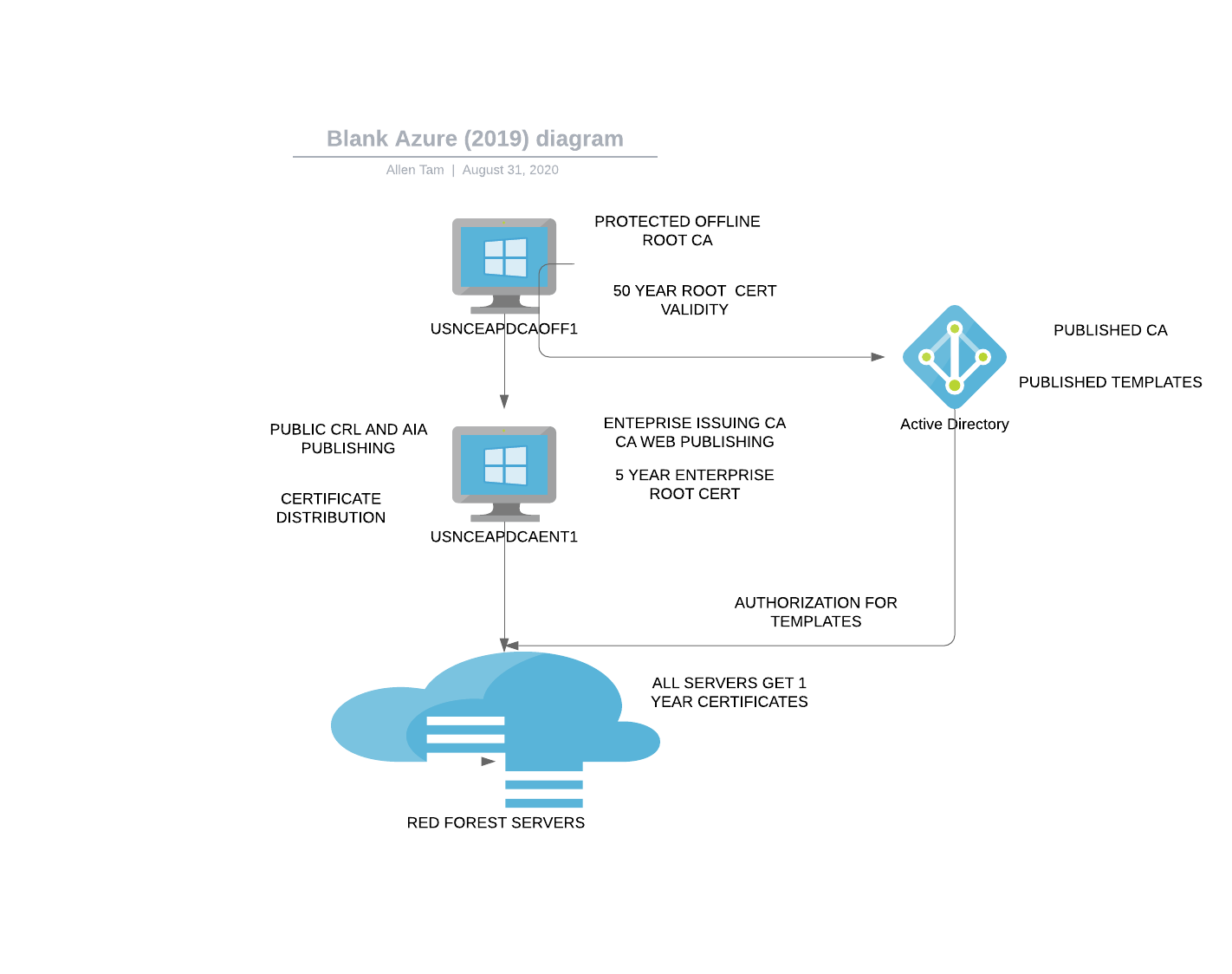
**Equifax Red Forest Enterprise PKI**

Equifax Red Forest Enterprise PKI is a two tier PKI Environment.

Below is a visual diagram:



1. Prep Work and Requirements
2. 2 servers 3 roles
3. off1 = rootca
4. ent1 = subca + web publishing
5. set dns cname for webcert to point to ent1
6. On mgmt make sure you have all remote admin tools
7. Install-WindowsFeature RSAT -includeallsubfeature
8. Install-WindowsFeature RSAT-Online-Responder

**B. Configuration Process (mostl Powershell commandline)**

**On Root CA server.**

1. Add-WindowsFeature ADCS-Cert-Authority -IncludeManagementTools
2. Run: Install-ADcsCertificationAuthority -CACommonName “ATLEAQTCAOFF1” -CAType StandaloneRootCA -HashAlgorithmName SHA512 -KeyLength 4096 -ValidityPeriod Years -ValidityPeriodUnits 40 -CryptoProviderName “RSA#Microsoft Software Key Storage Provider”
3. Clear Existing Distribution points
4. $CRLs = Get-CACrlDistributionPoint

foreach ($crl in $CRLs) {Remove-CACrlDistributionPoint $crl.uri -Force}

1. Add New Distribution point (webcert will be on the web role)

Add-CACrlDistributionPoint -Uri http://webcert/certenroll/%3%8.crl -AddToCertificateCdp –Force

4. Clear Existing AIA

1. $AIAS= Get-CAAuthorityInformationAccess

foreach ($aia in $AIAS) {Remove-CAAuthorityInformationAccess $aia.uri -Force}

1. Add AIA distribution point

Add-CAAuthorityInformationAccess -AddToCertificateAia -Uri <http://webcert/certenroll/%1_%3.crt>

5. Set publication locations

1. certutil.exe -setreg ca\DSConfigDN "CN=Configuration,DC=domaindomain,DC=com”
2. certutil.exe -setreg ca\DSDomainDN "DC=domaindomain,DC=com"
3. After root cert has been issued to c:\windows\system32\certsrv\certenroll\ Make sure it looks right Then configure the server as follows:

certutil.exe -setreg CA\CRLPeriodUnits 26

certutil.exe -setreg CA\CRLPeriod "Weeks"

certutil.exe -setreg CA\CRLDeltaPeriodUnits 0

certutil.exe -setreg CA\CRLDeltaPeriod "Days"

certutil.exe -setreg CA\CRLOverlapPeriodUnits 12

certutil.exe -setreg CA\CRLOverlapPeriod "Hours"

certutil.exe -setreg CA\ValidityPeriodUnits 5

certutil.exe -setreg CA\ValidityPeriod "Years"

certutil.exe -setreg CA\KeySize 4096

certutil.exe -setreg CA\AuditFilter 127

**ON ENT1**

1. Add-WindowsFeature ADCS-Web-Enrollment
2. Copy root certs to ENT1 from to c:

\\OFF1\C$\Windows\System32\CertSrv\CertEnroll\ATLEAQTCAOFF1.crl

\\OFF1\C$\Windows\System32\CertSrv\CertEnroll\ATLEAQTCAOFF1\_ATLEAQTCAOFF1.crt

**ON Ent1**

1. Publish Root CA

certutil.exe -dsPublish -f ATLEAQTCAOFF1\_ATLEAQTCOFF1(3).crt rootca

1. ADD ROOT CERT TO STORE

certutil.exe –addstore –f root ATLEAQTCOFF1(3).crl

certutil.exe –addstore –f root atleaqtcaoff1.crt

1. ADD CA Feature but dont configure yet

add-WindowsFeature ADCS-Cert-Authority

1. Get virtual directory ready

MKDIR c:\CERTS

$acl = get-acl c:\certs

$rule = new-object System.Security.AccessControl.FileSystemAccessRule(“domaindomain.com\Cert Publishers”,”Modify”,”ContainerInherit,ObjectInherit”,”None”,”Allow”)

$acl.addaccessrule($rule)

Set-ACL C:\windows\Temp $acl

$acl |Format-List

New-smbshare -name “certenroll” -path “C:\certs” -fullaccess “domaindomain.com\cert publishers”

**Install Web Server**

1. install-windowsfeature web-server -includemanagementtools

**Install WEb Management Feature**

1. install-windowsfeature web-mgmt-service -includemanagementtools

**Allow IIS Remote management**

1. netsh advfirewall firewall add rule name=”Allow Web Management” dir=in action=allow service=“WMSVC” remoteip=10.12.12.71
2. Set-ItemProperty -Path HKLM:\Software\Microsoft\WebManagement\Server -Name EnableRemoteManagement –Value 1
3. Set-Service wmsvc –StartupType “automatic”
4. Start-Service wmsvc
5. Shutdown /r /f /t 0

**ON MGMT2**

1. configure virtual directory

open IIS management connect to ent1

go to default site - right click -new virtual directory

1. Enable directory browsing

Under application pools select the proper one you’re using, go to advanced configuration, and select either system or network account

1. Create Virtual Alias

under alias enter certenroll and physical path c:\certs

1. Allow Anonymous to access files

select virtual directory and make sure anonymous authentication is set to enabled

set ssl to do not require

1. Set directory permisisons

Right click on the location of the directory in windows explorer and set permissions Grant permissions to which ever account you selected in the application pool to full permissions, as well as everyone to for read

**Install Subordinate**

1. Install-ADcsCertificationAuthority -CACommonName “subca1” -CAType EnterpriseSubordinateCA -CryptoProviderName “RSA#Microsoft Software Key Storage Provider” -HashAlgorithmName SHA512 -KeyLength 4096

You will be prompted to submit the cert req in c:\

**On OFF1**

copy request to off1

then submit request

certreq -submit "subca1.domaindomain.com\_subca1.req"

resubmit approve

certutil –resubmit "RequestID#"

get cert

certreq –retrieve 9 C:\subca1.domaindomain.com\_subca1.cer

**ON ENT1**

1. copy .cer to ent1
2. Install cert

certutil –installcert “C:\subca1.domaindomain.com\_subca1.cer”

**clear distribution points**

$CRLs = Get-CACrlDistributionPoint

foreach ($crl in $CRLs) {Remove-CACrlDistributionPoint $crl.uri -Force}

**ADD DISTRIBUTION POINT**

Add-CACrlDistributionPoint -Uri C:\Windows\System32\CertSrv\CertEnroll\%3%8%9.crl -PublishToServer -PublishDeltaToServer –Force

Add-CACrlDistributionPoint -Uri http://subca1/CertEnroll/%3%8%9.crl -AddToCertificateCDP –Force

Add-CACrlDistributionPoint -Uri file://\\WebCert\CertEnroll\%3%8%9.crl - PublishToServer -PublishDeltaToServer –Force

**REMOVE AIA**

$AIAS= Get-CAAuthorityInformationAccess

foreach ($aia in $AIAS) {Remove-CAAuthorityInformationAccess $aia.uri -Force}

**CONFIGURE AIA**

Add-CAAuthorityInformationAccess –AddToCertificateAia "ldap://CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11"

Add-CAAuthorityInformationAccess -Uri C:\certs\%3%4.crt –Force

Add-CAAuthorityInformationAccess -Uri http://WebCert/Enroll/%%3%4.crt –Force

**Configure CA settings**

netsh int ipv4 set dynamicport tcp start=54445 num=555

netsh int ipv4 set dynamicport udp start=54445 num=555

netsh int ipv6 set dynamicport tcp start=54445 num=555

netsh int ipv6 set dynamicport udp start=54445 num=555

certutil -setreg policy\EditFlags 0x00040044

certutil -setreg CA\DSConfigDN CN=Configuration,DC=domaindomain,DC=com

certutil -setreg CA\CRLPeriodUnits 2

certutil -setreg CA\CRLPeriod "Weeks"

certutil -setreg CA\CRLDeltaPeriodUnits 1

certutil -setreg CA\CRLDeltaPeriod "Weeks"

certutil -setreg CA\CRLOverlapPeriodUnits 12

certutil -setreg CA\CRLOverlapPeriod "Hours"

certutil -setreg CA\CRLDeltaOverlapPeriodUnits 12

certutil -setreg CA\CRLDeltaOverlapPeriod "Hours"

certutil -setreg CA\ValidityPeriodUnits 2

certutil -setreg CA\ValidityPeriod "Years"

certutil -setreg CA\AuditFilter 127

certutil -setreg CA\CRLFlags +CRLF\_REVCHECK\_IGNORE\_OFFLINE

certutil -setreg policy\EditFlags +EDITF\_ATTRIBUTESUBJECTALTNAME2

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ \EncryptionCSP" -Name Provider –Value "Microsoft Software Key Storage Provider"

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\domaindomain-subca1-CA\EncryptionCSP" -Name ProviderType –Value 0

certutil -setreg CA\EncryptionCSP\CNGEncryptionAlgorithm AES certutil -setreg CA\EncryptionCSP\SymmetricKeySize 512

shutdown /r /f /t 0

Done your cert authority should be working now