Install CA on workstations

Installation depends on the operating system of the workstation (or other device) you need the CA installed on. Note, this is only needed on workstations or machines which will be accessing the services. You do not need to install this on the servers which provide the service, though it is acceptable to do so.

For a few workstations, it is easier to do a manual install. For a more complex environment, it is better to spend some time writing scripts to do the installation for you.

Generally, the public key for a CA has a .crt suffix. However, some tools assume a .pem suffix. If your particular system does not undertand when you are trying to import CA.crt, simply rename it to CA.pem will work.

Microsoft Windows

Manual Install

This is the simplest for a small number of Windows computers. Put the Certificate (PEM file) on a thumb drive or a Windows File Share (SMB). On each machine:

1. Be sure you are an administrator
2. Locate Certificate
3. Double click on the certificate
4. Follow the prompts to install Certificate in the ROOT store

Automated Install

The simplest thing I can come up with is to create a share (SMB, whatever) that you can access from all machines, then place the CA Certificate (PEM file) in that share. A possible PowerShell script (untested so far) can be placed in that directory. Now, you can go to that directory on each machine and run the script. This script does not check if the CA was already there; it just replaces it if it exists.

The script requires administrator privileges.

installCA.ps1

```
# Ensure this script runs as an administrator
if (-Not ([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.
Principal.WindowsBuiltInRole]::Administrator)) {
    throw "Run this script as Administrator!"
}
```

```
# change this to the actual name of your Certificate
$PemFileName = "ca.pem"

# Define the path to the PEM file
$CurrentDir = Split-Path -Parent $MyInvocation.MyCommand.Path
$PemFilePath = Join-Path -Path $CurrentDir -ChildPath $PemFileName

# Check if PEM file exists
if (-Not (Test-Path $PemFilePath)) {
    throw "CA PEM file not found at path: $PemFilePath"
}

# Import CA from PEM file using certutil
Write-Host "Importing the Certificate Authority from PEM file..." -
ForegroundColor Cyan

certutil -addstore -f "ROOT" $PemFilePath

# Verify that the CA was imported successfully
$importedCA = Get-ChildItem Cert:\LocalMachine\Root | Where-Object {
$_.Subject -like "*CN=*" }
if ($importedCA) {
    Write-Host "Successfully imported CA from PEM file:" -
ForegroundColor Green
    $importedCA | Format-Table -Property Subject, Thumbprint
} else {
    Write-Host "Failed to import CA from PEM file." -ForegroundColor
Red
}
```

Using GPO in a Windows Domain

It is possible (untested) to run the above script from a GPO script to install the CA Certificate on many machines if they are connected to a Windows Domain. The following script is modified to work within a Windows Domain.

installCADomain.ps1

```
# Ensure this script runs as an administrator
if (-Not ([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.
Principal.WindowsBuiltInRole]::Administrator)) {
    throw "Run this script as Administrator!"
}

# change this to the actual name of your Certificate
$PemFileName = "ca.pem"
```

```
# Define the path to the PEM file
$CurrentDir = Split-Path -Parent $MyInvocation.MyCommand.Path
$PemFilePath = Join-Path -Path $CurrentDir -ChildPath $PemFileName

# Function to check if CA is already installed
function Check-CAInstalled {
    $caExists = Get-CertificateAuthority -ErrorAction SilentlyContinue
    if ($caExists) {
        Write-Host "A Certificate Authority is already installed:" -
ForegroundColor Yellow
        $caExists | Format-Table -Property CAName, CAType, CADuration
        return $true
    }
    return $false
}

# Check if a CA is already installed
if (Check-CAInstalled) {
    Write-Host "Exiting script as CA installation is not required." -
ForegroundColor Green
    exit
}

# Check if PEM file exists
if (-Not (Test-Path $PemFilePath)) {
    throw "CA PEM file not found at path: $PemFilePath"
}

# Install the AD Certificate Services role if it's not installed
Install-WindowsFeature -Name AD-Certificate -IncludeManagementTools

# Import the CA from PEM file using certutil
Write-Host "Importing the Certificate Authority from PEM file..." -
ForegroundColor Cyan

certutil -addstore -f "ROOT" $PemFilePath

# Verify that the CA was imported successfully
$importedCA = Get-ChildItem Cert:\LocalMachine\Root | Where-Object {
$_.Subject -like "*CN=*" }
if ($importedCA) {
    Write-Host "Successfully imported CA from PEM file:" -
ForegroundColor Green
    $importedCA | Format-Table -Property Subject, Thumbprint
} else {
    Write-Host "Failed to import CA from PEM file." -ForegroundColor
Red
}
```

Linux

Some web browsers <cough>Firefox</cough> maintain their own list of CA's on Linux, not reading the ones in the operating system. In these cases, you must manually add the new CA to the web browser.

Each type of Linux distribution can have a different way of importing a CA, but the procedure is basically the same.

1. Copy PEM to a specified directory
2. run a command to update the list of CA's

Debian derivatives

```
sudo cp ca.pem /usr/local/share/ca-certificates/
sudo update-ca-certificates
```

RedHat Based

```
cp pemfile /etc/pki/ca-trust/source/anchors/
update-ca-trust
```

Automated for Unix

The following script is suitable for use from a centralized server which has root access via ssh to multiple Unix machines. This is written for something like an Ansible server.

It will detect Debian and RedHat based Linux, and FreeBSD Unix.

It will

1. copy pem file to the /tmp directory on the target machine
2. Attempt to detect the operating system type
    1. If successful, copy pem to appropriate directory and run udpate command
    2. Otherwise, give an error message

Called as

```
./updateCALinux target /local/path/to/ca.pem
```

updateCALinux

```
#!/bin/bash
```

```
# Check if the required parameters are provided
if [ $# -ne 2 ]; then
    echo "Usage: $0 <target_machine> <path_to_ca_cert>"
    echo "Example: $0 target_machine /path/to/ca.pem"
    exit 1
fi

TARGET_MACHINE=$1
CA_CERT_PATH=$2

# Check if the CA certificate file exists locally
if [ ! -f "$CA_CERT_PATH" ]; then
    echo "CA certificate not found at $CA_CERT_PATH"
    exit 1
fi

# Copy the CA certificate to the target machine
echo "Copying CA certificate to $TARGET_MACHINE..."
scp "$CA_CERT_PATH" root@"$TARGET_MACHINE":/tmp/ca.pem

# Connect to the target machine and determine the OS
ssh root@"$TARGET_MACHINE" << 'EOF'
    # Detect the OS
    if [ -f /etc/debian_version ]; then
        echo "Detected Debian/Devuan system."
        # Install the CA certificate
        cp /tmp/ca.pem /usr/local/share/ca-certificates/
        update-ca-certificates

    elif [ -f /etc/redhat-release ]; then
        echo "Detected Red Hat/CentOS system."
        # Install the CA certificate
        cp /tmp/ca.pem /etc/pki/ca-trust/source/anchors/
        update-ca-trust

    elif [ "$(uname)" = "FreeBSD" ]; then
        echo "Detected FreeBSD system."
        # Install the CA certificate
        cp /tmp/ca.pem /usr/local/share/certs/ca.pem
        c_rehash /usr/local/share/certs/

    else
        echo "Unsupported OS. Exiting."
        exit 1
    fi

    echo "CA certificates updated successfully."
EOF

echo "CA certificate installation completed on $TARGET_MACHINE."
```

MacOS

MacOS is based on FreeBSD and could likely be detected by the generic script under the previous section, but I'll show manual here.

GUI

1. Open Finder, then navigate to Applications | Utilities | Keychain Access.
2. Open File | Import Items
3. Find your certificate and select Open
4. Choose which keychain to import it to
    1. System - Available to all users
    2. login - Available only to the current user
5. Locate the new Cert in the keychain and double click to open it
6. Expand the **Trust** section
7. Change *When using this certificate* to **Always Trust**
8. Close and save, answering yes to all questions

Command Line

To install rapidly, simply open Terminal (Finder | Applications | Utilities | Terminal) and issue the following command. You'll need to make sure you know where the PEM file is.

```
sudo security add-trust-anchor -d -r trustAsRoot -k
/Library/Keychains/System.keychain /path/to/ca.pem
```

Create Server Certificates

Once you have the CA's installed on your workstations, you are ready to Create some Server (service) certificates signed by the CA. These certificates will be authorized without a problem because your CA was installed on these machines.