
UserRo	oles											
	Assigned Ro	les				AOR	Role Definiti	on	Clear Li	st		
۲	1,2,3					MattsComputer	IEC62351-8	<b>n</b> /				
	0					TOPS	IEC62351-8	<b> ⊢ ∡</b>				
	-1.3					ChucksComputer	ChuckInfo					
									Confirm Cre	ation of Cert		
									~			
									Generate Cer	tificate		

- 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.

le	Certificate A	bout				100					
Dutput	Directory: C:	Users\herb\Desktop	CA2 Certs		Valid From	1: 12/16/201	19 04:34				
ile Pr	efix: AC	_PCltek-AC			Valid To	12/17/201	12/17/2019 04:34				
					Issuer:	C=US, S=	MO, L=Shell Knob, Ol	J=AttributeCertificateGeneration. 0=PCI	tek, C		
					Holder	: 0-Matt					
Rolell	Ds					-man					
	Role Name	ID	Select	^	Non-standard Role	ID load	Role Definition:	ChuckInfo			
	Engineer	2					AOR:	ChucksComputer			
•	Installer	3	✓		Select All Role	Select All RoleIDs					
	Security Admin	4		DeSelect All RoleIDs	elDs						
	Security Auditor	5			Creation Comple	te	e 🛛 🗶				
	RBAC Managm	ent 6	1								
	herb	-1	Attribute Cer	Attribute Certificate Manifest Created: C:\Users\berb\Deskton\CA2							
	herbrest	-2	Certs\AC_PC	tek-AC_20	01912161634_20191217	1634.zip					
<		ш									
JserF	loles						OK				
	Assigned Role	s					OK	Clear List			
•	1.2.3				mattscomputer	12062301-8					
	0				TOPS	IEC62351-8					
	-1.3				ChucksComputer	ChuckInfo					
								Confirm Creation of Cert			
								Generate Certificate			

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

<b>()</b>					readme.txt - Notepad	
File Edit Format	View Help					
¢ertificate In	formation:					
Issuer Holder	: C=US, S=MO, L=S : O=Matt	hell Knob, OU=At	tributeCertific	ateGeneration,	O=PCItek, CN=PCItek-AC	
Validt	y From: 12/16/201	9 4:34:05 PM	To: 12/17/2019	4:34:06 PM	(Local Time)	
Validt	y From: 12/16/201	9 9:34:05 PM	To: 12/17/2019	9:34:06 PM	(UTC Time)	
Area o	f Responsibilitie ChucksComputer MattsComputer TOPS	s in Certificato	2:			

Feedback is welcome. Please send to:

Email: <u>sales@pcitek.com</u> Phone: 903-477-7176

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