Realtime
publishers

The Shortcut Guide™ To

Certificates in the Enterprise

sponsored by

thawte™
it's a trust thing™

Don Jones

Copyright Statement

© 2009 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers or its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

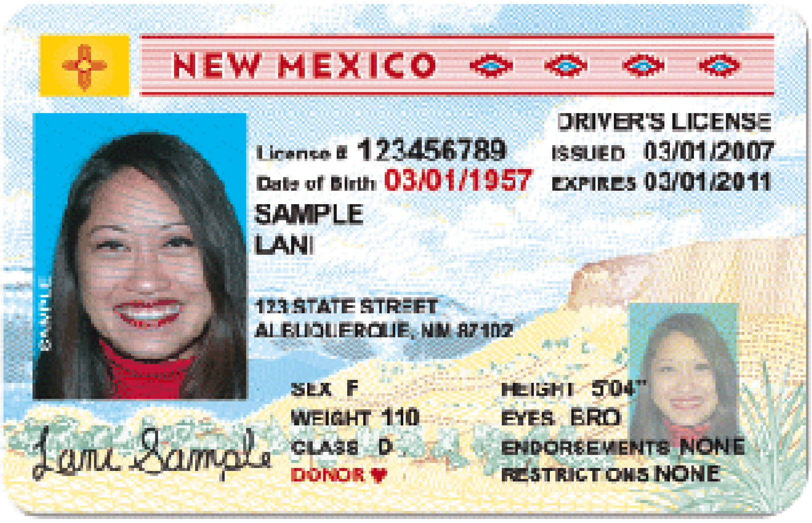
[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library for IT Professionals. All leading technology eBooks and guides from Realtime Publishers can be found at http://nexus.realtimepublishers.com.]

Chapter 3: Trust, Trust, Trust—the Root of a Useful Certificate

In previous chapters, I've written briefly about the role that trust plays in digital certificates, and how digital certificates are essentially ID cards. In this chapter, we're going to dive into that concept in a lot more depth, and really illustrate how certificates work from a trust perspective.

Certificates Are ID Cards

Do you recognize Figure 3.1?



NEW MEXICO

DRIVER'S LICENSE

License # 123456789

Date of Birth 03/01/1957

ISSUED 03/01/2007

EXPIRES 03/01/2011

SAMPLE

LANI

123 STATE STREET

ALBUQUERQUE, NM 87102

SEX F

WEIGHT 110

CLASS D

DONOR ♥

HEIGHT 5'04"

EYES BRO

ENDORSEMENTS NONE

RESTRICTIONS NONE

Lani Sample

Figure 3.1: A familiar-looking ID card.

This is a driver's license, of course, but for the sake of this illustration, we're going to refer to it as a *physical certificate.* It is, after all, something tangible that you carry around with you. There are a few important properties shared by all physical certificates of this basic type—that is, by driver's licenses:

- The name of the CA who issued this certificate—New Mexico in this case—is clearly displayed.
- Watermarks and other physical measures help identify this certificate as a valid certificate that was indeed issued by the authority whose name is displayed on the face.
- The *contents* of the certificate contain information about the person to whom it was issued. Of general interest on a certificate such as this is the birth date.

Now if Lani, the woman to whom this certificate was issued, walked into a bar, the bar would let her consume alcohol. The cool thing is that it doesn't matter if the bar is in New Mexico or in Delaware—her New Mexico-issued certificate would still work. Why? Because of *trust.*

Figure 3.2 illustrates how this trust works. In the United States, every citizen and business is configured (through our laws) to trust at least 52 CAs: all 50 states, the District of Columbia, and the federal government.

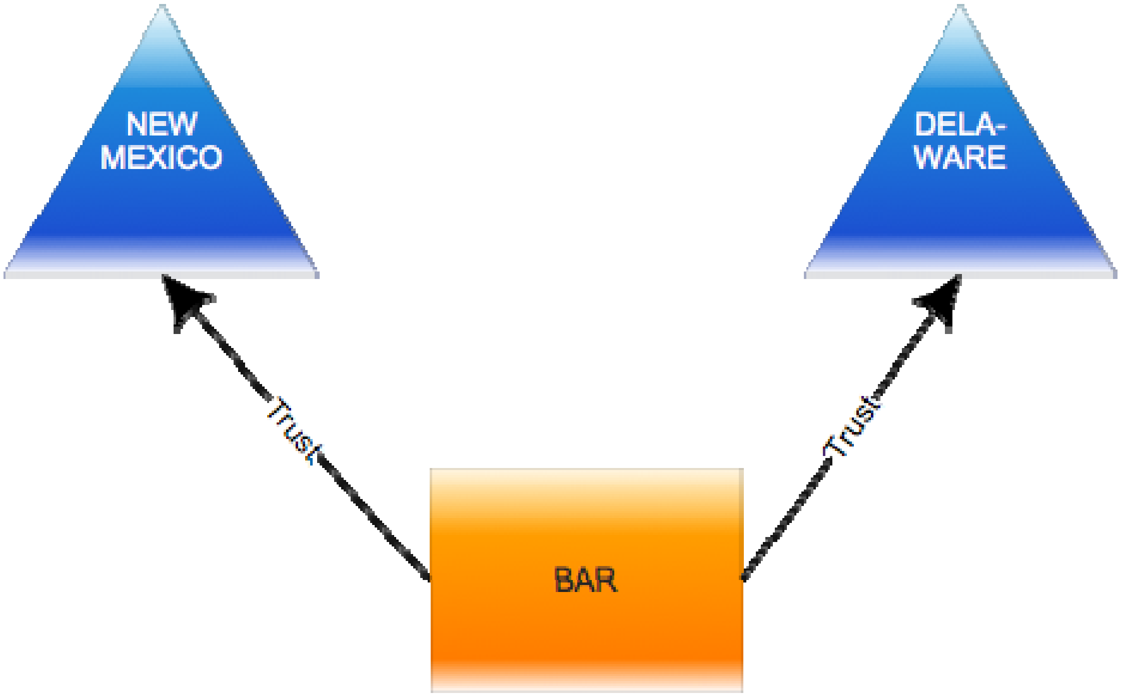


Figure 3.2: Trusting multiple CAs.

This trust means that the bar Lani walked into would accept a certificate from Delaware, where the bar is located, but also from New Mexico, California, Washington DC, or the federal government (such as a military ID). But why?

Where Trust Comes From

There are obviously complex legal reasons why the bar trusts so many CAs but there are also practical reasons. Practically speaking, the bar is interested in only four things:

- Is the person handing me the certificate the person to whom it was issued?
- Is the person old enough to drink?
- Is the certificate genuine?
- Is the certificate valid?

The first question is answered by examining the photo on the certificate and comparing it with the appearance of the person who possesses it. The second question is answered by looking at the information on the certificate *and through trust.* The bar—implicitly, every US citizen—trusts that the CA did a good job of checking into Lani's actual age and other personal details before handing Lani a certificate containing those details. In reality, that meant Lani probably had to show a birth certificate or some other document when obtaining her first license.

Note

The birth certificate is yet another physical certificate; it was issued by a CA we commonly call a "hospital." Those certificates are also widely trusted.

The bouncer at the bar doesn't *know* Lani's age, or anything else about her, and has no ready way to verify that information independently. He's placing his trust in the CA to have verified the information that he cares about.

To check the certificate's authenticity, the bouncer might examine it under an ultraviolet light, looking for telltale watermarks and other features that are difficult to forge. To check the certificate's validity, the bouncer looks at the expiration date printed on it.

Note

Wait—how does your birth date expire? This is an excellent illustration of why certificates expire in the first place. It's true that if the CA of New Mexico did a good job of verifying Lani's birth date in the first place that her birth date will never change, so there's no reason why an expired driver's license couldn't still be accepted as proof of age. But what if New Mexico realized they had made an error in verifying her age? It would be difficult to notify everyone in the US of the error on Lani's certificate, and so the CA relies in part on the fact that the certificate will eventually expire and be useless. They make a note in their own records that Lani will need to furnish proof of age in order to renew her certificate.

After reviewing this information, the bouncer now has four answers:

- The certificate matches the identity of the person holding it
- The certificate was issued by a trusted CA, so the information on the certificate is believed
- The certificate *really was* issued from that CA and not forged; the watermarks attest to its authenticity
- The certificate is within its validity period, and so can be accepted

The bouncer has verified that it's a certificate he trusts, and the information on it allows him to let Lani into the bar just in time for Happy Hour.

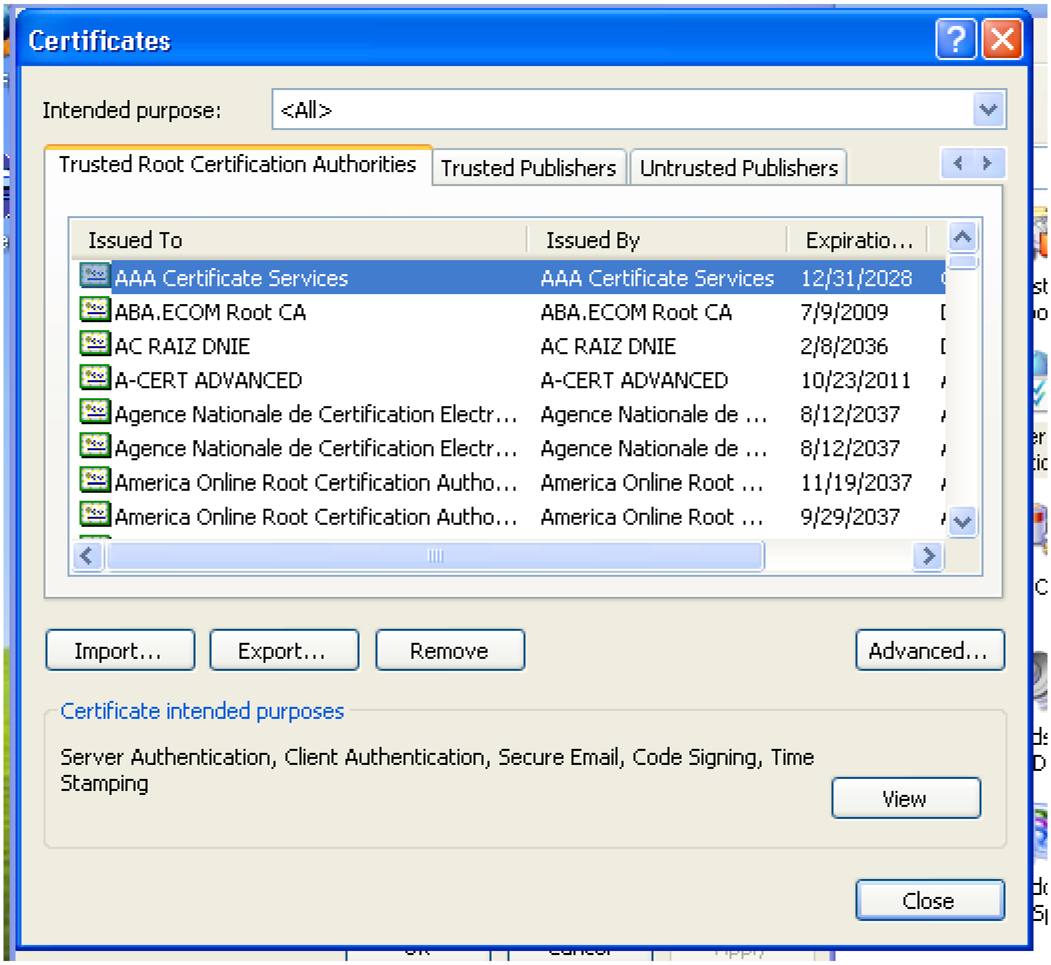
What Trust Gets You

We like to think that having a valid driver's license that shows proof of age gets us into the bar to drink, but that's not actually the case. The certificate was merely a trusted third-party way for us to communicate critical information to a second party, the bouncer. If the bouncer hadn't trusted the certificate, we wouldn't be drinking. And even if the bouncer trusts the certificate, it's not that his trust got us the alcohol—it's that his trust verified our *identity.*

That's the key thing a certificate gets you: It allows you to prove your identity to a second party by means of your mutual trust in the third party that issued the certificate. *Identity* is what certificates are truly all about. Everything else is a secondary benefit.

Digital Trust

So how does all this relate to a digital certificate? Like a driver's license, digital certificates are issued by CAs. Just as we are configured by law and custom to trust the CAs who issue licenses, we must also configure our computers to trust the CAs who issue digital certificates. Figure 3.3 shows where this trust is configured in Windows' Internet Options Control Panel.



Intended purpose: <All>

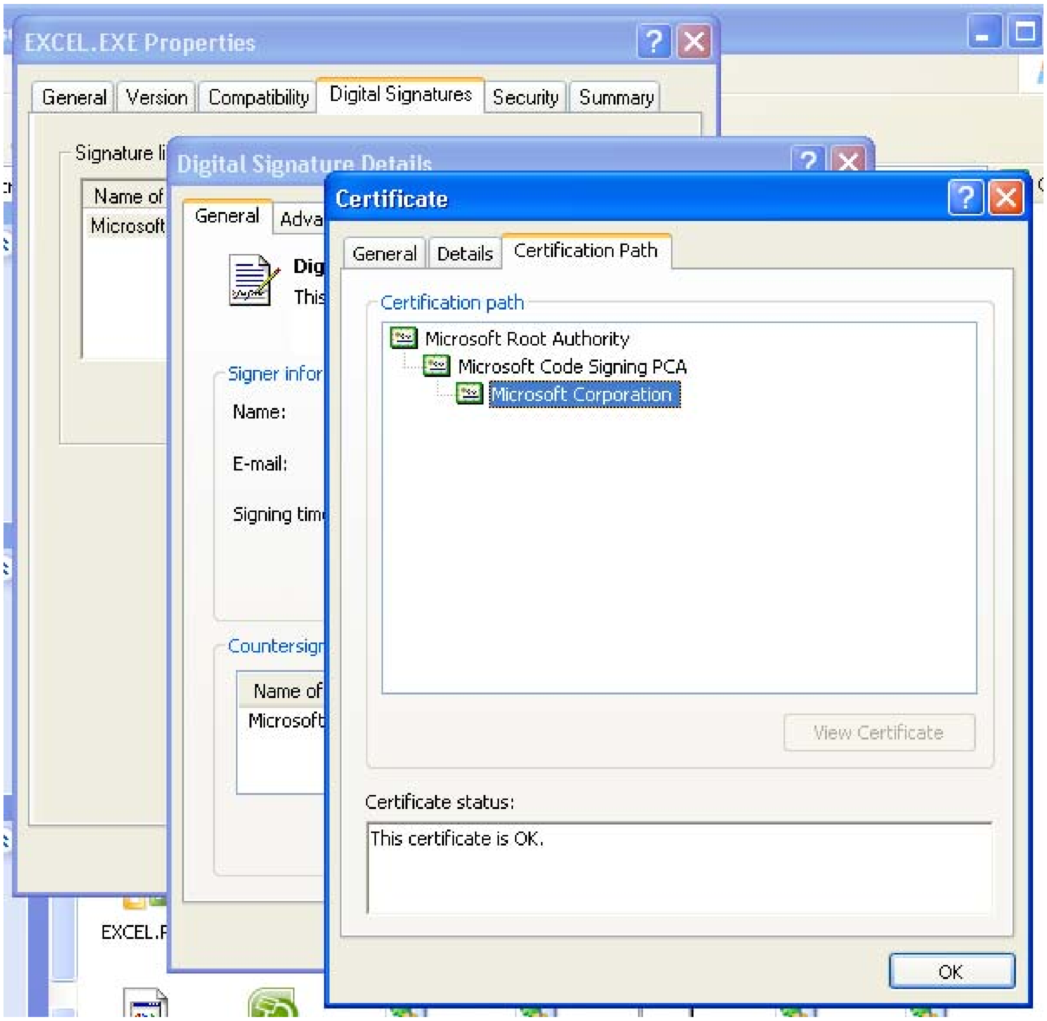
Issued To	Issued By	Expiratio…
AAA Certificate Services	AAA Certificate Services	12/31/2028
ABA.ECOM Root CA	ABA.ECOM Root CA	7/9/2009
AC RAIZ DNIE	AC RAIZ DNIE	2/8/2036
A-CERT ADVANCED	A-CERT ADVANCED	10/23/2011
Agence Nationale de Certification Electr…	Agence Nationale de …	8/12/2037
Agence Nationale de Certification Electr…	Agence Nationale de …	8/12/2037
America Online Root Certification Autho…	America Online Root …	11/19/2037
America Online Root Certification Autho…	America Online Root …	9/29/2037

Certificate intended purposes

Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping

Figure 3.3: Trusted root publishers (CAs) in Windows.

Just as the license carries watermarks to attest to its authenticity, digital certificates carry encrypted information that attest to their provisioning by a particular CA. Figure 3.4 shows this “certificate path” for a certificate in Windows.



Microsoft Root Authority
Microsoft Code Signing PCA
Microsoft Corporation

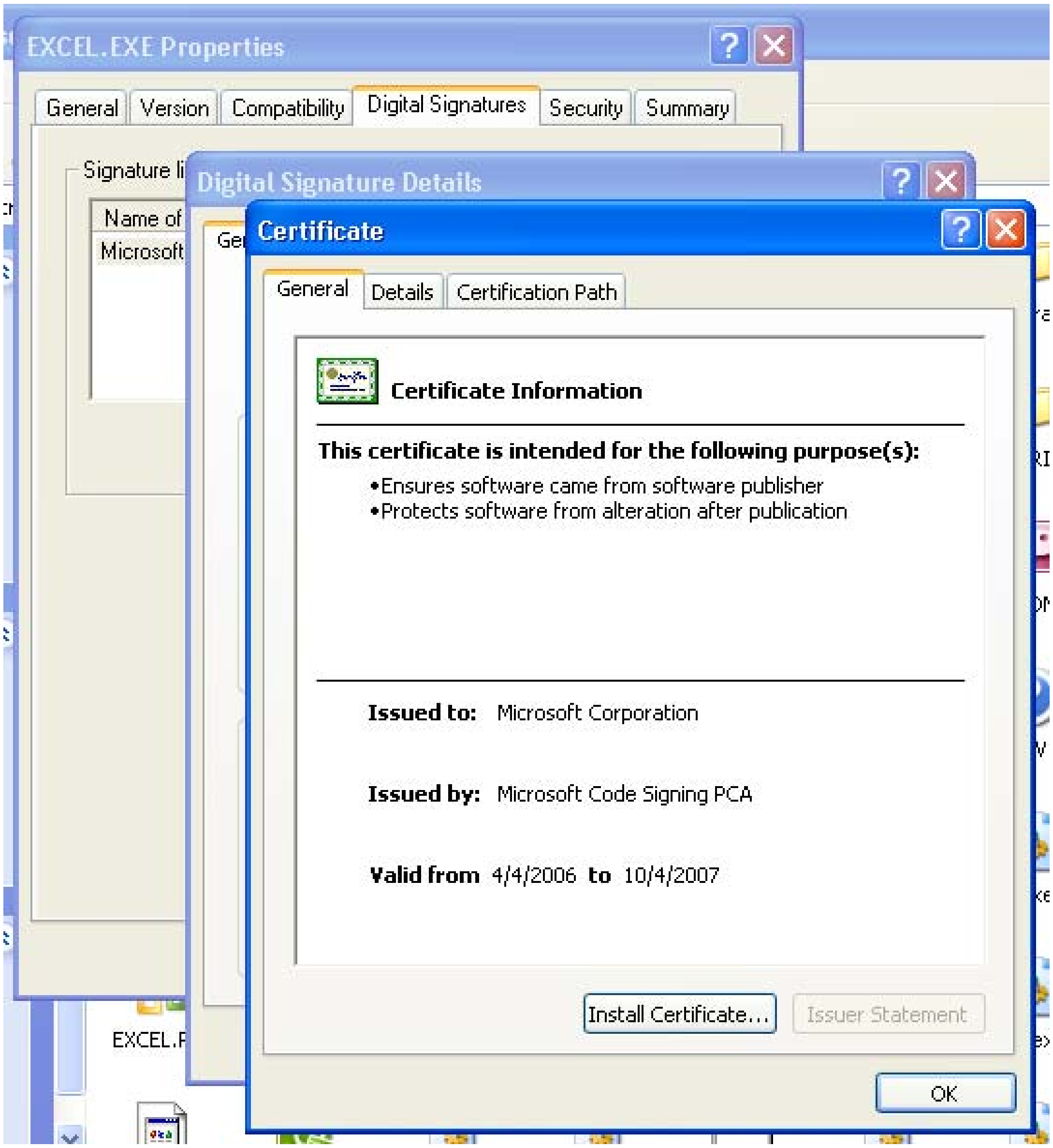
Certificate status:

This certificate is OK.

Figure 3.4: Certification path for a certificate.

Just as the license is a means of proving our identity, a digital certificate is a means of proving our identity—it just works over electronic networks rather than in-person. Unlike a license, which has a photo that allows someone to match it to our physical appearance, a digital certificate can't be physically paired to a human being. Instead, it's split into two pieces, one of which we're supposed to keep private. Our possession of that private half is what allows us to prove that a given certificate really belongs to us.

Like a license, a digital certificate comes equipped with an expiration date, beyond which it is no longer valid—even though the information on it might still be correct. Figure 3.5 shows a certificate in Windows that is past its expiration date.



Certificate Information

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

- Ensures software came from software publisher
- Protects software from alteration after publication

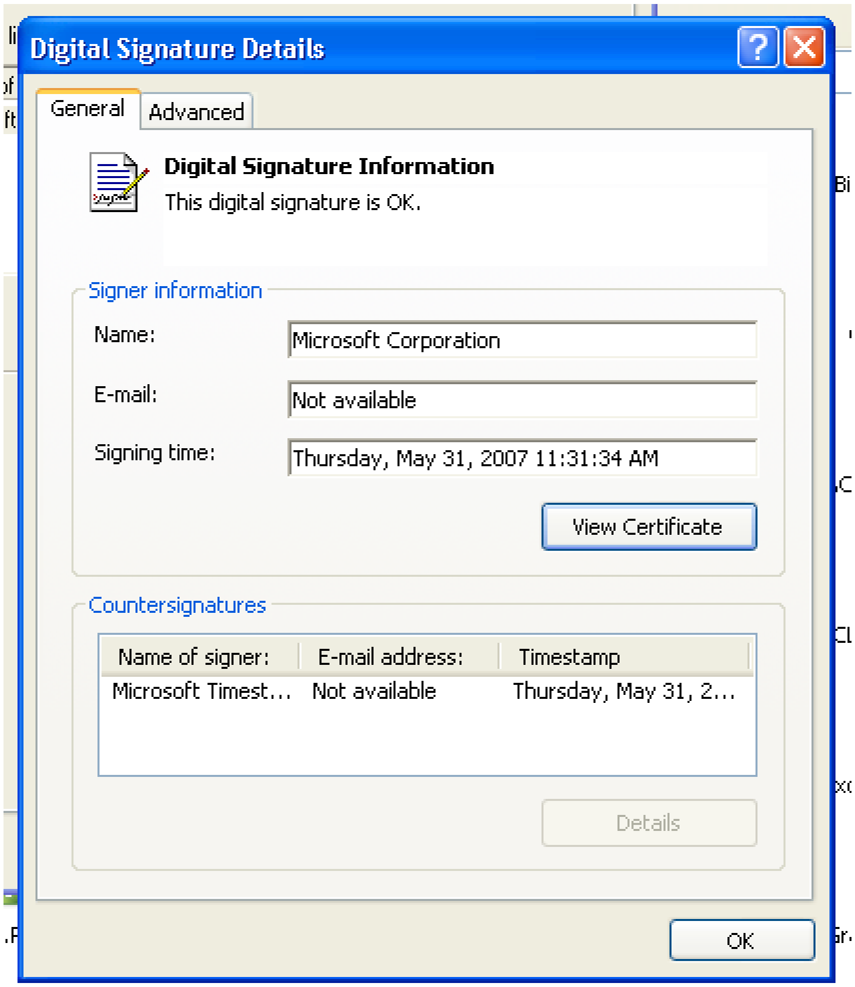
Issued to: Microsoft Corporation

Issued by: Microsoft Code Signing PCA

Valid from 4/4/2006 **to** 10/4/2007

Figure 3.5: Certificate expiration date.

Like a license, which offers the side benefit of getting you into bars, a digital certificate can offer side benefits, such as data encryption, that stem from the certificate's ability to attest to your identity. Figure 3.6 shows a certificate's use for digitally signing code.



Digital Signature Details

Digital Signature Information

This digital signature is OK.

Signer information

Name: Microsoft Corporation

E-mail: Not available

Signing time: Thursday, May 31, 2007 11:31:34 AM

Countersignatures

Name of signer:	E-mail address:	Timestamp
Microsoft Timest...	Not available	Thursday, May 31, 2...

Figure 3.6: Digitally signed application executable.

Note

Encryption *is* a side benefit of a certificate. What's important is *identity.* If you can't verify the identity of someone to whom you're going to send data, why bother encrypting it? That is, if you're not sure who is on the other end, does it really matter whether it's encrypted? Even though encryption is a *very* commonly used side benefit, it remains a side benefit: The primary function of the certificate is the verification of identity, which is why trust is so important.

Breaking Trust

What if it became known that New Mexico had erroneously attributed 1957 birth dates to hundreds of people whose birth dates were actually in 1997? A forty-year difference! Suddenly, all the people who used to trust the New Mexico CA might be a little less trusting. It's possible that Lani's trip to Delaware would be entirely free of cocktails because bars would no longer accept her suspect certificate—even if her CA hadn't explicitly revoked it.

Digital certificates carry the same consequences. If it becomes known that a CA did a bad job of verifying someone's identity, folks might stop trusting the certificates issued by that CA—and every certificate the CA issued would then be useless. So *trust* is a very important part of a CA's business model, because in essence, they're not really selling certificates. They're selling *trust.*

Note

In fact, one well-known commercial CA did accidentally issue a certificate to someone they shouldn't have due to a flaw in their internal processes. Fortunately, digital certificates—unlike their physical cousins—can be revoked fairly easily, so the CA was able to correct the situation pretty quickly. Still, the situation did make folks at the time take more notice of identity verification procedures.

Levels of Trust

We can all agree that there are varying levels of trust. Letting someone in to see an "R" rated movie isn't as severe as allowing them to drink alcohol, and even that is less severe than, say, allowing them to purchase a handgun. Because verifying someone's identity over the Internet can be difficult and expensive, the industry has decided on numerous trust levels. Lower levels of trust generally require less-stringent efforts to verify someone's identity; higher levels of trust often require more intensive identity checks that might even include offline public records checks.

One of the earliest commercial CAs developed a hierarchy of classes that helped to communicate the level of trust associated with a specific type of certificate.

- Class I certificates are for individuals and are typically used for sending email. The certificate is often issued to an email address, rather than a human being, and the only verification might be checking to make sure the applicant actually has control of that email address—meaning they can use it to send and receive email.
- Class II certificates are for organizations, and the CA will usually require proof of the organization's identity, such as a copy of their articles of incorporation.
- Class III certificates are usually used for Web servers (commonly called "SSL certificates") and for code-signing. This may require more stringent checks of the organization's identity, but, then again, they might not. I'll cover this in particular in the next section of this chapter.

- Class IV certificates are designated for online transactions between different businesses.
- Class V certificates are commonly issued for governmental security, and require some of the most stringent background checks.

> **Note**
>
> Class I and III certificates are the most commonly used. Many people will go their entire careers or lives without ever interacting with a certificate other than Class I and III types.

Understand that there are no significant *technological* differences between these certificates, other than a flag contained within the certificate that says for what uses it was issued. The differences between these are simply the amount of effort that went into verifying the applicant's identity. The reason a certificate might be flagged "for email only" is because the CA only verified the applicant's control of the email address; without more stringent background checks, the CA doesn't want to attest to any greater level of trust in the applicant's identity.

> **Note**
>
> There are minor differences between certificates intended for different purposes, due entirely to the software that must use the certificate. I call these "packaging" differences because they primarily relate to how the certificate is actually encoded, bundled, and delivered to the applicant.

How CAs Verify Identity

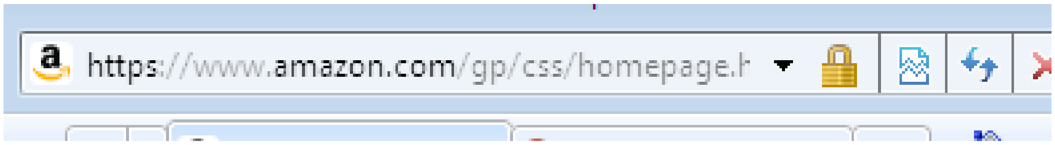
Verifying the identity of someone who applied for a certificate through a Web site is tricky. Companies that maintain their own internal CAs—called a *public key infrastructure,* or PKI—often have an easier time visually confirming an employee's identity before issuing certificates, but that is not practical for commercial CAs operating over the Internet.

Different CAs have devised different schemes, all of which relate back to the level of trust required:

- If I need a certificate that can attest to my *identity*—not just my control of an email address—I might need to have a printed statement signed by a local notary public. I could then fax that statement to the CA, who could use it as proof that my identity had been visually verified. They could then issue me a certificate attesting to whatever identity was described on the photo ID I showed the notary.
- If I need a certificate that attests to my email address—used for digitally signing and encrypting email, for example—I might just need to prove control over that email address. The CA might just need to send a confirmation email containing a confirmation code or URL that I could enter or click on.

Things can actually get stickier when you start talking about Class III certificates, and this is where the subtle aspects of trust, not to mention the fine-print in the certificate, can become really important.

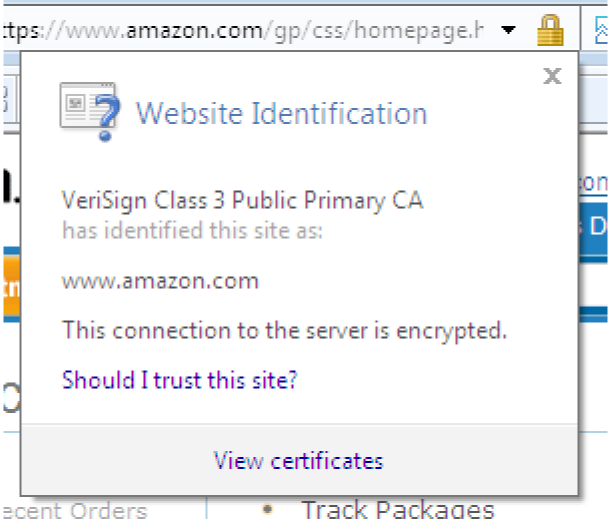
Let's say you go shopping online at Amazon.com. You're going to be handing off credit card information, so you look for the appropriate icons in your Web browser to make sure the connection is encrypted. You might even look at the URL to make sure it starts with "https://" rather than http:// (although https:// is no guarantee of encryption; it only requires verification of identity; encryption is optional). As Figure 3.7 shows, browsers use locks and other icons to indicate the encryption is turned on.



https://www.amazon.com/gp/css/homepage.h

Figure 3.7: Verifying an encrypted browser session.

Figure 3.8 shows that some browsers even offer additional information; in this case, by clicking the lock icon. Doing so tells you who issued the certificate that's creating the encrypted connection because, again, you should care less about encryption than you do about who's actually receiving your data.



tps://www.amazon.com/gp/css/homepage.h

Website Identification

VeriSign Class 3 Public Primary CA
has identified this site as:

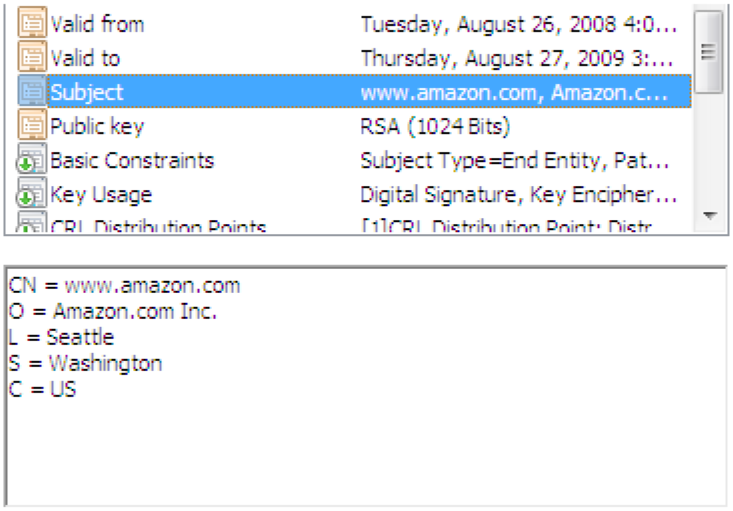
www.amazon.com

This connection to the server is encrypted.

Should I trust this site?

Figure 3.8: Viewing details about the encrypted connection.

Ideally, your browser will also show you the full certificate, where you can see (as Figure 3.9 shows) the company to whom the certificate was actually issued.



Valid from	Tuesday, August 26, 2008 4:0...
Valid to	Thursday, August 27, 2009 3:...
Subject	www.amazon.com, Amazon.c...
Public key	RSA (1024 Bits)
Basic Constraints	Subject Type=End Entity, Pat...
Key Usage	Digital Signature, Key Encipher...
CRL Distribution Points	[1]CRL Distribution Point: Distr

```
CN = www.amazon.com
O = Amazon.com Inc.
L = Seattle
S = Washington
C = US
```

Figure 3.9: Reviewing a Web site's certificate.

At this point, you need to ask yourself a couple of questions. First of all, do you trust the CA that issued the certificate? *Do you know what they did to verify the company's identity and control over this Web site?* You probably don't. You probably think all CAs do basically the same thing. If so, you'd be wrong.

This goes back to the bouncer at the bar in Delaware: He *does* basically know what each state's CA did to verify Lani's birth date. We all basically know what happens in that case. But when it comes to Web sites, we tend to make *assumptions,* which is a bad idea.

Let me give you two examples from opposite ends of the spectrum. Both of these are real, currently-used techniques employed by different CAs to issue Class III certificates that are used as Web server SSL certificates. There is also a spectrum of techniques in between these—as I said, these are extremes:

- The CA receives the request for a certificate bearing the "amazon.com" name. They send an email to someone in that domain, maybe "admin@amazon.com," and if the person applying for the certificate receives that email and confirms it (maybe by clicking a link in the email), the CA issues the SSL certificate for www.amazon.com.
- The CA receives the request for a certificate bearing the "amazon.com" name. The CA checks to see who owns that domain, and sees that it's registered to Amazon.com of Seattle, Washington. They call Dunn and Bradstreet, who maintain credit reports on companies (in much the same way that Equifax maintains reports on individuals), they check local phone listings, and they may even check with the Washington Secretary of State to see if Amazon.com, Inc. is really registered and in good standing. Once they verify all that information, they'll issue the certificate.

Can you spot the difference? The first CA issued a certificate *to a domain name.* The second CA issues a certificate *to a company.* In the first case, you know that you're connected to "amazon.com" but you actually have no idea what *entity* is behind that. Here's why that can be dangerous:

1. You mistakenly type “amzon.com” instead of “amazon.com.”
2. You go to a Web site that looks like Amazon.com’s. Your browser shows an encrypted connection and you don’t bother to check the certificate.
3. You have no idea who you’re sending your data to.

With the second CA, though, you know who you’re doing business with… *if you check the certificate.* Which, yes, you should always do. That’s telling you that yes indeed, you’re connected to the “amazon.com” server—but you could tell that by carefully reading the URL in the browser’s address bar. The certificate tells you what *company* is behind that Web site—where they’re headquartered, and so forth.

The first CA isn’t technically proving anyone’s *identity,* and since that is what certificates are supposed to do, that SSL certificate is worse than useless because it can also be misleading. A “secure” Web connection is about more than just a lock icon; it should be about your *trust* in the company to which you’re sending your data. That’s why different CAs exist, and it’s why they charge different prices. You may think they’re competing just on profit margins—after all, how much can it really cost to push a few buttons and make a certificate? In fact they are competing on *trust*—or they should be, for a knowledgeable consumer—and the amount of effort that they put into verifying someone’s identity before issuing a certificate attesting to that identity.

Put another way: If someone took our Delaware bar bouncer a driver’s license like the one shown in Figure 3.10, do you think he’d accept it?

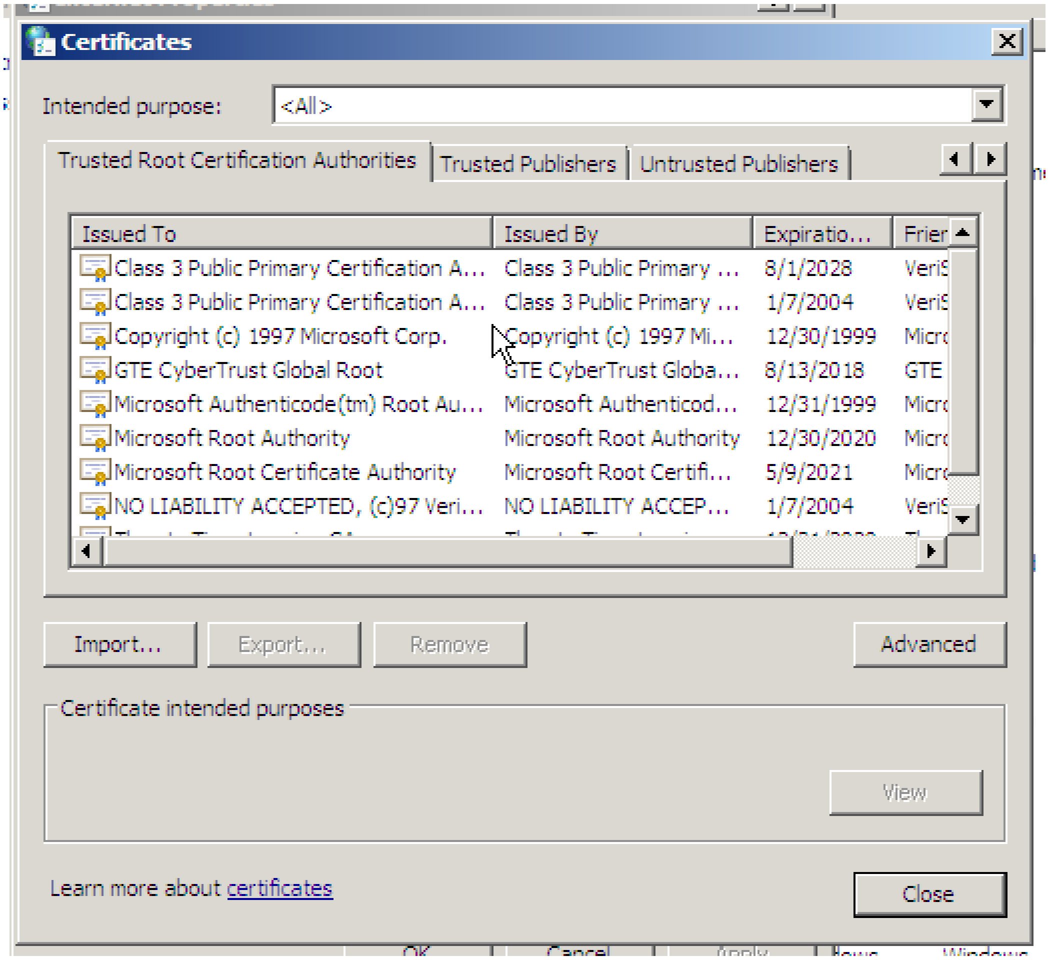
Figure 3.10: A driver’s license?

Obviously not because he *wouldn’t trust whoever issued it.*

Managing Trust

Managing trust in a large organization can be difficult. The Windows OS in particular (when in a domain environment), makes it easier by implementing centralized policy controls over trust.

You've already seen Windows' Internet Options Control Panel, where users can configure their own trusted root CAs. This is generally a bad idea, as most users aren't equipped with enough knowledge or training to make smart decisions in that dialog box. Indeed, one wonders about Microsoft's own decision-making capabilities; Figure 3.3 was from Windows XP, which trusts—by default—more than 100 root CAs from all over the world. Fortunately, later versions of Windows are much less trusting by default. Figure 3.11 shows Windows Server 2008's default list, with less than a dozen CAs.

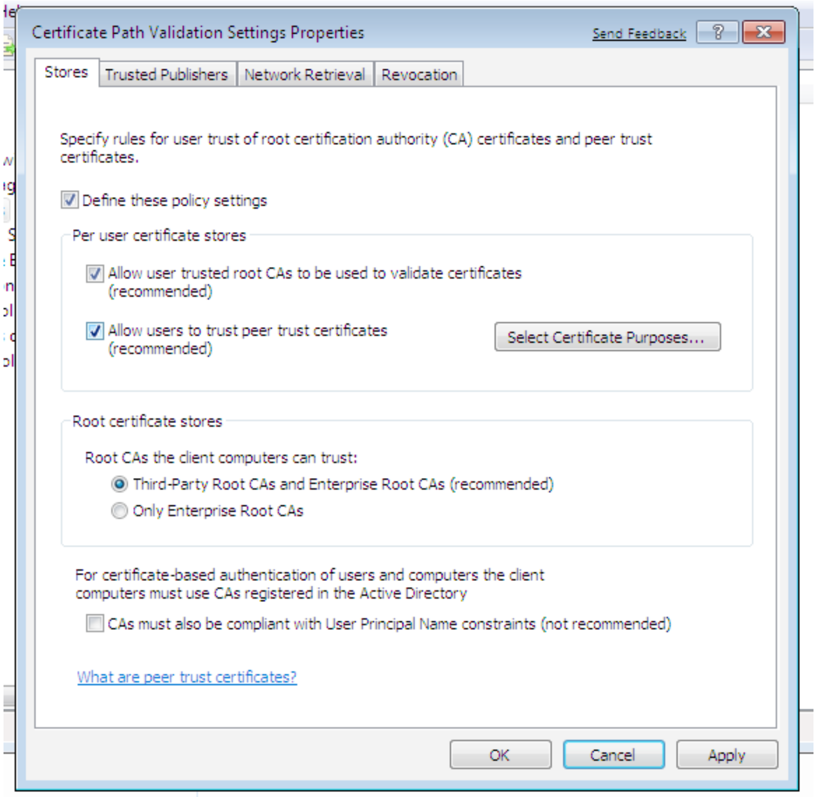


Intended purpose: <All>

Issued To	Issued By	Expiratio...	Frier
Class 3 Public Primary Certification A...	Class 3 Public Primary ...	8/1/2028	VeriS
Class 3 Public Primary Certification A...	Class 3 Public Primary ...	1/7/2004	VeriS
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Mi...	12/30/1999	Micrc
GTE CyberTrust Global Root	GTE CyberTrust Globa...	8/13/2018	GTE
Microsoft Authenticode(tm) Root Au...	Microsoft Authenticod...	12/31/1999	Micrc
Microsoft Root Authority	Microsoft Root Authority	12/30/2020	Micrc
Microsoft Root Certificate Authority	Microsoft Root Certifi...	5/9/2021	Micrc
NO LIABILITY ACCEPTED, (c)97 Veri...	NO LIABILITY ACCEP...	1/7/2004	VeriS

Figure 3.11: Trusted CAs in Windows Server 2008.

In addition, Windows' Active Directory (AD) implements several centralized Group Policy settings that can be used to configure trust. Figures 3.12 and 3.13 show two such policy settings, which can be used to restrict users' capability to make trust decisions on their own.



Specify rules for user trust of root certification authority (CA) certificates and peer trust certificates.

☑ Define these policy settings

Per user certificate stores

☑ Allow user trusted root CAs to be used to validate certificates (recommended)

☑ Allow users to trust peer trust certificates (recommended)

Root certificate stores

Root CAs the client computers can trust:

● Third-Party Root CAs and Enterprise Root CAs (recommended)

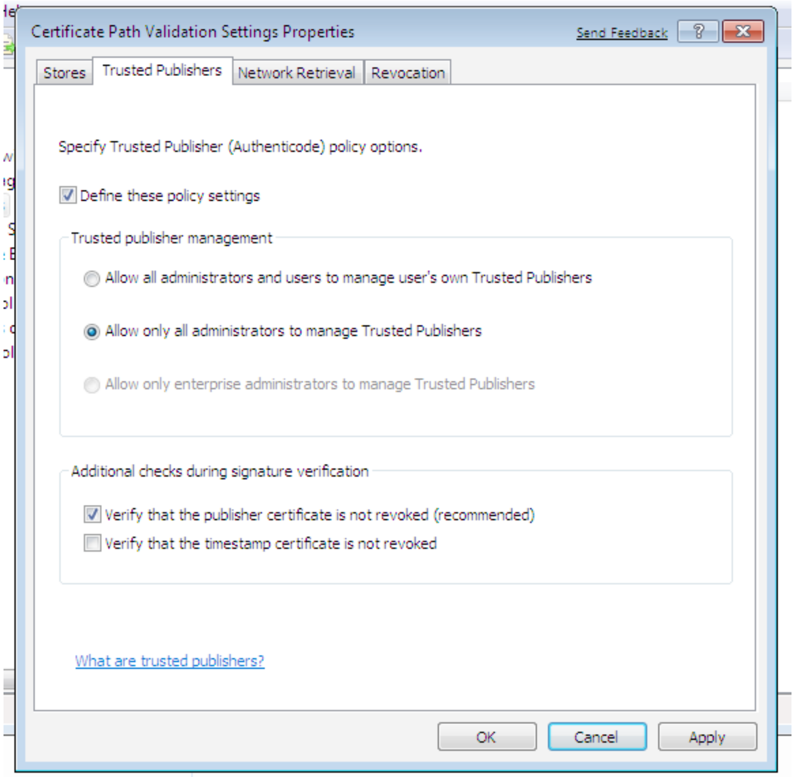
○ Only Enterprise Root CAs

For certificate-based authentication of users and computers the client computers must use CAs registered in the Active Directory

□ CAs must also be compliant with User Principal Name constraints (not recommended)

What are peer trust certificates?

Figure 3.12: Trust validation path settings (1 of 2).



Specify Trusted Publisher (Authenticode) policy options.

☑ Define these policy settings

Trusted publisher management

○ Allow all administrators and users to manage user's own Trusted Publishers

● Allow only all administrators to manage Trusted Publishers

○ Allow only enterprise administrators to manage Trusted Publishers

Additional checks during signature verification

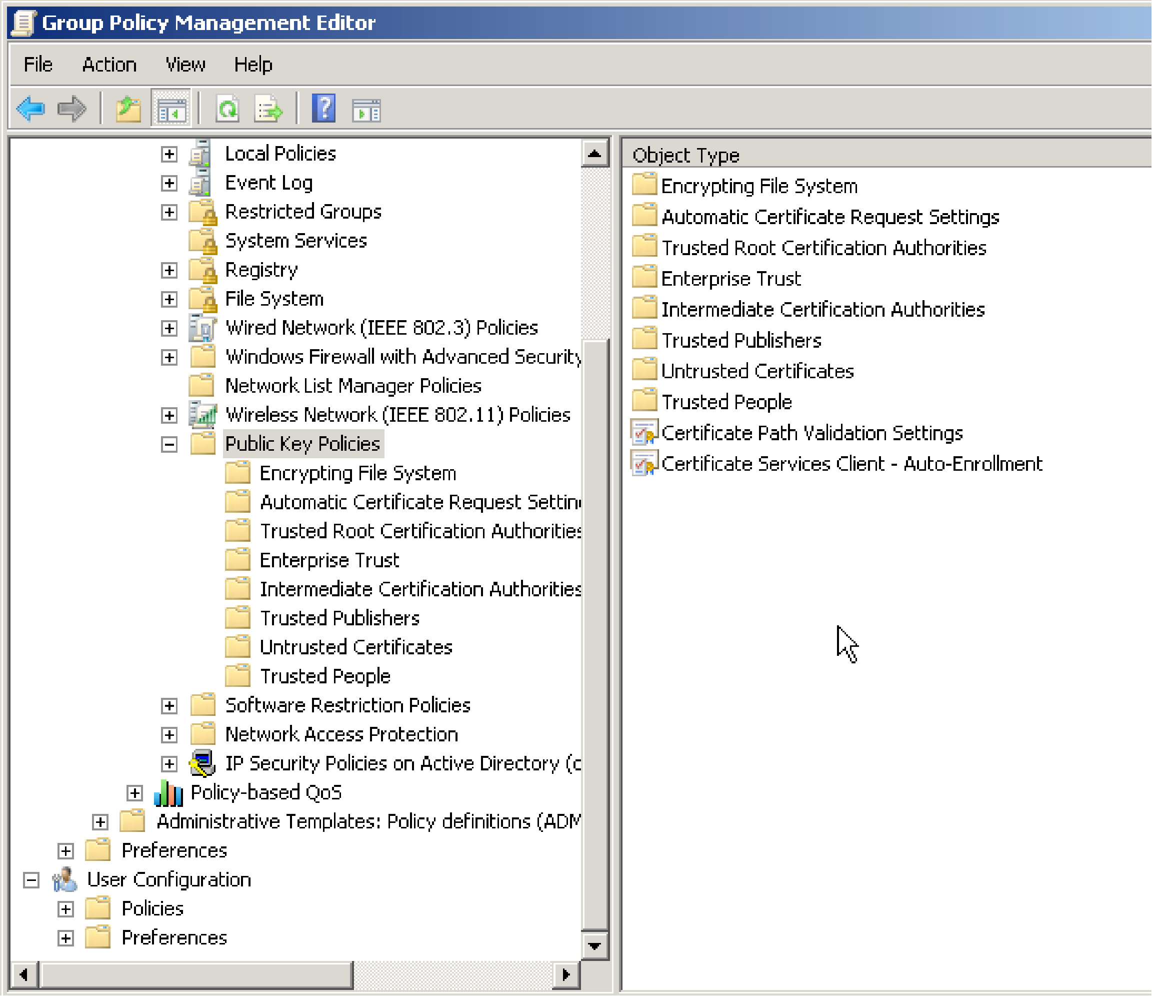
☑ Verify that the publisher certificate is not revoked (recommended)

□ Verify that the timestamp certificate is not revoked

What are trusted publishers?

Figure 3.13: Trust validation path settings (2 of 2).

In addition, Group Policy can be used to deploy an entire set of trusted root CAs to client computers and servers on the network. Doing so enables the business to make umbrella decisions about which CAs' identity-validation processes the business trusts, and to push that decision out to all their computers. It enables the business to restrict users from trusting additional root CAs, as well—helping to ensure the actual security of the entire business network (and the information it contains) without placing the burden of understanding CAs' verification policies on each user's shoulders. Figure 3.14 shows the Windows Group Policy Management Console opened to the Public Key Policies node.



- Local Policies
- Event Log
- Restricted Groups
- System Services
- Registry
- File System
- Wired Network (IEEE 802.3) Policies
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Wireless Network (IEEE 802.11) Policies
- Public Key Policies
  - Encrypting File System
  - Automatic Certificate Request Settin
  - Trusted Root Certification Authorities
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Trusted Publishers
  - Untrusted Certificates
  - Trusted People
- Software Restriction Policies
- Network Access Protection
- IP Security Policies on Active Directory (c
- Policy-based QoS
- Administrative Templates: Policy definitions (ADM
- Preferences
- User Configuration
  - Policies
  - Preferences

Object Type
Encrypting File System
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment

Figure 3.14: Centrally configuring trusted certificates.

Note that the administrator actually has very flexible options for defining these policies:

- You can define a list of trusted publishers (root CAs as well as intermediates)
- You can define explicitly-untrusted publishers
- You can define a list of "trusted people"—that is, certificates issued to individuals who are trusted

This kind of centralized control over trust is absolutely what most companies should be using. Why rely on users' good judgment when a "Do You Want to Trust This Site?" dialog box pops up? Most users, as I've said, don't have the training or knowledge needed to answer that question, and tend to just click "Yes" if they think it'll make the dialog go away and let them get on with their business.

Coming Up Next

Certificates aren't the only thing you need to deal with: How users' software utilizes and interacts with those certificates is also critical. In the final chapter of this guide, we'll look at how "What You Don't Know Will Hurt You"—a collection of caveats and gotchas that frequently frustrate those who are new to certificates.