**Enterprise PKI configuration Guide**

**Prerequisites:**

Build 2 servers with the following configuration

Create Azure Storage and Create Azure file share

Open Scripts within Powershell ISE and run step several steps at a time and adjust for failures (file naming)

Scripts MUST be run Sequentially

**Server1**

Offline Root CA

Not Domain Joined

PSPKI powershell module

Mount x:\ to azure fileshare

Scripts:

1. Pkiconfig1.ps1

2. Pkiconfig3.ps1

3. PkiConfig5.ps1

**Server 2**

Subordinate Issuing + Web enrollment server

Domain Joined

PSPKI powershell module

Mount x:\ to azure file share

Scripts:

1. Pkiconfig2.ps1

2. Pkiconfig4.ps1

3. Pkiconfig6.ps1

**Manual Step 7**

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

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Eassfq-ATLEAQTCAENT1-CA\EncryptionCSP" -Name ProviderType ñValue 0

certutil -setreg CA\EncryptionCSP\CNGEncryptionAlgorithm AES

certutil -setreg CA\EncryptionCSP\SymmetricKeySize 512

Alternatively, search regedit from Windows explorer and under Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Eassfq-ATLEAQTCAENT1-CA\EncryptionCSP. Modify Provider, ProviderType, CNGEncryptionAlgorithm and SymmetricKeySize

**Manual Step 8**

Open Cert Authority

Go to templates

Right click select manage

Create and issue the Enterprise templates needed

**Manual Step 9**

Open mmc.exe

add Enterprise PKI or run pkiview from the run command

Check certificate health.