Technical white paper

Certificate-based authentication for data security

Table of Contents

Introduction

This document uses a simple analogy to help you understand how certificates are used for identity and authentication. Analogies are good at showing how a new idea is very similar to an idea that people are already very familiar with. This analogy compares digital certificates to the old-fashioned paper certificates. The analogy works so well that a lot of questions about digital certificates can be answered by thinking of how things work with paper certificates.

A certificate (digital or paper) is nothing more than a statement about something that is being made by someone with recognized authority.

Analogy: A simple checking account

For quite some time, people have been writing little notes which promise that a person will receive a certain amount of money if they bring the note to the bank. These have been called "bank notes" or "checks". The banks have set up rules that apply to checks so that a customer's account can't be wiped out by someone presenting a fraudulent (forged) check. One of the most important rules is that the check be signed by the account holder. The signature is presumed to be unique and difficult to copy. And, the bank keeps an example of it on hand (the "signature card") for whenever direct comparison is needed. Another common rule requires that the person receiving the money be the same as the person named on the check.

The check is a paper certificate. It states that a certain person should be paid a certain amount of money from a certain account at a certain bank. The statement is made by the owner of the bank account. If the validity of the certificate (check) can be verified, then the money is paid.

The bank authenticates the check using the following process:

- Verify the signature of the account holder (the "signature card").
- Verify the identity of the person presenting the check (endorsement signature, other certificates like driver's license or government ID which contain a photo and a signature).

A digital certificate is also a statement. Most often, it declares that a specific person or device has some special authority and/or capabilities. And, it has a digital signature which comes from a recognized authority which is unique and difficult to copy.

A digital certificate is authenticated using the following process:

- Verify the signature of the authoritative source.
- Verify the identity of the device presenting it.

This is basically the same process as verifying a paper check.

Verifying a digital certificate

The first step in verifying a digital certificate is to check the digital signature. The "signature card" for a digital certificate is called a "CA Certificate". "CA" stands for "Certificate Authority". It is a special kind of certificate that is used to apply signatures to other certificates. It contains a perfect copy of the digital signature. You can get one of these anywhere certificates are being signed. They are given out freely to

anybody who asks. Renown or big-name certificate vendors (such as Verisign, DigiCert, Symantec, GeoTrust, etc.) put their CA certificates on their public web sites for everybody to download. They also make sure to put them into web browsers so that certificates on popular web sites can be automatically checked without the user even knowing. Many businesses are set up to sign their own certificates. They have a CA certificate too and will also share it with all their employees.

Thanks to the complicated math implemented by cryptologists, it is nearly impossible to forge a digital signature and there is virtually no security problem sharing CA certificates with everyone everywhere. Digital certificates can't work unless CA certificates are freely shared.

For most situations that you might encounter while surfing the web, everything will happen automatically. That's because most browsers have built-in security features that automatically verify all certificates that are presented to them. And, most browsers include many built-in CA certificates from the "big-name" Certificate Authorities. So, if you surf to a web site that uses a certificate from a big-name CA then the certificate they present will be automatically trusted.

But, what about little web sites that don't use certificates from big-name CAs?

The HP Embedded Web Server (HP EWS) for an HP LaserJet printer is a prime example of a small web site that does not use a big-name certificate. In fact, the default certificate it uses is "self-signed". So, you're pretty much guaranteed to get a warning from the browser when you surf to its secure (HTTPS) address. What do you do? Well, you just need to get the right signature card (CA certificate) and install it into the Certificate Store on your computer. Here's how to do it:

Obtain and install the CA certificate from an HP LaserJet printer

1. Access the HP Embedded Web Server (HP EWS) of the printer using a web browser.
    a. Obtain the IP address or host name of the printer.
    On the printer control panel, touch the "i" Information button and select the network interface you need to use (Ethernet or Wireless). This will display the IP address and host name.
    b. Open a Web browser, and in the address line, type the IP address or host name of the printer exactly as it displays on the printer control panel. Press the Enter key on the computer keyboard. The EWS opens.

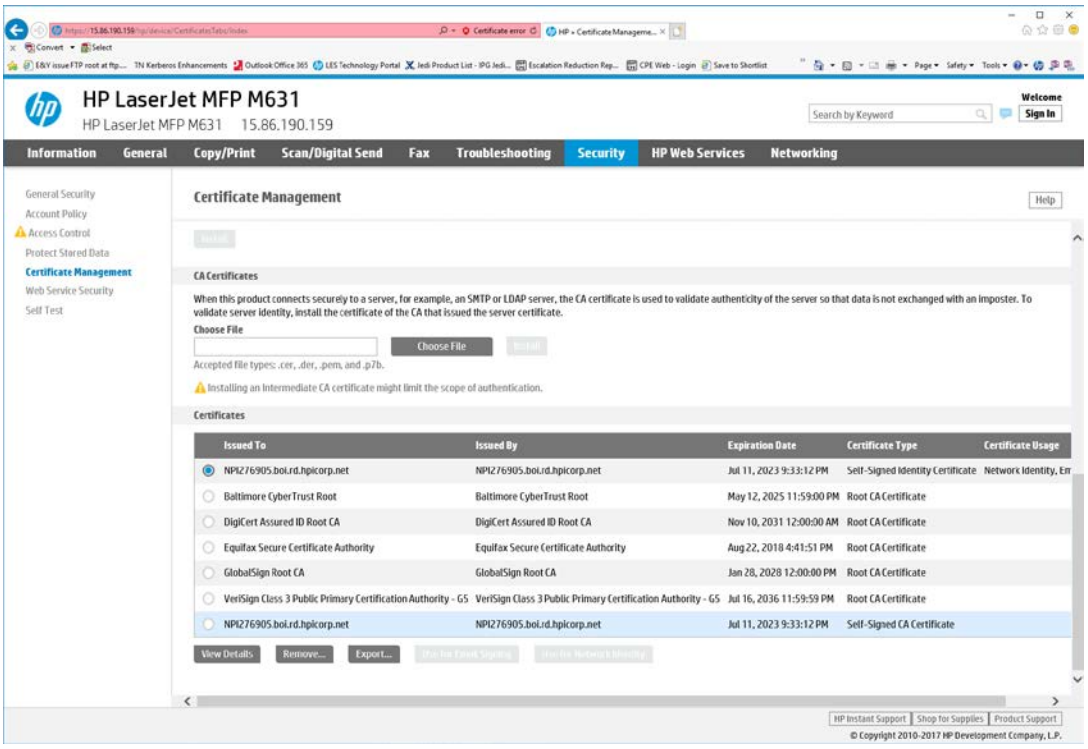
    NOTE: If the Web browser displays a message indicating that accessing the website might not be safe, select the option to continue to the website. Accessing this website will not harm the computer.

2. On the top navigation tabs, click "**Security**".

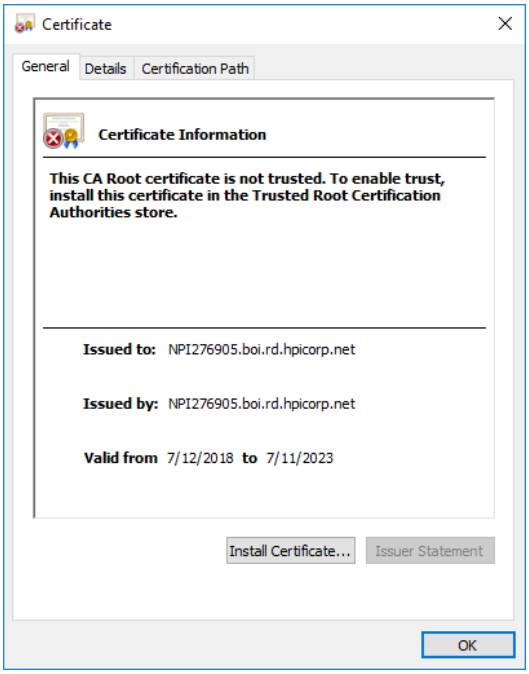
3. In the left navigation pane, select "**Certificate Management**" and scroll to the "**Certificates**" section.

4. Select the certificate that is labeled: "Self-Signed CA Certificate".

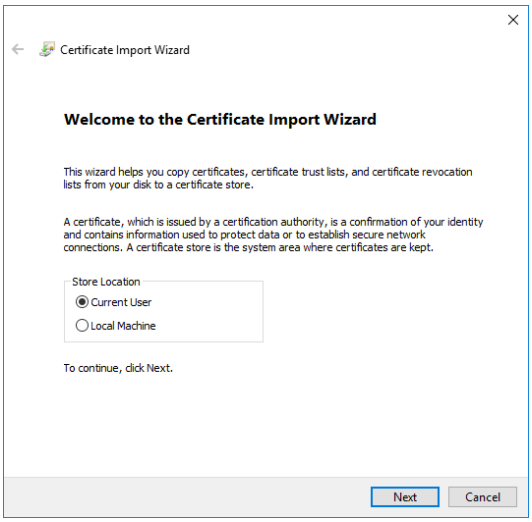
5. Click the "**Export**" button, and then save the file to on your computer.
    NOTE: Make sure to note the location of the file on your computer



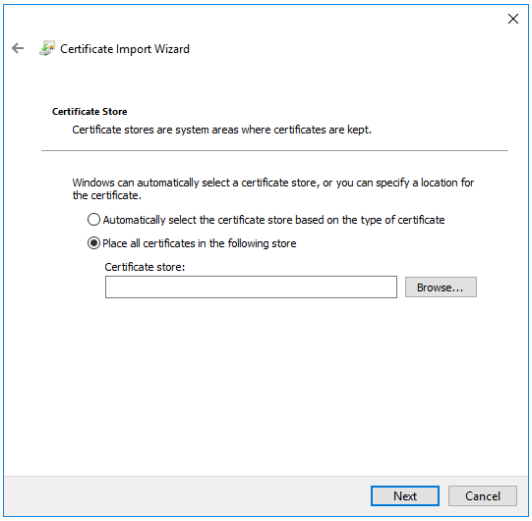
6. Open the file (using the Windows certificate viewer: Crypto Shell Extensions), and then click on the "Install Certificate..." button.



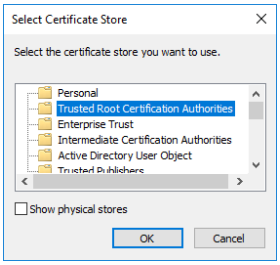
7. Select “**Current User**” option, and then click “**Next**”.



8. Select “**Place all certificates in the following store**” option.

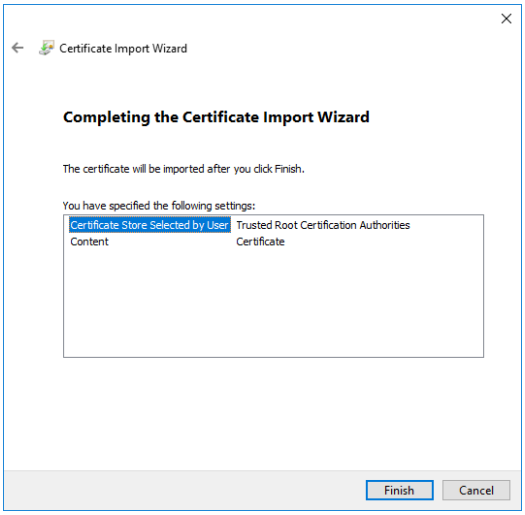


9. Click on the “**Browse…**” button, select “**Trusted Root Certification Authorities**” from the certificates listed on the Certificate Store, and then click “**OK**”.



10. Click on the "**Next**" button.

11. Review the confirmation screen, and then click "**Finish**".

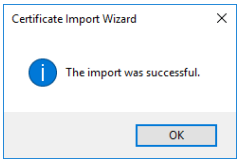


NOTE: If you see the following **Security Warning** pop-up message, click "**Yes**" to continue.

12. When the message displays, "*The import was successful.*", click "**OK**".

Your browser now has access to your printer's "signature card" and will trust the ID certificate that it sends.

NOTE: There might still be other issues that your browser flags, but the trust issue will be eliminated.



What do you do if you are not using the default self-signed certificate for ID? You go to whoever signed your printers ID certificate and ask them for a CA certificate. After you have the CA certificate the rest of the steps are identical.

Checking the identity of the device presenting the certificate

The second step in verifying a certificate is to verify that the right person or device is presenting it. This is a bit more complicated. Most of the time, web sites that require identification provide a way to enter a user name and password. A few very high security sites will go one step further: "mutual authentication". It involves the only part of a certificate that is absolutely top secret – the "Private key".

Encryption keys to create a digital certificate

The first step in creating a digital certificate is to make a pair of encryption keys. These are usually long strings of bits (2048 bits each or longer). And, they are mathematically related to each other. What one key encrypts, only the other key can decrypt. So, both keys are necessary for a two-way conversation. This is called "Paired Key Infrastructure" or PKI for short.

One of the keys is called the "Private" key. It is hidden away in a safe place where nobody but you have access. The other key is called the "Public" key and it is bundled together with the rest of the certificate to get signed by the Certificate Authority (CA).

So, there are two parts: The Private key, which is hidden away and never shared with anybody. And, there's the signed certificate, which contains the Public key and is shared with everybody.

Identifying the real certificate owner

If you want to know if someone is the genuine owner of a certificate, take their certificate and use the Public key to encrypt a message. Then wait to see if they can decrypt it. Remember, these keys come in pairs. If I encrypt with one key, only the other key can decrypt. So, when sending a message encrypted with the Public key, only the holder of the Private key will be able to decrypt it. And for this reason, it is important to keep the Private key to yourself.

Protections against forgery

What if you take a certificate with its genuine CA signature and replace the original key pair with your own key pair. Then you could use your own private key to decrypt anything that was encrypted with the public key. But, certificates have a self-checking feature that makes it easy to detect any changes. This feature renders the digital signature invalid. So, you really can't impersonate someone else unless you can steal their private key.

Is it possible to use the CA certificate to sign a new certificate which uses your key pair and your name? Yes, it is. But, this would only work if you have the CAs private key. A valid signature cannot be generated without the private key.

Summary

Obviously, this analogy leaves out a lot of detail. But, the essentials are all there. The biggest difference between digital and paper certificates is in how quickly they can be verified. Digital certificates are verified literally billions of times per day, every day. Paper certificates take so much time and effort to verify that they only get examined when there's a problem. The bank only verifies the signature on a check when you complain about a possible forgery.

Important points to remember

1. The CA certificate is the "signature card" for digital certificates. You get one so that you can make sure a signature is genuine. They are available anywhere certificates are being signed.

2. You can't verify a check from John Doe with a signature card from Joe Smith. So, don't expect that any old CA certificate can be used to validate a new ID certificate. It must be the exact same CA certificate that originally signed the ID certificate.

3. You can't validate a certificate without a CA certificate. We call this "Fake Security" and it's not uncommon among MFPs and printers from other manufacturers.

4. There is no security issue with sharing CA certificates or ID certificates freely. This is how it all works. No sharing, no security. Just make sure you share only the public key and keep the private key to yourself.

This document is a simplified explanation designed to help foster better understanding of the process. Ultimately, certificate authentication is a complex topic and there are many variances (like multi-tier Certificate Authorities) which are not mentioned in this document.

More Information

For more information about managing data security in the HP EWS, go to the following support document:

https://support.hp.com/us-en/document/c05389308

To read more about this issue, go to: hp.com/support

DocID: c06143896, Created: October 2018