

# Generating a certificate

To request a certificate from a Certificate Authority (CA), you will need to give them a Certificate Signing Request (CSR).

For instructions on how to generate a certificate please see

[https://docs.google.com/document/d/1FPXAE7U2yOGPUuQwE56ZwGEYkMEDTyf\\_8fqzdvrNwMw](https://docs.google.com/document/d/1FPXAE7U2yOGPUuQwE56ZwGEYkMEDTyf_8fqzdvrNwMw)

Located at

LAVA Drive > Information, Guides, and How To > Certificate Generation

## Install

SAGE2 doesn't use the built in Windows hosting services, it uses Nodejs.

Nodejs handles certificates itself using the **sage\_install\_folder/keys** folder.

Someone might normally double click on a **.crt** or **.key** file to install into the default Windows service, this does not work for SAGE2.

Within the keys folder, each hostname/IP address will come in sets of three.

Two **.crt** and one **.key**.

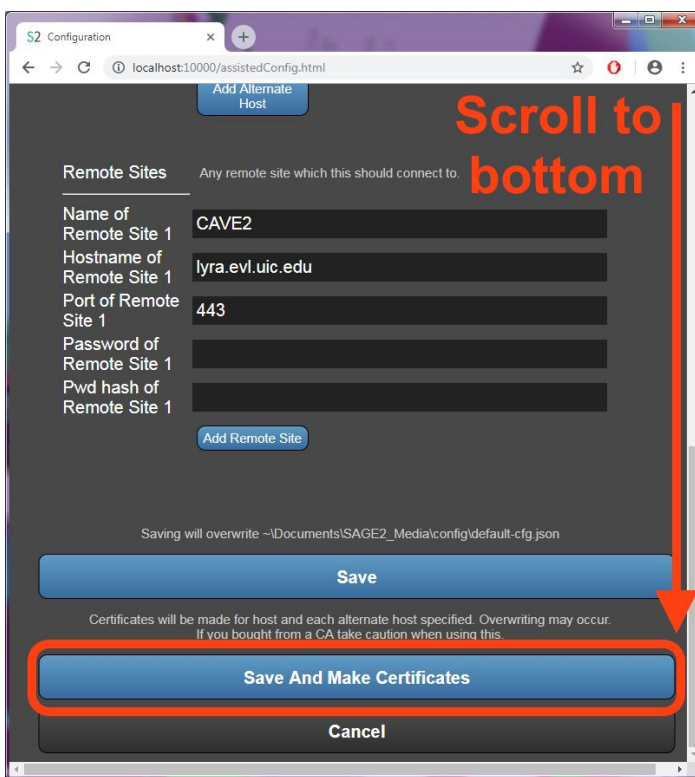
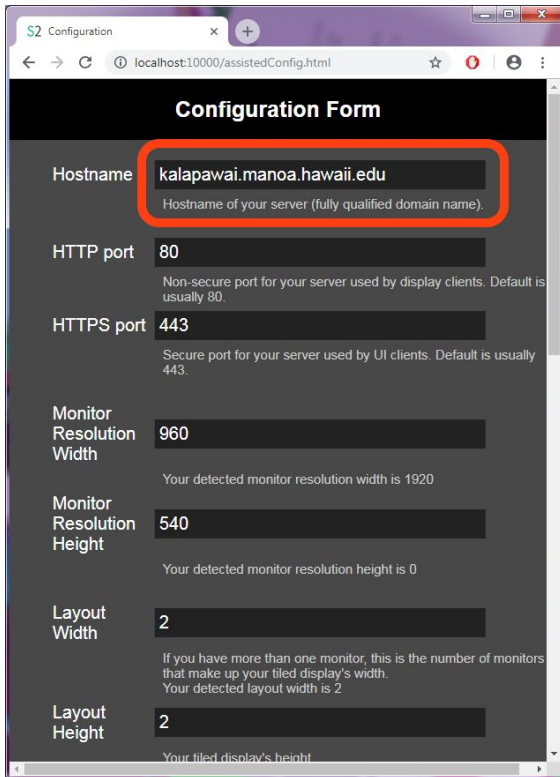
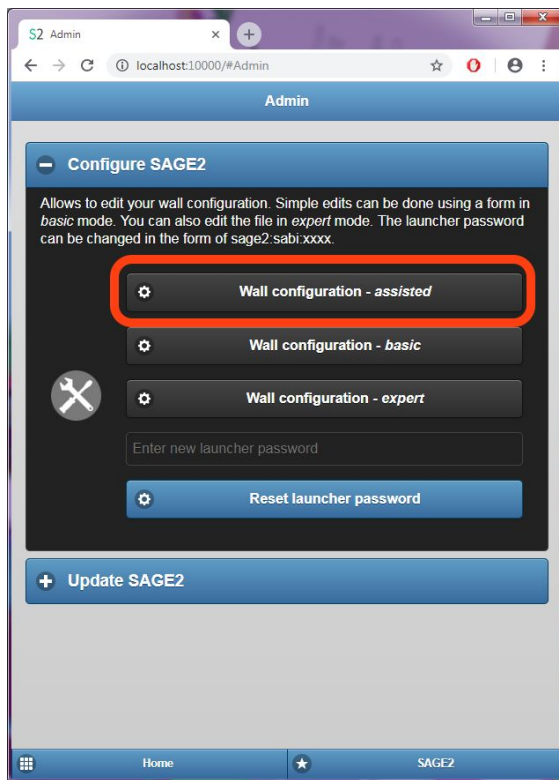
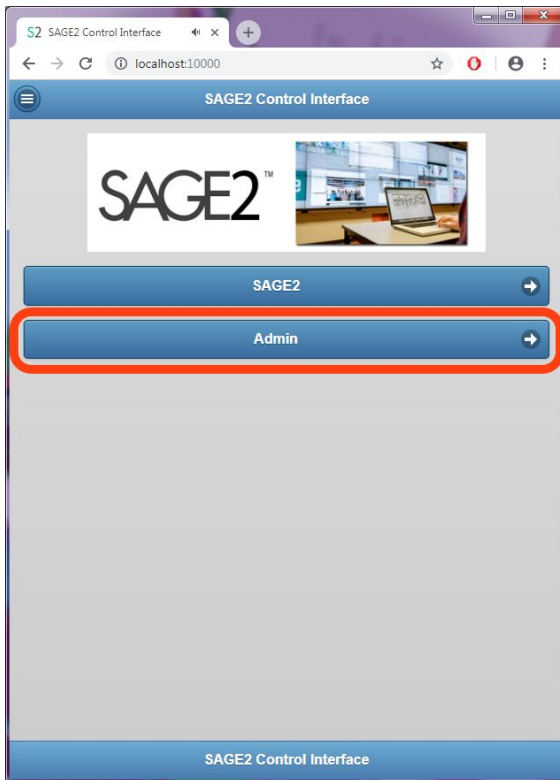
By default, Windows binaries come with localhost and 127.0.0.1 files:

127.0.0.1-ca.crt  
127.0.0.1-server.crt  
127.0.0.1-server.key  
localhost-ca.crt  
localhost-server.crt  
localhost-server.key

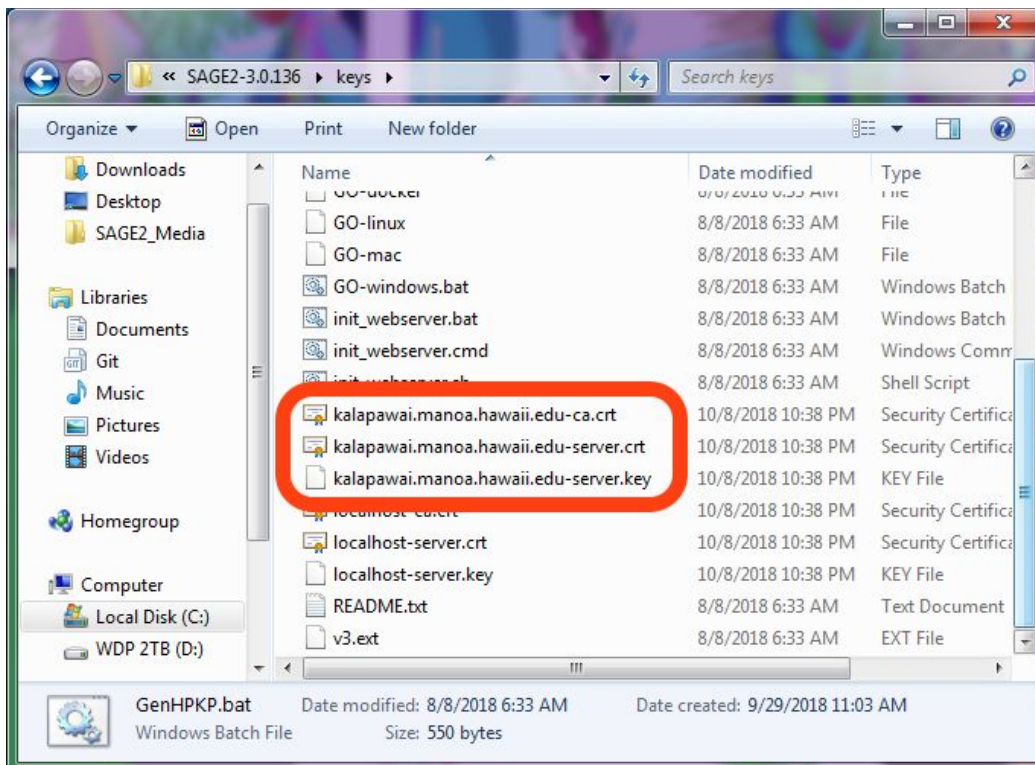
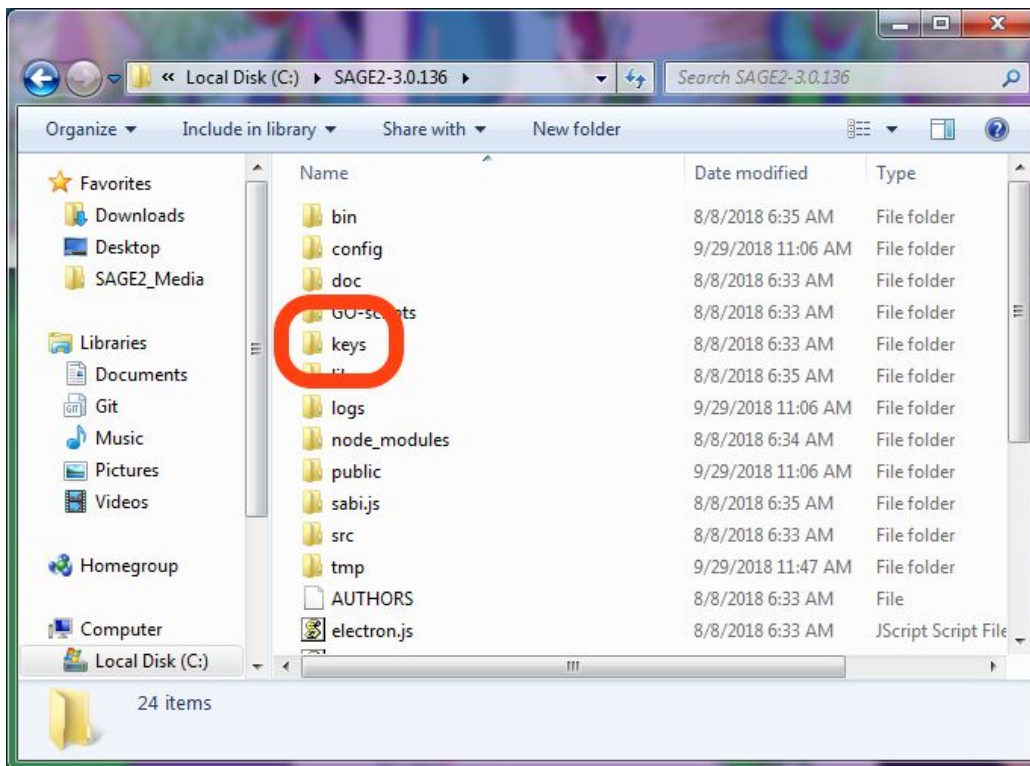
The naming scheme must match and all three files are needed. However, CA wil only provide the server **.crt** file. The **.key** is generated when the CSR file is made. It is easier to let SAGE2 create the third file.

It is first recommended to let SAGE2 generate the three necessary files, if you have already been using certificates for the hostname and are updating them, the following steps may be skipped.

- Open the control panel, **http://<hostname>:1000/**
- Click on **Admin**
- Click on **Wall configuration - assisted**
- Set the **Hostname**
- **Save And Make Certificates**, at the bottom of the page

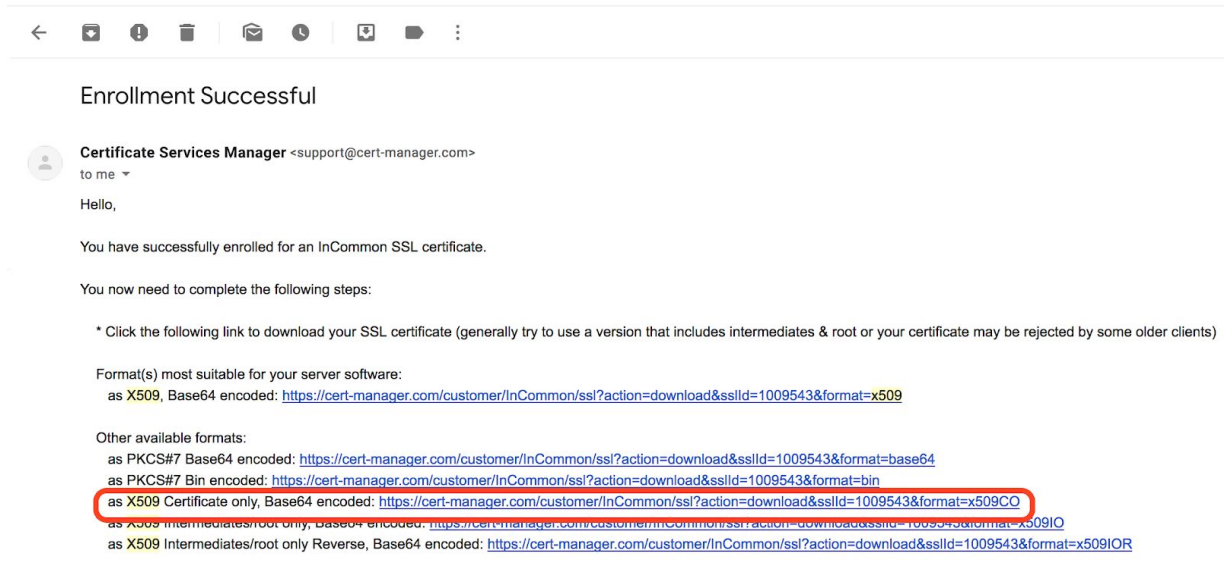


The above steps will generate the three file set, where they will be located in the keys folder.

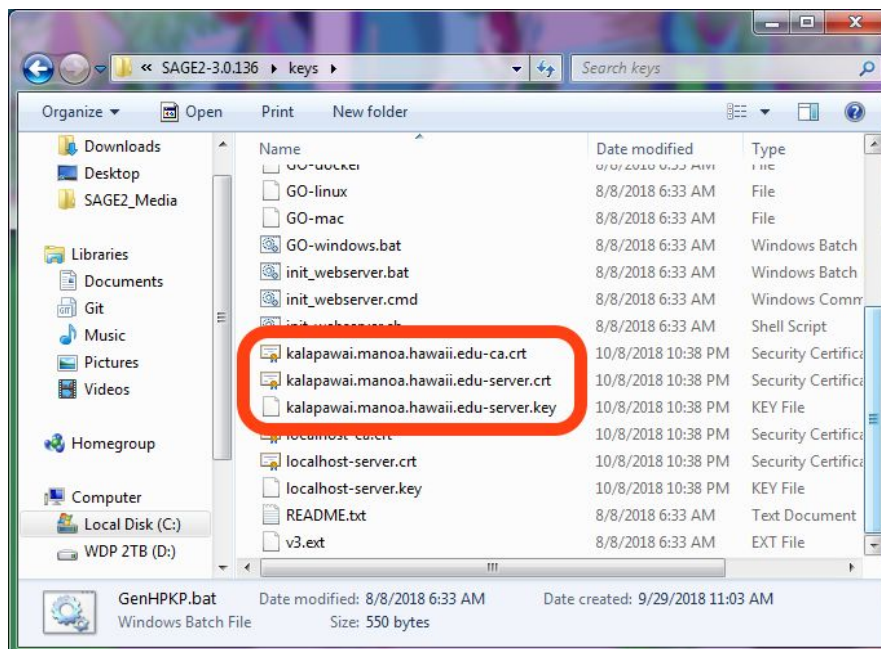


Now the certificate and key will need to be moved to the keys folder

- After submitting a CSR to a CA, they usually respond back with a download link to a variety of options for the certificate.
- Use the link and download the **X509 Certificate only, Base64 encoded**
  - If that that option is not available, get the **X509, Base64** file. It will need to be trimmed to work correctly through trial and error. More on this later.



- Edit the downloaded file's name to match the **<hostname>-server.crt** file
- Then get the **.key** file that was generated when the CSR was generated and make its file name match the **<hostname>-server.key** file.
- Make duplicates of the **.key** and **.crt** file you just renamed.
  - Sometimes the CA will put a time limit to how long the **.crt** file download is available.
  - If the **.key** file is lost, it cannot be recovered and the **.crt** file becomes unusable.
  - Should the **.key** file be lost, usually CA will allow regeneration. Some will charge a fee for regeneration.
- Replace the old files with the ones you just name edited. The names should match the formatting of those generated using the control panel





- Restart SAGE2
- Test to see if it was installed
  - Connect to the SAGE2 interface using the certificate hostname
  - After the page loads, look at the address bar
  - To the left of the URL should be a lock icon
  - Click on the lock icon
    - If the information popup says “Secure Connection” then it has been installed correctly.
    - If there is no lock icon, it was not installed correctly

## If the **X509 Certificate only**, Base64 encoded file is unavailable

You may have to manually reduce the **X509, Base64** file.

This can be a guess and check process

For example this image shows that the contents of the X509, Base64

It contains four separate certificates for different usage cases.

However only one will work correctly

```

1  |-----BEGIN CERTIFICATE-----
2  |MIIEAjCCAx6gAwIBAgIBATANBgkqhkiG9w0BAQUFADBVMQswCQYDVQGEwJTRTEU
3  |MB4XDTAwMDUzMDUwNDgzOFoXDTIwMDUzMDUwNDgzOFowbzELMAkGA1UEBhMCU0Ux
4  |IFRUUCB0ZXR3b3JrMSIwIAYDVQDEExLBZGRUcnVzdCBFeHRlcm5hbnB0QSB0290
5  |MB4XDTAwMDUzMDUwNDgzOFoXDTIwMDUzMDUwNDgzOFowbzELMAkGA1UEBhMCU0Ux
6  |FDASBgNVBAoTC0FkZFRydXN0IEFCSYwJAYDVQQLEx1BZGRUcnVzdCBFeHRlcm5h
7  |bCBUVFAgTmV0d29yazEiMCAGA1UEAxMZQWRkVHJ1c3QgRXh0ZXJ1YmVwQ0EgUm9v
8  |dDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALf3GjPm8gAELTngTLvt
9  |H7xsD821+i02zt6bET0XpLmfZ0fvUq8k+0DGu0Pz+VtUFRwLymUWoCwSXrbLpX9
10 |uMq/NzgtHj6RQa1wVsfwTz/oMp50ysiQV0nGXw94nZpAPA6sYapeFI+eh6FqUNzX
11 |mk6vBb0mcZScbNQYArHE504B4YCq0moaSYykKtMsE8jqzpPhNj fzp/haW+710LX
12 |a0Tx63ubUffclpxCDezeWkWaCUN/cALw3CknLa0Dhy2xSoRcRdKn23tNbE7qzN
13 |E0S3ySvdQwAl+mG5aWpYIxG3pz0PVnVZ9c0p10a3CitlttNCbxWyuHv77+ldU9U0
14 |WicCAwEAAa0B3DCB2TAdBgNVHQ4EFgQUrb2YejS0Jvf6xCZU7w094CTLVBowCwYD
15 |VR0PBAQDAGEGMA8GA1UdEwEB/wQFMAMBAf8wgZkGA1UdIwSBkTCBjoAURb2YejS0
16 |Jvf6xCZU7w094CTLVBqhc6R8xMG8xCzAJBgNVBAYTA1NFMRQwEgYDVQKEwtBZGRU
17 |cnVzdCB0QjEmMCQGA1UECXMdQWRkVHJ1c3QgRXh0ZXJ1YmVwVFRQIE5ldHdvcm5x
18 |IjAgBgNVBAMTGUFkZFRydXN0IEV4dGVybmFsIENBIFJvb3SCAQEwDQYJKoZIhvcN
19 |AQEFBQADggEBALCb4IUlwtYj4g+WBpKdQZic2YR5gdkeWxQHIzZlj7DYd7usQWxH
20 |YINRsPkyPef89iYTx4AWpb9a/I fPeHmJIZriTAcKhjW88t5RxnKwt9x+Tu5w/Rw5
21 |6wwCURQtjr0W4MHfRnXnJK3s9EK0hZNwEGe6nQY1ShjTK3rMUUKhemPR5ruhXSVc
22 |Nr4TDea9Y355e6cJDUCrat2PisP29owaQgVR1EX1n6diIWgVIEM8med8vSTYqZEX
23 |c4g/Vhsx0Bi0cQ+azcg0no4uG+GMmIPLHzHxREzGBHNJdmAPx/i9F4BrLunMTA5a
24 |mnkPIAou1Z5jJh5VkpTYghdae9C8x490hgQ=
25  |-----END CERTIFICATE-----
26  |-----BEGIN CERTIFICATE-----
27  |MIIEFdzCCBF+gAwIBAgIQE+oocFv0700MNMmJgGFDNjANBgkqhkiG9w0BAQUFADBv
28  |MQswCQYDVQGEwJTRTEUwJTEUwJTEUwJTEUwJTEUwJTEUwJTEUwJTEUwJTEUwJTEU
29  |ZFRydXN0IEV4dGVybmFsIFRUUCB0ZXR3b3JrMSIwIAYDVQDEExLBZGRUcnVzdCBF
30  |eHRlcm5hbnB0QSB0290MB4XDTAwMDUzMDUwNDgzOFoXDTIwMDUzMDUwNDgzOFow
31  |gYgxCzAJBgNVBAYTA1NFMRQwEgYDVQKEwDQYJKoZIhvcNAQEFBQADggEwDQYJKo
32  |ZXJzZXkgQ2l0eEteEwBGA1UEChMVVGVhZGVzZXJ1YmVwVFRQIE5ldHdvcm5x
33  |

```

Make a copy of the file and try test each of the certificate section one at a time.

---BEGIN CERTIFICATE---

<hash>

---END CERTIFICATE---

It will not work correctly if all of them are in the file at the same time.

The contents should only contain one cert section, just like the localhost file

```
localhost-server.crt x
1  -----BEGIN  CERTIFICATE-----
2  MIIDCzCCAf0gAwIBAgIJAPcRar8RZN0dMA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNV
3  BAMTCWxvY2FsaG9zdDAeFw0xODA4MDgwNjMzMDFaFw0xOTA4MDgwNjMzMDFaMBQx
4  EjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
5  ggEBAMd+C49VU3DGHlmKReD6tNhkd13EqsTs6QmfZRYMEGiFUNT6C60ZEWq02tsN
6  yRee2tmgZXmnTnmri3w+xmQ9Zo/YG1Bl6v5XJL8tCV7WQcKS0yDSZ+yTgxAbjfib
7  wjExYyDUqUrLSMx0v9ox5H3JLL0HPbhghyKv7KXDf1MA3YlWQRWmGUbH/SfRRBVU
8  QZxJUmdZ1hxojmCPYIGL0GBJ/zXbXNKwkgsw/gueo0h5aEQP2ZKZS0XH8aleCP7
9  HJl05ZhA+vzIVIj54p0Kfx9f5FGIdCNWcx/eoHi0YeqyJVenpsJB7W4tBvU8Q6Q6
10 my6aNJC66HmjKSQm26q7VjeZmAUCAwEAANgMF4wLgYDVR0jBCcwJaEYpBYwFDES
11 MBAGA1UEAxMJBG9jYWxob3N0ggkA9xFqvxFk050wCQYDVR0TBAlwADALBgNVHQ8E
12 BAMCBPAwFAYDVR0RBA0wC4IJBG9jYWxob3N0MA0GCSqGSIb3DQEBCwUAA4IBAQDC
13 T3GrrZ/fVdvDl10CiJdoIeCib2t2nJqwfFvn0w+GlConrYfv087CWUSd+FaqGRL+
14 j2YCy3Afp3iQHMH5hezrZZ3J9TCvKJe/B1fnDu1vfJUzC1rJBZw3cfQbUwoi8zy
15 vuyeVTuS6KiFvqT/N6UnIkY4dwaRvPd1KE1emE9tTeXdcfUNMZqCzjTAW+oocQrk
16 pxHQdgu1SYq1BNbJq8A1U+z2HZGgl4Ngvygkj8ppkQDj//REDFzdyctcP8gSN1NU
17 FbetWpARwjybfFUon0UudjFwY2u/EqDts/JR0181AB74270IEXnmo5XJHJRA9vn
18 wPaWoEnQnbLH00/9UMYu
19  -----END  CERTIFICATE-----
20
```