CA Certificates for Commercial Email Services

April 2014

Contents

Abstract..........2

Notable CA Certificates..........2

Certificates and Certificate Authorities (CA)..........2

Obtaining CA Certificates..........4

Obtaining CA Certificates for other services using SSSL-Tools (https://ssl-tools.net)..........4

Appendix 1: Installing a CA certificate into a LaserJet with Jetdirect networking..........7

Appendix 2: Certificate Validation..........9

Appendix 3: Certificate Chaining..........12

Abstract

Digital Sending features that use eMail servers should use an SSL-encrypted connection. When working with commercially provided services such as Gmail, Office365, Yahoo, or even with Enterprise services, SSL should be properly configured with the correct Certificate Authority (CA) certificates. This bulletin gives guidance on obtaining the proper CA certificate.

Notable CA Certificates

Certificates for the following commercial services can be downloaded from the links below:

- Gmail (April 2014): https://www.geotrust.com/resources/root_certificates/certificates/Equifax_Secure_Certificate_Authority.pem
- Yahoo (April 2014): https://www.digicert.com/CACerts/DigiCertAssuredIDRootCA.crt
- Office365 (April 2014): http://secure.globalsign.net/cacert/Root-R1.crt

Certificates and Certificate Authorities (CA)

The identity and authenticity of servers across a network is established by the use of *identity certificates* issued by *certificate authorities (CAs).* A certificate authority, after independently verifying information about a server, assembles and cryptographically *signs* that information to create an identity certificate. A client later examining the server's identity certificate can validate it by reversing the cryptographic signature. The cryptographic key necessary to reverse the signature is found in the *CA Certificate* that is distributed by the CA. The CA Certificate, rather than being used to prove the identity of the CA, is used to prove that the certificate was issued by the CA.

As an example, here is how a certificate comes into existence and is used:

A) A Certificate Authority, e.g. Verisign, issues a certificate to a server, e.g. www. Amazon.com.
B) A client receives a certificate from www.Amazon.com.
C) The client uses the CA Certificate from Verisign to prove that Verisign did in fact sign the certificate received from www.Amazon.com.

An Identity Certificate is thus tightly bound to the CA Certificate – only the CA Certificate can validate the Identity Certificate.

For most users, CA Certificates are invisible since they are pre-installed into browsers and operating systems. In contrast, specialized printers such as HP Multifunction Printers (MFPs) do not have certificates preloaded and the proper CA certificates must be installed before such printers can correctly validate a server.

Obtaining CA Certificates

There are a number of ways to obtain the correct CA Certificate.

1) Request the CA Certificate from the administrator of the server.
2) After identifying the Certificate Authority, request the certificate directly from the Certificate Authority.
3) After identifying the Certificate Authority, search for the CA Certificate in the certificate repository of a trusted operating system or browser.
4) Use an online tool such as **https://ssl-tools.net** .
   For more information, see Obtaining CA Certificates for other services using SSSL-Tools

For information about CA Certificates for a number of popular email providers, see Notable CA Certificates.

Obtaining CA Certificates for other services using SSSL-Tools (https://ssl-tools.net)

The https://ssl-tools.net/mailservers site can be used to query any publicly accessible mail server for its certificate chain and download the appropriate CA certificate. This tool only checks for servers using the STARTTLS method; if the mail service uses SMTPS, this tool will not be able to query the service.

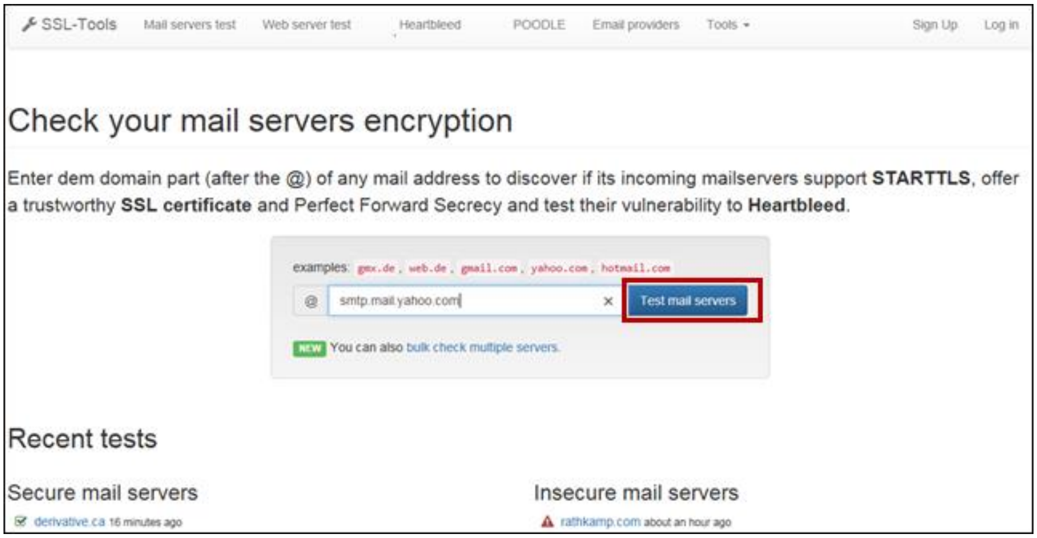
> *Disclaimer: https://ssl-tools.net is owned and operated by a private enterprise. The use of services and information from this site is entirely at the user's risk. Hewlett Packard does not endorse this site nor warrant the accuracy or suitability of any information derived from the use of this site. At the writing of this document (May 2014), the information obtained from https://ssl-tools.net is accurate for the email services that were checked. No statement can be made about any other email services.*

Follow these steps to obtain the CA Certificates:

1) Go to https://ssl-tools.net/ , and then click **Test mail servers**.
2) In the **Check your mail servers encryption** page, type the hostname of the mail server in the text box (smtp.mail.yahoo.com, for example), and then click Test mail servers.

   Note: This hostname should be the same hostname that is used to configure the Scan to Email feature of an MFP.

Figure 1: Check your mail servers encryption



Check your mail servers encryption

Enter dem domain part (after the @) of any mail address to discover if its incoming mailservers support **STARTTLS**, offer a trustworthy **SSL certificate** and Perfect Forward Secrecy and test their vulnerability to **Heartbleed**.

examples: gmx.de, web.de, gmail.com, yahoo.com, hotmail.com

@ smtp.mail.yahoo.com ×

NEW You can also bulk check multiple servers.

Recent tests

Secure mail servers

☑ derivative.ca 16 minutes ago

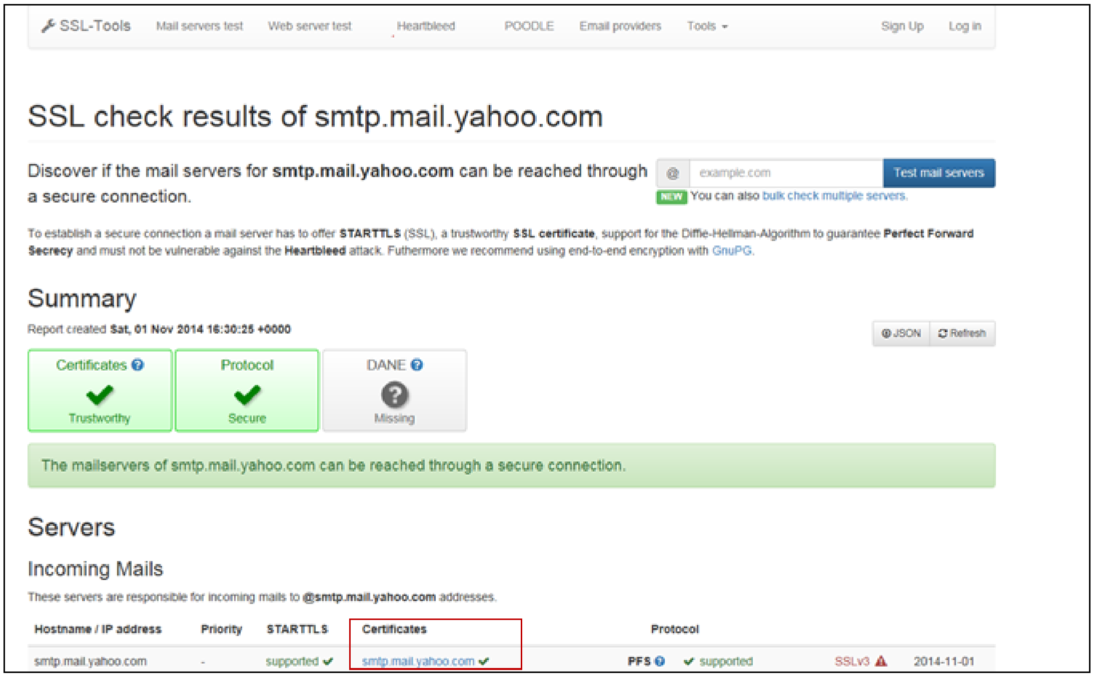
Insecure mail servers

⚠ rathkamp.com about an hour ago

3) In the **SSL check results** page, click the certificate for the server.

Note: Make sure to select the correct certificate for the server as one or more servers will be displayed, along with their CA certificates.

Figure 2: SSL check results



SSL check results of smtp.mail.yahoo.com

Discover if the mail servers for **smtp.mail.yahoo.com** can be reached through a secure connection.

@ example.com

NEW You can also bulk check multiple servers.

To establish a secure connection a mail server has to offer **STARTTLS** (SSL), a trustworthy **SSL certificate**, support for the Diffie-Hellman-Algorithm to guarantee **Perfect Forward Secrecy** and must not be vulnerable against the **Heartbleed** attack. Futhermore we recommend using end-to-end encryption with GnuPG.

Summary

Report created **Sat, 01 Nov 2014 16:30:25 +0000**

Certificates	Protocol	DANE
✓ Trustworthy	✓ Secure	? Missing

The mailservers of smtp.mail.yahoo.com can be reached through a secure connection.

Servers

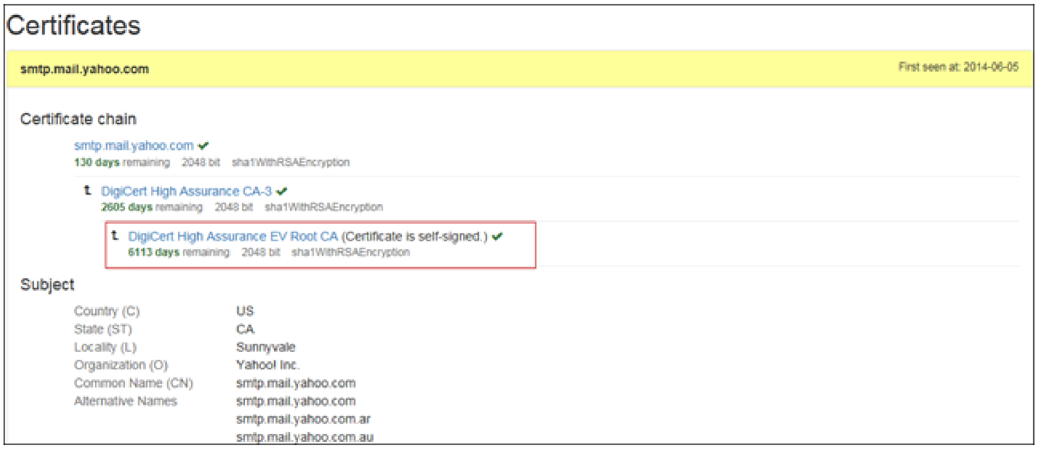
Incoming Mails

These servers are responsible for incoming mails to **@smtp.mail.yahoo.com** addresses.

Hostname / IP address	Priority	STARTTLS	Certificates	Protocol			
smtp.mail.yahoo.com	-	supported ✓	smtp.mail.yahoo.com ✓	PFS ?	✓ supported	SSLv3 ⚠	2014-11-01

4) In the Certificates details page, click on the Root CA certificate or self-signed certificate (Certificate is self-signed), the last certificate in the Certificate chain.

Figure 3: Certificate chain



Certificates

smtp.mail.yahoo.com First seen at: 2014-06-05

Certificate chain

smtp.mail.yahoo.com ✓
130 days remaining 2048 bit sha1WithRSAEncryption

↳ DigiCert High Assurance CA-3 ✓
2605 days remaining 2048 bit sha1WithRSAEncryption

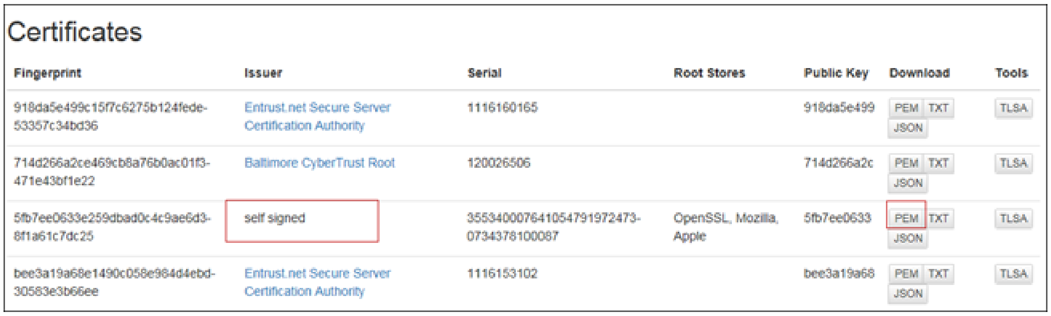
↳ DigiCert High Assurance EV Root CA (Certificate is self-signed.) ✓
6113 days remaining 2048 bit sha1WithRSAEncryption

Subject

Country (C)	US
State (ST)	CA
Locality (L)	Sunnyvale
Organization (O)	Yahoo! Inc.
Common Name (CN)	smtp.mail.yahoo.com
Alternative Names	smtp.mail.yahoo.com smtp.mail.yahoo.com.ar smtp.mail.yahoo.com.au

5) On the **DigiCert High Assurance EV Root CA** page, select the self-signed certificate and download the PEM format.
The PEM format is the certificate required to validate the SMTP server.

Figure 4: Certificates



Certificates

Fingerprint	Issuer	Serial	Root Stores	Public Key	Download	Tools
918da5e499c15f7c6275b124fede-53357c34bd36	Entrust.net Secure Server Certification Authority	1116160165		918da5e499	PEM TXT JSON	TLSA
714d266a2ce469cb8a76b0ac01f3-471e43bf1e22	Baltimore CyberTrust Root	120026506		714d266a2c	PEM TXT JSON	TLSA
5fb7ee0633e259dbad0c4c9ae6d3-8f1a61c7dc25	self signed	35534000764105479197 2473-0734378100087	OpenSSL, Mozilla, Apple	5fb7ee0633	PEM TXT JSON	TLSA
bee3a19a68e1490c058e984d4ebd-30583e3b66ee	Entrust.net Secure Server Certification Authority	1116153102		bee3a19a68	PEM TXT JSON	TLSA

Appendix 1: Installing a CA certificate into a LaserJet with Jetdirect networking

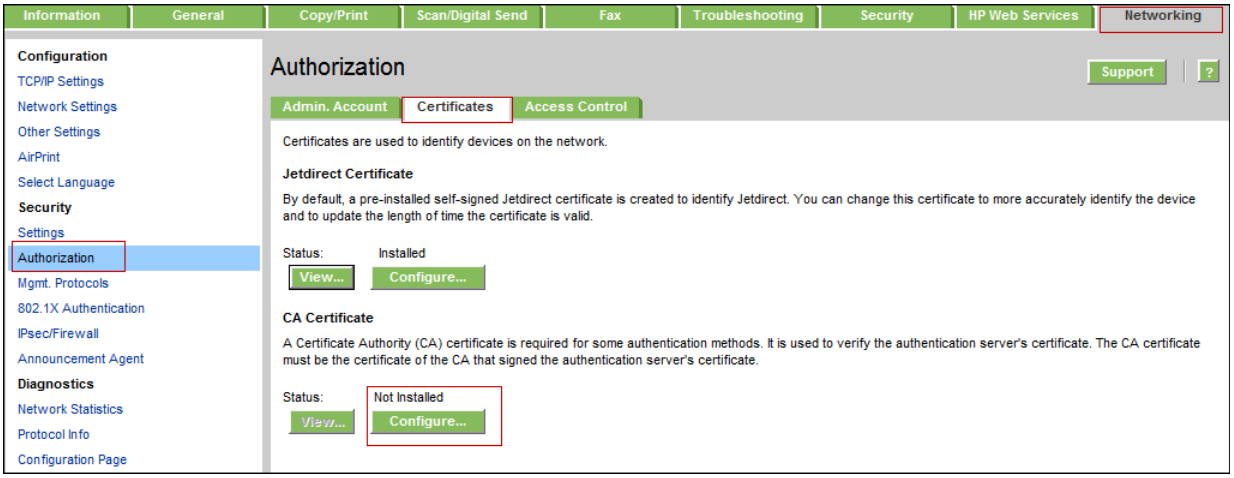
Note: Certificate Management will be revised in mid-2015. This section will no longer apply for the newer firmware releases.

After identifying and obtaining the CA certificate for your email service, the certificate should be installed into your HP LaserJet printer using the EWS interface.

Follow these steps to install the CA certificate for HP LaserJet printers using FutureSmart firmware version released before mid-2015:

1) Open the EWS.
2) Click the **Networking** tab, and in the left pane select **Authorization**.
3) In the **CA Certificate** section, click **Configure**.

Figure 5: Networking screen in the EWS



Certificates are used to identify devices on the network.

Jetdirect Certificate

By default, a pre-installed self-signed Jetdirect certificate is created to identify Jetdirect. You can change this certificate to more accurately identify the device and to update the length of time the certificate is valid.

Status: Installed

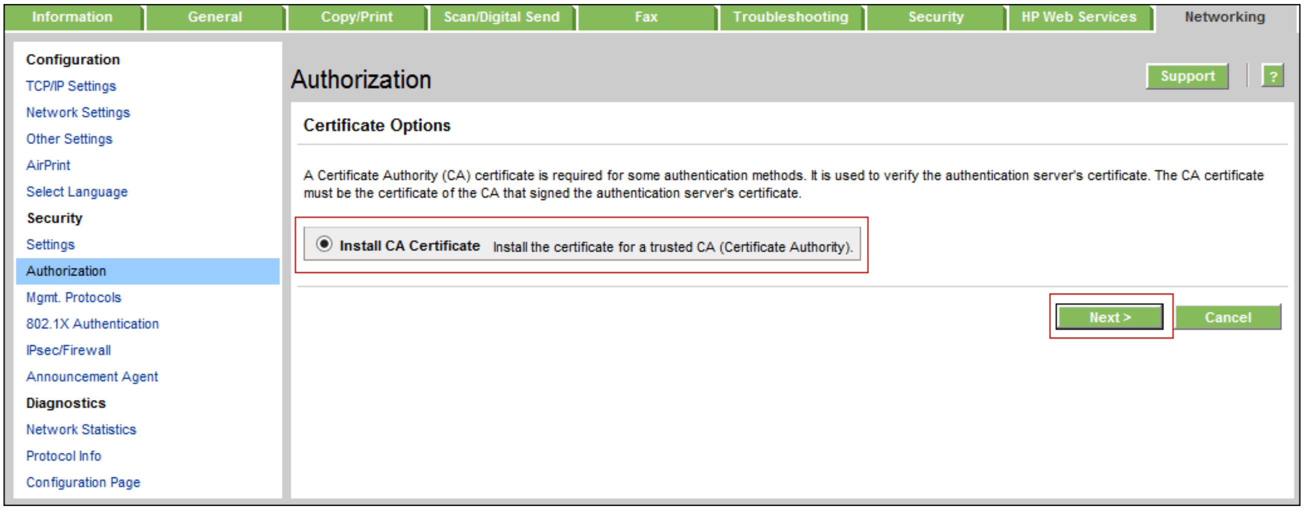
CA Certificate

A Certificate Authority (CA) certificate is required for some authentication methods. It is used to verify the authentication server's certificate. The CA certificate must be the certificate of the CA that signed the authentication server's certificate.

Status: Not Installed

4) In the **Certificate Options** section, make sure that the **Install CA certificates** is enabled and then click **Next**.

Figure 6: Certificate options



Authorization

Certificate Options

A Certificate Authority (CA) certificate is required for some authentication methods. It is used to verify the authentication server's certificate. The CA certificate must be the certificate of the CA that signed the authentication server's certificate.

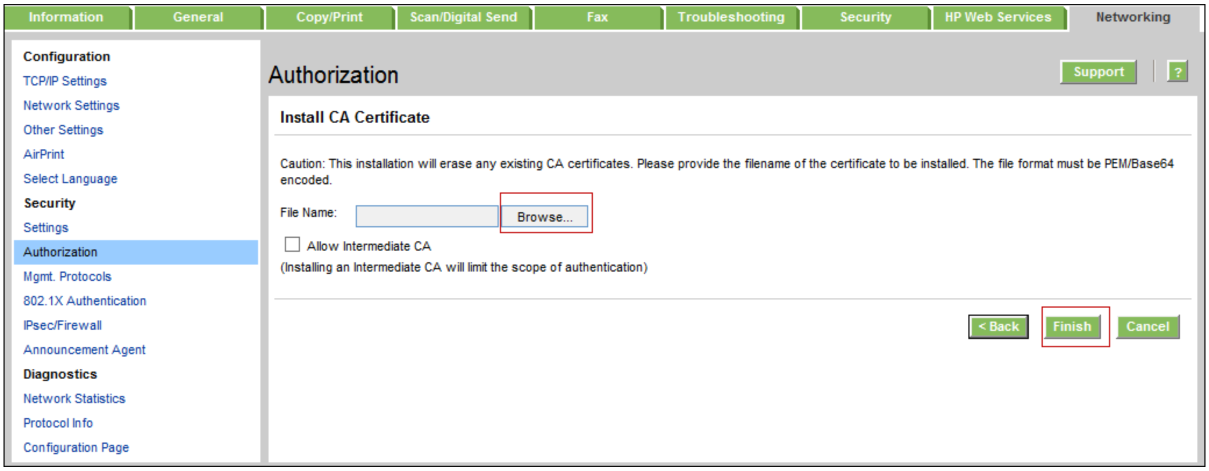
● **Install CA Certificate** Install the certificate for a trusted CA (Certificate Authority).

5) In the Install **CA Certificate** section, click **Browse**, select the certificate from your PC, and then click **Finish**.

Note: If the certificate is an *Intermediate* certificate, check the “Allow Intermediate CA” checkbox.

An intermediate CA certificate is a CA certificate in which the Subject and Issuer are not the same. In general, an intermediate CA certificate does not validate certificates as broadly as a root CA certificate; a root CA certificate should be used when available. For more information, see Appendix 3: Certificate Chaining .

Figure 7: Install CA Certificate



Authorization

Install CA Certificate

Caution: This installation will erase any existing CA certificates. Please provide the filename of the certificate to be installed. The file format must be PEM/Base64 encoded.

File Name:

□ Allow Intermediate CA

(Installing an Intermediate CA will limit the scope of authentication)

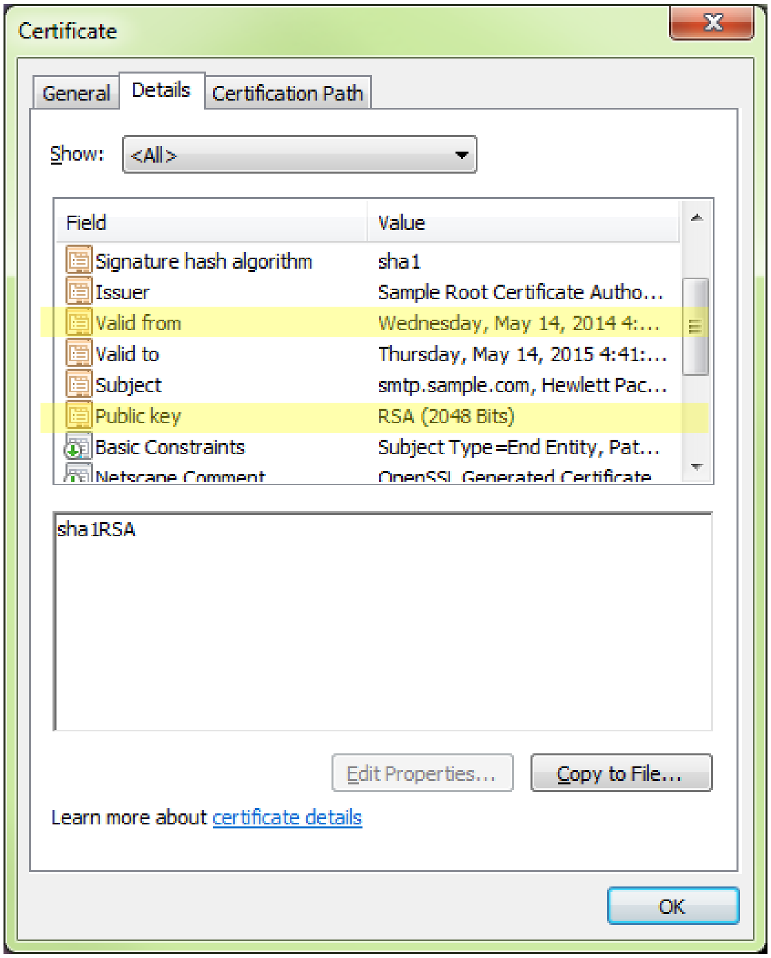
Appendix 2: Certificate Validation

A certificate, whether CA or Identity, consists of a number of plain text fields that are user-readable, and a few mathematical items that are readable, but nonsensical to normal users. This document provides information about the *Subject* and *Issuer* fields; the *Valid from* and *Valid to* fields are of secondary interest. It will also provide information of the *Public Key* and the *Private Key* mathematical encryption objects.

In an identity certificate, the Subject field identifies the entity to which the certificate was issued and the Issuer field identifies the Certificate Authority that issued the certificate. Though the contents of both the Issuer and Subject fields are arbitrary strings, generally speaking, a URL is used for the Subject while the name of the certificate authority is used in the Issuer.

Here is a partial view of a sample identity certificate:

Figure 8: Certificate Details - Valid from and Valid to fields



Show: <All>

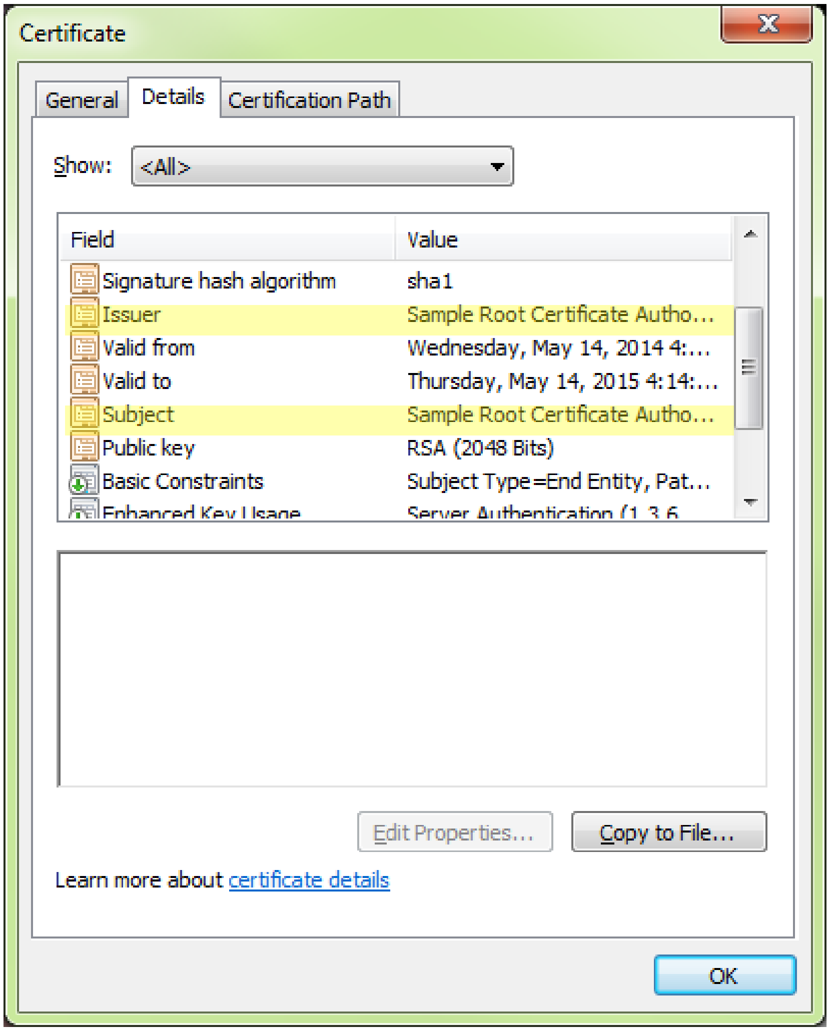
Field	Value
Signature hash algorithm	sha1
Issuer	Sample Root Certificate Autho...
Valid from	Wednesday, May 14, 2014 4:...
Valid to	Thursday, May 14, 2015 4:41:...
Subject	smtp.sample.com, Hewlett Pac...
Public key	RSA (2048 Bits)
Basic Constraints	Subject Type=End Entity, Pat...
Netscape Comment	OpenSSL Generated Certificate

sha1RSA

This certificate was issued by *Sample Root Certificate Authority* to *smtp.sample.com.*

A CA Certificate is essentially the same as an identity certificate, with Subject and Issuer fields having the same significance. A sample CA certificate is shown below:

Figure 9: Certificate Details – Issuer and Subject fields



Field	Value
Signature hash algorithm	sha1
Issuer	Sample Root Certificate Autho...
Valid from	Wednesday, May 14, 2014 4:...
Valid to	Thursday, May 14, 2015 4:14:...
Subject	Sample Root Certificate Autho...
Public key	RSA (2048 Bits)
Basic Constraints	Subject Type=End Entity, Pat...
Enhanced Key Usage	Server Authentication (1.3.6

The Subject of this certificate is *Sample Root Certificate Authority,* the organization to which the certificate was issued and that will use the certificate. The Issuer of the certificate is also *Sample Root Certificate Authority* – i.e. the organization that uses the certificate is also the issuer of the certificate. The organization *Sample Root Certificate Authority* is what is known as a *Root* Certificate Authority. It is the root of a hierarchy of certificates, an idea that we will explain later.

The most important parts of any certificate, whether it is a CA or an identity certificate, are the public and private encryption keys. These matched keys have the important properties that a) anything encrypted by the public key can only be decrypted by the private key, and b) anything encrypted by the private key can only be decrypted by the public key.

The public/private key pair provides the key elements for the validation of an identity certificate by a CA certificate. When a CA issues a certificate, it encrypts all the certificate information with its private key and attaches the encrypted version to the unencrypted information. This encryption process results in the signed certificate that is issued to the entity identified in the Subject field.

Since the encrypted part of the certificate (the signature) can only be decrypted with the public key matching the private key that encrypted it, it provides an extremely strong bond between the certificate contents, the CA and the certificate data that the CA validated before signing the certificate. Specifically, the signature in the identity certificate can be decrypted with the public key of the CA to reveal the original data. If this original data matches the certificate data, then it is certain that the certificate data is correct, and that the CA signed this exact data.

Thus a certificate's validity is created and checked in the following steps:

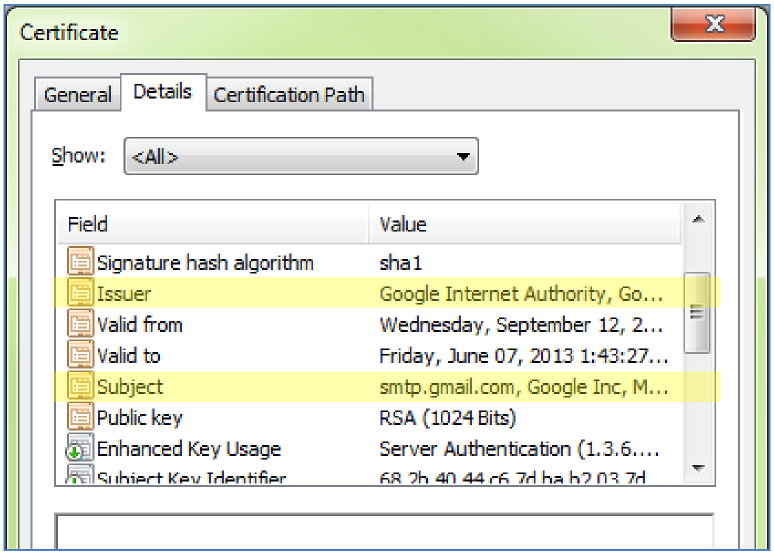
1) A Certificate Authority (CA) verifies information (subject, validity dates, usage, etc) about the server requesting an identity certificate.
2) The CA signs the certificate by attaching to the certificate an encrypted version of the certificate information as a signature. The encryption is performed with the CA's private key. The (identity) certificate is provided to the server.
3) The CA certificate is made publicly available and contains the public key.
4) The identity certificate is presented by the server to any client that would like to verify the identity of the server.
5) The client examines the Issuer field of the certificate to determine the CA that issued the certificate.
6) The client, having previously acquired the issuer's CA certificate, decrypts the signature of the identity certificate, and by verifying that the decrypted information matches the plaintext (not encrypted) part of the certificate, validates that the certificate is genuine and has not been adulterated.

Appendix 3: Certificate Chaining

When used in the real world, Certificate Authorities delegate the signing of certificates to other Certificate Authorities. Each such intermediate (or subordinate) Certificate Authority uses a certificate issued by the *root* CA (or an intermediate) to sign and issue certificates. In the real world, certificates form a *chain* between the identity certificate presented by the end-entity and the root CA certificate. See the following example:

A) An identity certificate is presented by smtp.gmail.com.

Figure 10: smtp.gmail.com in Subject field

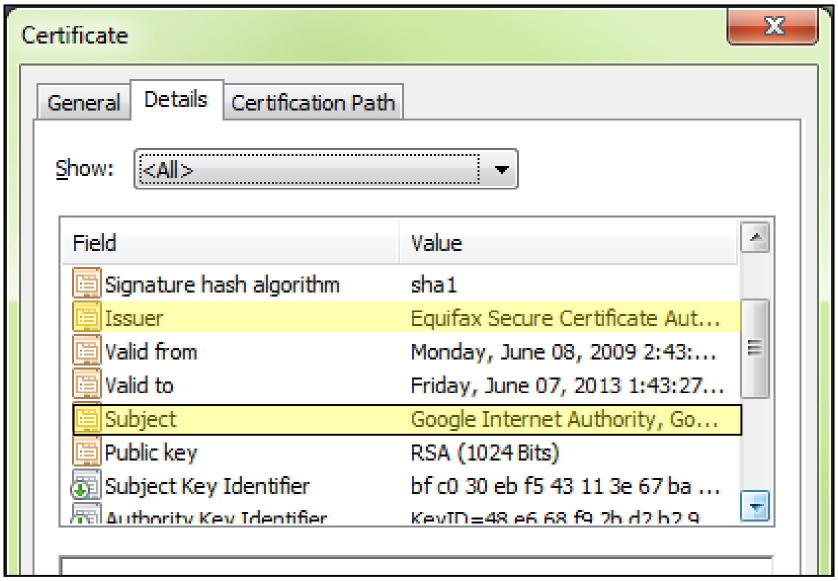


Show: <All>

Field	Value
Signature hash algorithm	sha1
Issuer	Google Internet Authority, Go…
Valid from	Wednesday, September 12, 2…
Valid to	Friday, June 07, 2013 1:43:27…
Subject	smtp.gmail.com, Google Inc, M…
Public key	RSA (1024 Bits)
Enhanced Key Usage	Server Authentication (1.3.6.…
Subject Key Identifier	68 2b 40 44 c6 7d ba b2 03 7d

B) It was issued by the CA Google Internet Authority.

Figure 11: CA Google Internet Authority in Subject field

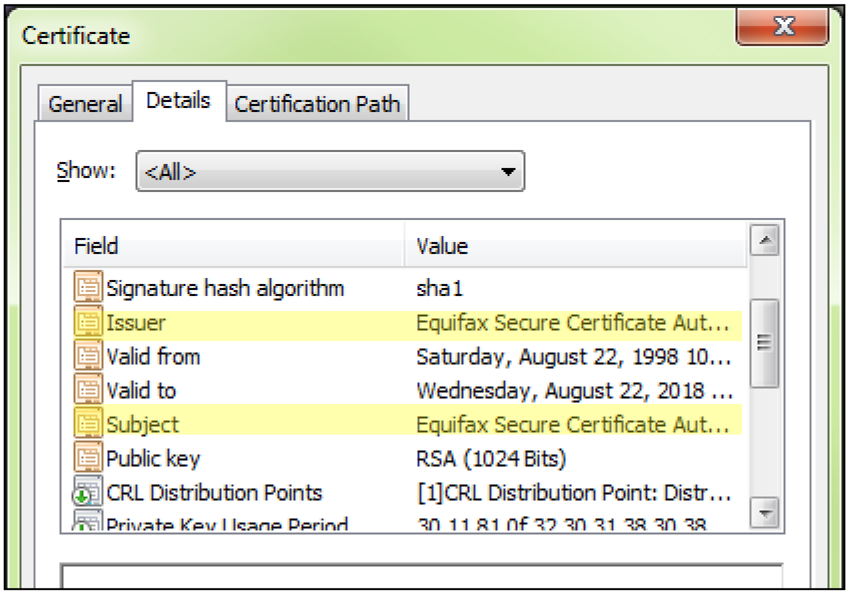


Show: <All>

Field	Value
Signature hash algorithm	sha1
Issuer	Equifax Secure Certificate Aut…
Valid from	Monday, June 08, 2009 2:43:…
Valid to	Friday, June 07, 2013 1:43:27…
Subject	Google Internet Authority, Go…
Public key	RSA (1024 Bits)
Subject Key Identifier	bf c0 30 eb f5 43 11 3e 67 ba …
Authority Key Identifier	KeyID=48 e6 68 f9 2b d2 b2 9

C) The certificate was issued by *Equifax Secure Certificate Authority,* which is *self-signed,* i.e. signed as well as issued by Equifax Secure Certificate Authority. Equifax Secure Certificate Authority takes the role of both issuer and subject because it is a *Root* certificate authority, a certificate authority that is the root of trust.

Figure 12: Equifax Secure Certificate Auth*ority* in Subject field



Show: <All>

Field	Value
Signature hash algorithm	sha1
Issuer	Equifax Secure Certificate Aut...
Valid from	Saturday, August 22, 1998 10...
Valid to	Wednesday, August 22, 2018 ...
Subject	Equifax Secure Certificate Aut...
Public key	RSA (1024 Bits)
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Private Key Usage Period	30 11 81 0f 32 30 31 38 30 38

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.