Unleashed

Self-Signed, Root CA and Intermediate CA Certificates

★★★★★

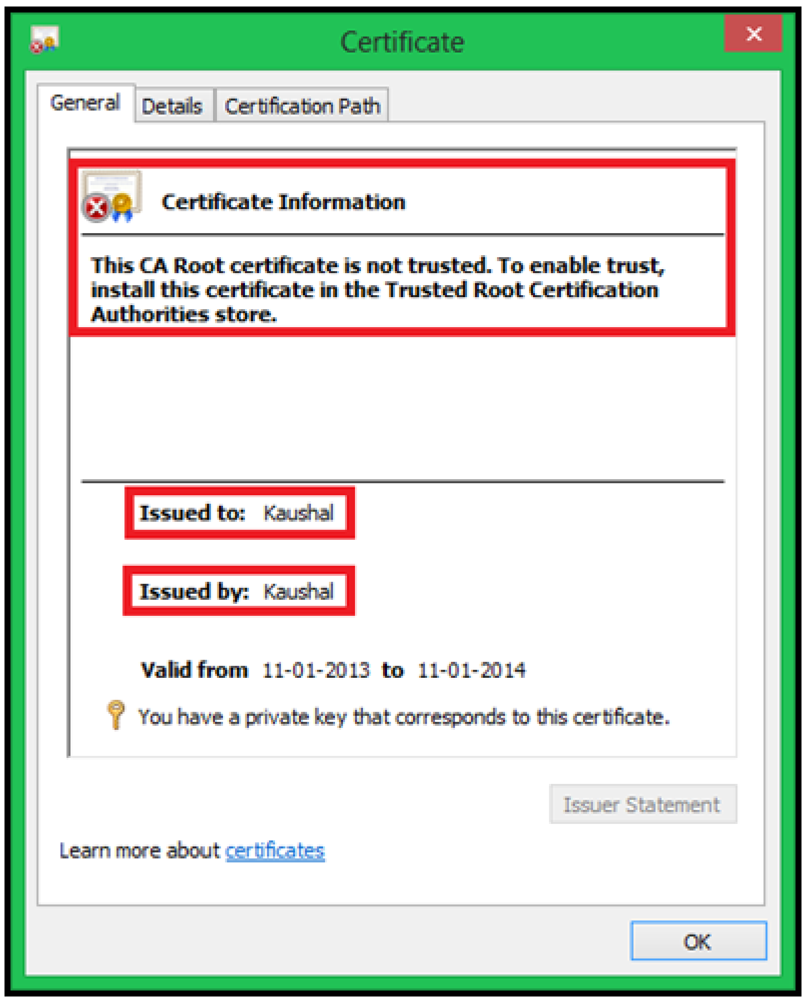
In this article I will be discussing about the following:

- Self-Signed Certificate
- Root CA Certificate
- Intermediate CA Certificate

At the end I would like everyone to be able to differentiate between these certificate types.

Self Signed Certificate

Self Signed Certificates are certs where both the **Issued To** and the **Issued By** field of the certificates are same. In simple words it is a certificate where one issues a certificate to itself and hence the name **Self Signed Certificate**. Here is one example:



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Kaushal

Issued by: Kaushal

Valid from 11-01-2013 **to** 11-01-2014

You have a private key that corresponds to this certificate.

As seen in the above image the **Issued to** and **Issued by** are same. You may also observe the warning indicating that the certificate is not trusted. Of course it is not as it is self-signed, none of the Known Public CA's have issued this, so it wont be trusted.

NOTE: To get past the above error put the cert in the Root CA store.

These certs come in handy as they can be created easily using several tools. Obtaining a certificate from a noted Certification Authority has a cost associated wi may not be feasible at all times. Developers typically test their applications using a self signed certificates most of the times.

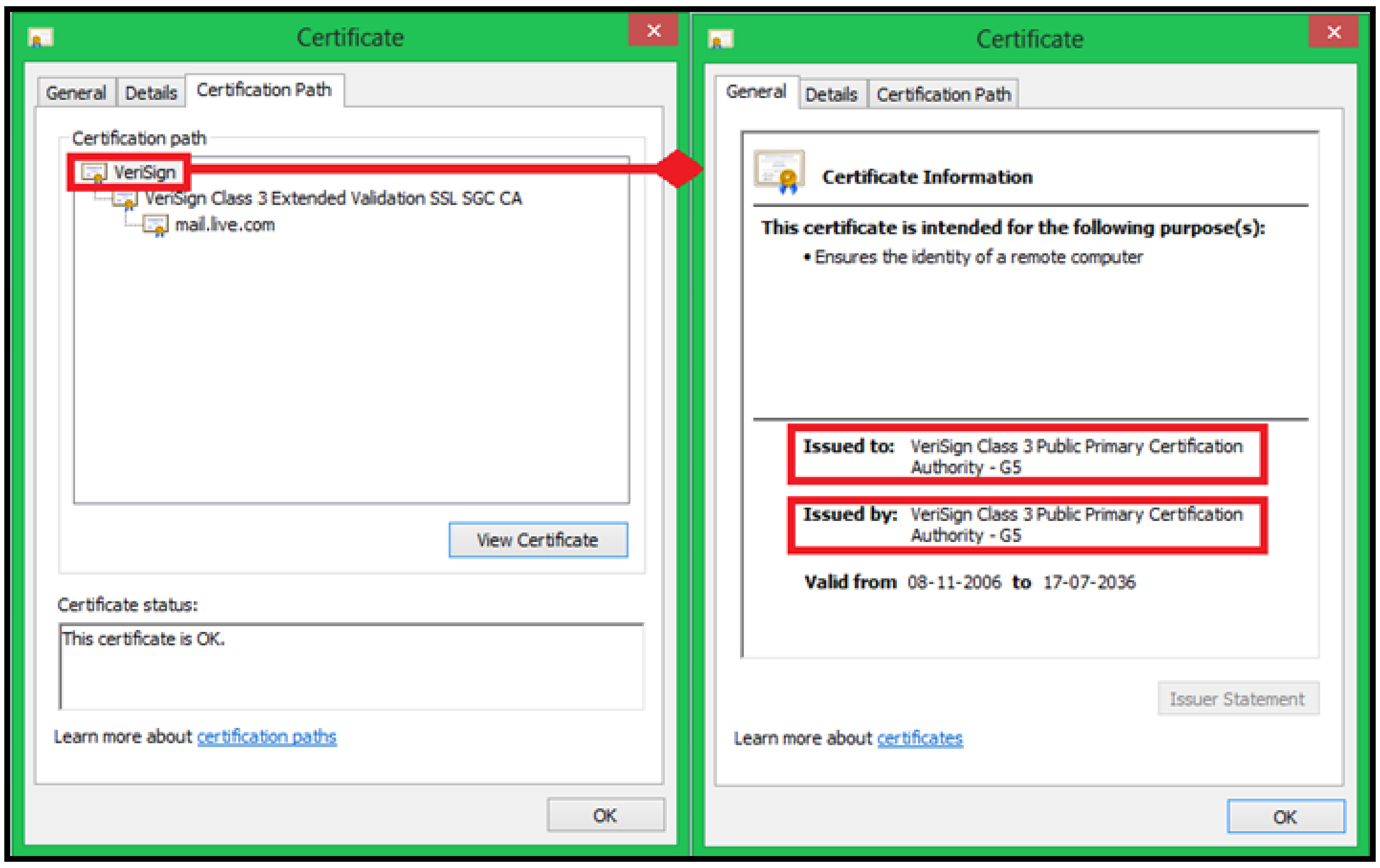
Root CA Certificate

Root CA Certificate is a **CA** Certificate which is simply a **Self-signed Certificate**. This certificate represents a entity which issues certificate and is known as **Certificate Authority** or the **CA**. The usage of the certificate distinguishes it with other normal certificates. Now a CA can be classified as either **Root CA's** or **Intermediate CA's**. On a **Windows OS**, if you are looking at the certificate store, you would see all the Root CA certificates in the **Trusted Root Certification Authorities**. This by default includes the list of public root CA's which are installed with Windows and are updated periodically through Windows Updates. The number of the certificates would be lesser.

NOTE: Don't add Intermediate CA certificates to the Trusted Root Certification Authorities store.

Identification of a Root CA:

Now how do we differentiate the CA certificates as **Root CA** or **Intermediate CA**. There is so much fuss around this. Its actually easy, look at the CA cert. If the **Issued to** and **Issued by** are same then it is a **Root CA** or else it is a **Intermediate CA**. Another identification would be to look at the **Certification Path**. The Cert which appears at the top of the list is the **Root CA**. Below is one example of one of the public root CA's:



Certification path

- VeriSign
  - VeriSign Class 3 Extended Validation SSL SGC CA
    - mail.live.com

Certificate status:

This certificate is OK.

Learn more about certification paths

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: VeriSign Class 3 Public Primary Certification Authority - G5

Issued by: VeriSign Class 3 Public Primary Certification Authority - G5

Valid from 08-11-2006 to 17-07-2036

Learn more about certificates

If you think logically this makes sense. CA's are supposed to issue certificates. Now if I start the process from the beginning, then someone has to issue a certificate to himself and then start the process of issuing the certs down the line.

I'm not going to discuss the purpose of the CA certificate as that would lead to a whole new discussion altogether.

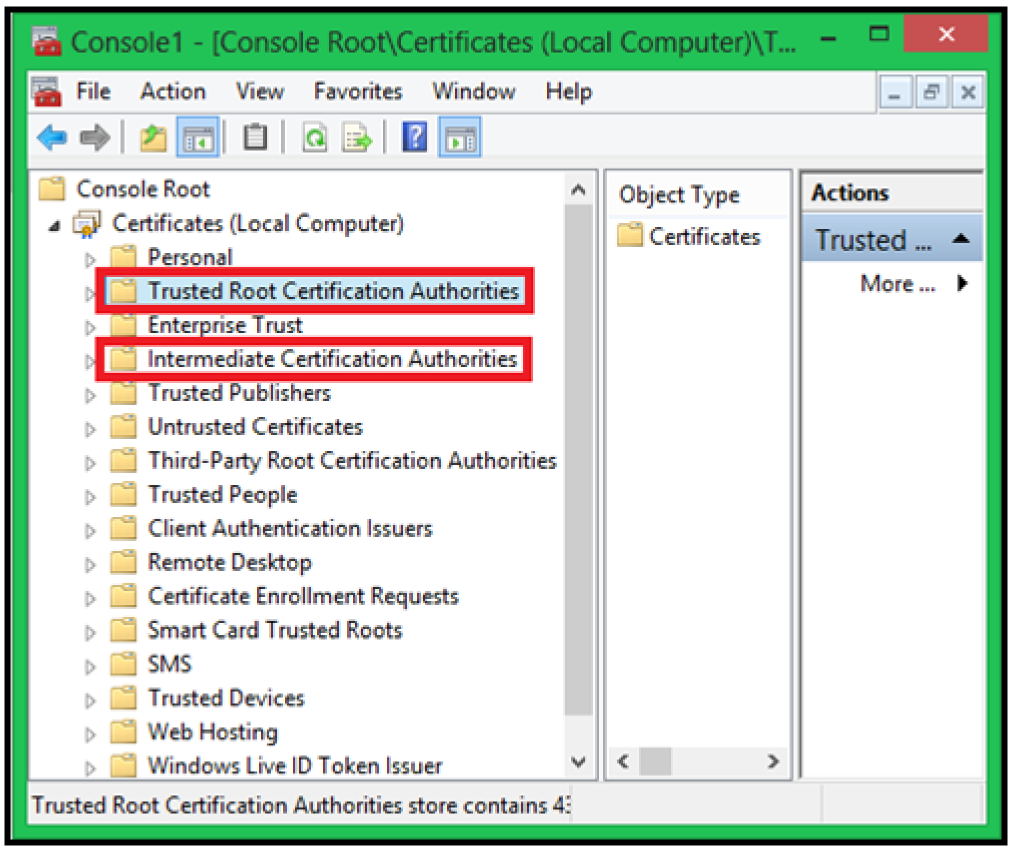
Intermediate CA Certificate

Intermediate CA Certificate is a CA certificate which is not a **Self-signed Certificate**. The purpose of this certificate may be same as the Root CA or different. Now one may think why to have a intermediate CA at all. Well here is what I think:

Initially it may not require to have a Intermediate CA, as the Root CA's will serve the purpose. However as the requirement for PKI increases so would the number of CA's. Understanding that CA at the end of the day is a Server Machine performing this computational task, it is required to have multiple machines. So they have to be replicated. Now it is again not viable to have many Root CA's in the case of a Internet Scenario as this could lead to fraud and other management issues. So the concept of Intermediate CA was introduced. The Root CA's delegated their tasks to the corresponding Intermediate CA's for this. This way they can have one or more Intermediate CA's.

On **Windows OS**, these certificates can be found in the **Intermediate Certification Authorities** Store. Comparatively the number of certificates in this store would be more compared to **Trusted Root Certification Authorities** store.

Below is a image of a certificate store of **MY** or **Local Computer** account. It contains many certificate stores, but I have only highlighted the ones relevant to this article.


Console1 - [Console Root\Certificates (Local Computer)\T...
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
SMS
Trusted Devices
Web Hosting
Windows Live ID Token Issuer
Object Type
Certificates
Actions
Trusted ...
More ...

Trusted Root Certification Authorities store contains 4:

Hope this article will clear some confusion at least.

Until then CIAO 😊