Realtime publishers

The Shortcut Guide™ To

Subject Alternative Name Certificates

sponsored by

VeriSign®

Mike Danseglio

Copyright Statement

This sponsored eBook is valid until August 31, 2011.

Chapter 3: The Business Value of SAN Certificates

Chapter 1 reviewed the basics of certificates. We established definitions for certificates and related technologies and processes. Although this chapter might have been a review for most readers, it is important to set up a common foundation before pressing on to the more technical and complex subject of SAN certificates, as we did in Chapter 2.

Chapter 2 explored the details of a SAN certificate. This exploration included examining the appropriate public key cryptography standards (PKCS) and comparing data between SAN and non-SAN certificates. We wrapped up by comparing SAN certificates to wildcard certificates to show the distinction between two somewhat similar objects.

Chapter 3 offers a look at a different aspect of certification—the business aspect.

> **Cross Reference**
>
> You should feel comfortable flipping back to Chapter 1 periodically as you read through this chapter, especially the glossary. Nobody memorizes every PKI-related definition, and you're certainly not expected to. But if you see a term that you're not very familiar with (for example, CRL Distribution Point), the glossary is there for you. Flipping back to Chapter 1 is also useful for recalling processes such as secure sockets layer (SSL) cryptography.

The Business Value

This chapter focuses almost exclusively on non-technical concerns. The business value of PKI is fairly well understood. However, the options that SAN certificates offer to the PKI business proposition are not always clear. They are extremely powerful options that can make a significant difference in this infrastructure investment.

One of the most important business values that SAN certificates offer is in the area of certificate reuse. Simply put, you can use a single SAN certificate in a number of systems for several different tasks. Although that certificate might require a bit more of an initial investment, in the long run, the SAN certificate can usually save time and money by simplifying your IT investments and getting more mileage out of that single certificate.

Using Existing Resources

One of the best ways to examine the business resources expended on PKI certificates is to examine the various phases of certification. There are a number of ways to describe these phases. We'll use one that works from both a business and technical perspective, based on the certificate life cycle. The phases we'll examine are:

- Certificate request
- Certificate issuance
- Certificate deployment
- Certificate maintenance

For each of these phases, we'll first look at the common tasks normally completed in the phase using common, non-SAN certificates. Once we list the tasks, we'll begin to assign detailed statistics around how much of an investment the phase might be in terms of both money and time. Finally, for each phase, we'll compare using a SAN certificate and what difference the certificate would make in terms of time and cost.

> **The Difference Between Public and Private Certification Authorities**
>
> The one enormous differentiator in this process is whether your organization uses a public or private certification authority (CA) for certificates. This makes a difference in virtually every task and, therefore, in virtually every component of the cost and the business decisions.
>
> In today's IT landscape, many organizations use a combination of both public and private CAs to cover their security needs. Often, private authorities are used for lower-value transactions and authentication, while public-facing services and higher-value or higher-risk data will require a public CA's validation.
>
> For this section, we will assume that you're using a public CA; in cases where there is a significant difference that might impact a business decision, we'll compare both.

Certificate Request

Certificate request seems to many people like the easiest part of certification. You simply login to a secure Web site, provide a credit card or other payment option, and you get a certificate. Right?

Well, it's not quite that simple.

A certificate request is, technically, a set of data that is presented to a CA. The data—including a public portion of a public-private key pair, a list of object identifiers specifying key use, and other cryptographic details—is not very important for this section. What is important, however, is how those details are created. They are created by an administrator. Often the technical details are created individually without an automated or documented process. This requires a significant amount of work to do correctly.

Common Tasks

The first part of the certificate request process is very important in business value: justifying the need for a certificate. Each certificate has a significant value associated with it. Thus, before any certificate request process is begun, care must be taken to analyze whether the certificate is even required. The common terminology for this process and decision is return on investment (ROI).

When determining the ROI, the entire certificate life cycle is examined. A certificate is valid for months or years, and there is a certain amount of expenditure required to keep the certificate both valid and secure. For example, let's assume that you request a Web server end-entity certificate that contains pointers to two certificate revocation lists (CRLs) and chains to a trusted root. For the certificate to remain valid, at least two servers must always be available: one of the two CRL servers (preferably both) and the root CA. As we know, keeping a server up and functioning is a significant cost, and this setup requires the maintenance of two servers in addition to the end-entity server.

Some questions you should ask when making an ROI decision around certificate requests include:

- *Is there already a certificate that you can use for this task?* If so, use it! Get more bang for your PKI buck by reusing certificates where it makes sense and is within your established security policy.
- *Can you obtain a multi-use certificate?* If you need a new certificate, it may be cost-effective to purchase a more expensive one that can be used for many purposes in addition to the immediate one. There really are such things as Swiss Army certificates, and though they may cost a bit more, they are sometimes worth it. Just make sure that this is, again, within your established security policy.
- *What level of trust will this certificate provide?* You might need an ultra-trustworthy certificate, for example, if you're handing high-value financial transactions over the Internet. In contrast, a self-signed certificate might very well suffice for internal-only, low-impact trust situations. In general, the more trustworthy the certificate, the more it costs both initially and over time. So you should avoid using the same level of trust for all certificates unless that's a documented requirement.
- *How difficult will the issuance process be?* If you are requesting a highly trusted certificate, you might be required to provide a great deal of information during the issuance process to validate your identity. This can be a resource drain, especially in a smaller IT department where the issuance process can consume days or weeks of time and require cooperation with other departments. Carefully examine the issuance requirements for your CA and determine how much effort the process will take before you make a decision. This will also help you properly prepare for the application and issuance, which may significantly streamline the process.

Once the decision is made to obtain the certificate, the details of the certificate must be determined. That's because PKI certificates are issued when the CA digitally signs the request presented by the end-entity. Most of the information in the certificate request cannot be changed by the issuer. Thus, if it isn't correct or complete, the request must be denied so that the requestor can correct the issue and re-request the certificate.

The actual gathering of details isn't difficult. It mostly requires planning. But the planning is critical. If an inappropriate or unusable certificate is issued, you might wind up paying for it anyway.

The result of all this decision making and information gathering is a certificate request. During the creation of a certificate request, the technologists perform detailed tasks such as generate public/private key pairs, define required Key Usage parameters as numerical representations, verify connection to the CRL distribution point (CDP), and so on.

Figure 3.1 shows an example certificate request process grouped into a basic workflow.

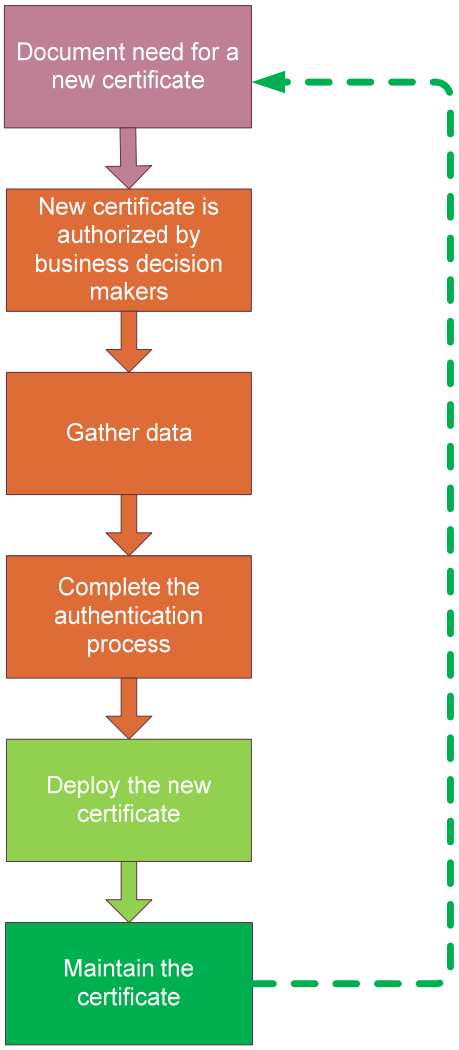

Figure 3.1: The process to obtain and deploy a new certificate.

As you can see from this workflow, the process is fairly linear. One task completes and the next begins. Very little work can be done in parallel.

The tasks that must be completed are a direct result of the business decisions made earlier. Thus, once the decision is made to create the request, there should no longer be any decisions being made.

Cost of Tasks

The cost of the certificate request process really breaks down into two main parts: making decisions and gathering information. Both of these functions can be very manpower-intensive. The costs will come in the form of a number of tasks including:

- Meetings with internal stakeholders
- Documentation creation and review
- Discussions with external vendors and consultants
- Decision maker signoffs
- Budget planning
- Data gathering and verification
- Preparing the data for presentation to the CA

There is not much in the way of money movement at this stage. The real cost is the time of your employees to get the request correct.

Analysis Paralysis

There is the notion in the business world of completely overanalyzing something to the point that no work gets done. This is often referred to as *analysis paralysis*—conducting so much analysis that the process becomes paralyzed.

During the certificate request phase, you might think that the process is encountering analysis paralysis. Do not fear. The first time this task is done properly, there is a necessary but significant time and energy investment. For example, educating decision makers on the value of PKI or examining your existing infrastructure to ensure compatibility with the certificate may require a great deal of time. However, you will see the phase become shorter and more efficient as it is used more often. Many organizations find that by the third or fourth time through this process, it is short and effective. That's because many of these tasks need to occur only once.

The best advice is to expect the first run through this process to be a bit sluggish. But you'll see a tremendous difference in even the second run.

SAN Certificate vs. Standard Certificate

In this phase of the certificate process, there's one big difference between a SAN certificate and standard certificate: cost. The cost of a SAN certificate from an external vendor is, in today's market, significantly higher than the cost of a standard single-namespace certificate. The reason is pretty apparent: you will need fewer SAN certificates because you can use them in a variety of ways compared with the traditional certificate. But it may well be worth the investment. That's why we emphasize the ROI process so strongly here.

The cost and number of additional namespaces per certificate do vary widely between vendors and over time. So part of this initial phase is to look at the cost difference between a SAN and non-SAN certificate. For example, at the time of this writing, one large PKI vendor charges an extra $500USD for a SAN certificate that supports up to 20 additional namespaces. If you used that certificate in just one additional application, you might recoup the $500 right there. And then you're free to reuse it over and over, each use driving up the return on your investment. Of course, if you have your own internally-managed PKI, there may be no cost at all to that extra SAN field.

Certificate Issuance

Once all the details of the certificate request are nailed down, it's time to get that certificate issued. This phase has less to do with technology and more to do with trust.

Common Tasks

The most obvious tasks during the certificate issuance phase are presenting the certificate request to the issuing CA and retrieving the issued certificate. Let's take a closer look at both of them, and the important piece that comes between them.

The data created in the request phase must be delivered via some secure method to the issuing CA. There are numerous methods. Secure online enrollment is the most common method today, with more rigid security methods such as overnight couriers, trusted Web sites, and physical travel being reserved for only the most critical enrollment requests. As the level of trust for the certificate request goes up, usually the method of delivering the request also becomes more secure. The reason for all this security is that if the request is intercepted between creation and presentation, it can potentially be modified to enable security compromise.

At the end of this phase, the issuing CA delivers a signed certificate to the requestor. The method for that delivery is almost always identical to the delivery method of the request itself, but because the certificate is now public, it could be delivered in a variety of ways.

Between the presentation of the request and the delivery of the response is where a great deal of process takes place. Because the issuing CA is responsible for the level of trust of every certificate it issues, it must take steps to ensure the validity of the request. That means that virtually any well-trusted CA will thoroughly analyze all certificate requests and require proof of authenticity before the certificate is issued.

Improperly Issued Certificates Can Be a Nightmare

The scrutiny that a well-trusted CA applies to certificate requests is often misunderstood by both IT professionals and business decision makers. It is seen as an unnecessary hindrance or delaying tactic. Because many businesses need immediate results from vendors, having to wait days or weeks for a certificate seems unacceptable. But this caution before issuance is very justified.

Not long ago, a large and well-trusted CA issued a new software-signing certificate to a large software publisher. The certificate was trusted by the most trustworthy certificate available. However, a few days later, the issuer noticed a discrepancy in the process. It turned out that the certificate request was bogus. It was made by someone who had no legitimate connection to the software publisher. Even worse was that this particular certificate chain did not specify a CDP, making certificate revocation exceedingly difficult and expensive.

The names have been omitted from this story, but the details are accurate. So when a well-known CA requests details about your organization or asks you to wait while they perform research prior to issuance, there is a reason they're taking so long.

One of the biggest mistakes is not building enough time into a project plan for this phase. Some issuers can take days or weeks to validate identity before the request meets the necessary requirements for issuance. There is also some cost associated with this set of events, which we'll cover in the next session.

Cost of Tasks

Writing a check or sending credit card payment to the CA is usually done at the beginning of this phase or the end of the previous one. That is a fixed and well-defined cost. Almost any PKI vendor will have the cost prominently displayed on its Web site. Their sales staff will also be happy to discuss various ways to save money, so you may wind up buying a block of certificates, some other services, etc. Because this is such a well-defined cost and it is so easy to comparison shop between vendors, we won't spend a lot of time discussing it. It would be best to spend time discussing the less obvious costs.

One cost that you will not hear about often is the cost of supporting the issuance process. As you learned in the previous section, the vendor will conform to whatever validation process they've established for the type of certificate you request. As we also discussed, the more trustworthy certificates require more thorough and exhaustive validation processes.

This is very similar to when you prove your personal identity. For example, when you go to the store to buy a bottle of wine, you're probably asked for some basic identification to ensure that you are old enough to make the purchase. The clerk just wants to see a piece of relatively trustworthy identification that shows your birth date. That's pretty much it. Compare that to when you want to obtain a passport. A passport is considered a very reliable piece of identification. As a result, the validation process is much more stringent. You might be required to provide multiple forms of trustworthy identification. The passport authority may take several days to validate the identification and might even ask you to provide further proof before the request meets their issuance requirements. Both the wine and passport requests require identification, but they have very different levels of trust associated with them.

During the validation process, a vendor may ask for a number of things that help ensure the authenticity and trustworthiness of the request. They might include:

- Tax records
- Bank account records
- Real estate records
- Lists of executive employees
- Interviews with personnel (usually IT personnel and executives)
- Inspection of the IT facilities

While responding to these requests might be a time and money investment, you should consider that they conform to the process that you agreed to during the first phase of the certification process.

On-Site Inspections

If you're using a well-known and trustworthy PKI vendor and requesting a highly-valued certificate, you may expect an on-site visit from one of their representatives at some point during the issuance phase. This isn't because they don't like you. They simply need proof of everything you've stated before they trust you with one of their certificates.

The on-site visit can be daunting for some IT personnel. They're not used to being questioned. They might see the process as harassment or a thinly-veiled insult. For example, if your operations staff shows the inspector your Web server and the inspector remarks that it is not in a secure configuration, the operations staff will likely be unhappy.

You should consider the on-site inspection as a form of audit. The inspector will almost always provide their criteria well in advance of the inspection so that your staff can prepare for the inspector and ensure a smooth visit. If there are any criteria that are not clear or unacceptable, work it out before the inspector shows up. That will help keep morale up and streamline the issuance process as well as prevent the cost of re-inspection and reconfiguration.

Another cost consideration for certificate issuance is in the actual receipt of the certificate. If your certificate vendor requires in-person delivery of an issued certificate to protect the trustworthiness of that certificate, the cost can be considerable.

You might notice a common theme throughout the details for this process: trust. Each step along this process is there to help ensure the trustworthiness of the process and the resulting certificate. Thus, while the process might seem a bit cumbersome and lengthy, when seen within the context of trust, the steps are both useful and necessary.

At the end of the certification issuance phase, you receive a signed and valid certificate. You already have the private key from the request, so the next step will be to deploy it and get it into use.

SAN Certificate vs. Standard Certificate

If you've requested a SAN certificate, the validation process might be a bit more complex. This entirely depends on the issuer and their validation requirements. For higher-value certificates, the certificate is almost always kept in a hardware security module (HSM) to provide the best level of protection and reliability. Because an HSM is a complex and highly-secure piece of technology, configuration and certificate implementation can take a significant amount of time.

When you request a SAN certificate, you probably want to store that certificate on more than one HSM to provide functionality to more than one system. Thus, you must configure each HSM individually. So, for example, if you've requested a SAN certificate with an extra four namespaces, you will probably spend time on all five of the HSMs (the one primary system and the four extra).

The math is very easy for this situation: multiply the amount of system configuration and deployment time by the number of SAN fields you've requested. The time should be a bit less as you or your staff repeat the process, but you should err on the high side.

> **Private Key Compromise**
>
> Whether you use SAN or standard certificates, when an attacker compromises the private key associated with a certificate, that certificate must be replaced. This means repeating the request, issuance, and deployment all over again. If you're using SAN certificates, you're probably using a single certificate in several places, so a single key compromise could be quite a bit of work to replace. Thus, when using SAN certificates, consider using HSMs to help protect the private key or a PKI management platform to expedite your recovery from key compromise. Also consider using multiple standard certificates to help minimize the impact of a single key breach.

Certificate Deployment

So far you've selected a CA and certificate usage, created and submitted a formal certificate request, paid some money, successfully endured a validation process, and received a signed certificate in return. Now you get to put the certificate into production!

Interestingly, deploying the certificate is one of the easiest parts of this process and, therefore, one of the least expensive. It requires relatively little investment from the business management viewpoint. There are a number of highly technical tasks to certificate deployment, but that will be covered in the next chapter.

Common Tasks

The certificate and its associated private key must be made accessible to each computer or server that will use it. In PKI-based server scenarios (for example, Web server, messaging server) that means the data must be copied to the server or installed on that server's HSM. This is usually a simple task that most IT staff is familiar with and is well documented.

The system must then be configured to use the certificate. Again, this is a relatively low-cost work item due to its simplicity and well-documented nature.

Finally, the system must be tested before it is put into production. Note that testing the proper functioning of the certificate itself is not the same as testing the entire system. The software and devices that are part of the system should be tested before the high-value certificate is loaded and used. That means that the system should be ready for the certificate to be installed so that basic tests to ensure that the new certificate works properly with the system can then be conducted. Because the system has already been tested, this phase is usually quick and easy.

Cost of Tasks

The cost of certificate deployment is very small compared with the previous two phases. Most of the investment in this phase is the time of your IT group to follow the proper (and hopefully well-documented) procedures for certificate handling. You might want to engage an outside company to test the proper operation of your systems with the new certificate or audit the proper configuration of your systems. Even this cost is relatively low, because at the time of this writing, the test and auditing functions are relatively inexpensive.

SAN Certificate vs. Standard Certificate

By definition, a SAN certificate is capable of being used on multiple domains. Thus, the cost of deploying a SAN certificate will depend on the number of systems that use the certificate. However, this should not be a significant concern because of the inexpensive nature of these tasks.

Certificate Maintenance

Once a certificate is requested, issued, and deployed, it must be maintained. This sustained-operations phase is overlooked by many IT departments. So you should understand what this phase entails and how much it costs. Although the cost may not have a huge impact on your plans, it is important nonetheless.

Common Tasks

The most important task in this phase is, ironically, the one that happens the least. Someone, or something, must keep an eye on the certificate expiration date. As you've learned in previous chapters and in other PKI-related materials, every certificate has a valid lifetime—both a beginning and ending date and time where the certificate can be trusted. The certificate lifetime is specified in the certificate request and is signed by the CA, so this window is well known to both parties. If you're using a well-trusted public CA, you will likely pay more for a certificate with a longer lifetime. But the benefit to the longer lifetime is that you can use the existing certificate for longer before it must be renewed or replaced.

If you've ever visited a Web site and gotten the following security error, you've seen an expired certificate in action:

The security certificate has expired or is not yet valid.

Figure 3.2 shows what a user might see if they're using Microsoft Internet Explorer as their browser.

Figure 3.2: An expired but otherwise valid certificate.

This is a horrible user experience and often causes users to leave a site or close down an application in fear of violating security. Even worse is that most applications do not handle invalid certificates as gracefully as Web browsers. Many simply display a generic error message or, worse, do not check the validity period at all and continue to use an invalid certificate.

Certificate renewal is very simply the CA issuing a replacement certificate with a new lifetime. This is usually done with the same key pair and often uses the existing customer verification information, making it a fast process. The process is relatively simple as it is nearly the same as the deployment process.

The other operational tasks that must be conducted after a certificate is deployed include:

- Periodic verification that the system is still using the certificate properly
- Regular verification that the CDP is accessible by client computers
- Maintenance of the key storage device (HSM), if any
- Maintenance of the security mechanisms protecting the private key

Each of these is relatively simple and low-cost but necessary to ensure proper ongoing use of the certificate.

Cost of Tasks

The cost of certificate maintenance is, as described in the previous section, relatively low. The biggest cost is when a certificate expires and needs to be replaced. This is usually a far lower cost than requesting a new certificate, and in fact, the renewal price should be specified when the original certificate price is determined.

SAN Certificate vs. Standard Certificate

There is a tremendous benefit realized in the maintenance phase when an organization is using SAN certificates. This is best illustrated in the following example.

Too Many Certificates on the Systems

A company I recently worked with was concerned about their PKI deployment. Because they did not have an accurate network or systems diagram, I created one. I was alarmed when I got to the point of documenting which PKI certificates were loaded in which systems. Apparently for redundancy, the IT staff had loaded every certificate, with its associated private key, in every system at the datacenter, regardless of whether the system even had the capacity to use the certificate (for example, Web server certificates loaded onto secure messaging servers and vice versa). Each system had 23 certificates.

On the surface, there may not appear to be much wrong with this situation. The data is less than 10Kb per certificate and private key, so there is no storage issue. And all the systems were well-patched and kept in a very secure data center, so there was little concern for security compromise.

But what happened when a certificate expired? Every system in the data center needed to have the expired certificate removed or replaced. That required a substantial investment for virtually no return. Because the certificates were issued at different times, and with different levels of trust, each renewal required individual planning and execution. Although there was an appearance of effectiveness for this configuration, there was no practical need for this redundancy.

Of course, the flip side of this point is that using a single certificate can present a single point of failure. For example, when the certificate expires, it expires on all computers simultaneously. Therefore, more care must be given to properly maintain the certificate's life cycle and security, or an automated PKI management platform must be implemented. An improperly managed SAN certificate deployment could be expensive and difficult to repair if it is allowed to fail.

If this company had used a single SAN certificate with the appropriate key usages specified in the request (via proper planning), there would not be an issue at all. That type of configuration would be far more efficient and just as, if not more, secure as a result of reduced complexity and improved efficiency. The redundancy aspect can easily be addressed with consistent, verified backups or the use of a managed HSM to ensure data protection.

Certification as a Business Driver

Why is all this work necessary? What is the value of the process and of certification in general? In a word, it's all about *trust*. Let's look at a brief example of how trust has changed over the years.

A hundred years ago, trust was very different. A person asserted their identity almost completely by a statement of "My name is Mike Danseglio." The process for validating that identity was simply asking neighbors and friends, "Is that person's name Mike Danseglio?" A great deal of trust came from appearance as well—if Mike asserted that he was a wealthy businessman, you might look at his clothes, his manner of speech, and his cleanliness to determine whether you trusted his assertion. In some cases, you might write a letter to a trusted authority in businessmen, but the response might comes months or years later and be as simple as "Yes, I know Mike. He's a great guy." This is certainly a great endorsement of Mike's reputation and honor, but it doesn't answer key questions that are part of any business decision.

There are many flaws to the historical trust process: Is this person really Mike Danseglio? Is the letter genuine? Does he have a good reputation with all business associates or just this one? Does his reputation mean he's a reliable partner? And again, because this is probably the most important question: Is this person really Mike Danseglio?

The most common way to solve these problems was for Mike to carry some form of proof of both his identity and his business reputation. For example, he might carry letters of credit from banks and wax-sealed envelopes from government officials proclaiming his identity. But because of the delayed communication of the time, verification of the data could take a very long time and the delay could often jeopardize or invalidate the business deal entirely. But this level of uncertainty was part of all business transactions. In short, trust was hard to come by and little or no trust was considered an acceptable risk in some cases.

The business world today is very different. You may have business relationships with people all over the world, many of which you never meet. Contracts and transactions execute in minutes compared with the years they took in the past. Any effective business decision maker recognizes this difference between *historical trust* and *modern trust*. It is this modern trust that we support with certification.

In today's world, trust is an essential component of all business transactions. Consider what your CEO would say if you suggested dealing with a previously unfamiliar partner based entirely on the unverifiable assertions of a single person. You'd be out of a job! Verified reputations, financial statements, and personal and company histories are all standard elements that go into modern trust. All of these elements are increasingly represented by digital data. But this data is still susceptible to modification or forgery unless some protection is provided. That's where the concept of *certification* comes in.

Certification provides the technology and infrastructure necessary to provide reliable proof of information. It allows us to securely communicate, providing authenticity, data integrity, and data non-repudiation in addition to the better-known data security benefit. These four elements are often defined in the context of certification, but the business value is not often described. In short, the values map as:

- Authenticity—The value of knowing that the person or company you're communicating with is the person or company that you believe them to be. They have proved their identity to a trusted third party, and because you trust the third party, you trust the person or company to be authentic.
- Data integrity—You can trust that when the person or company (entity) sends you data, it has not been modified or replaced en route. The data they send is the same as the data you receive.
- Data non-repudiation—There is tremendous value in proving that an entity made a specific statement or sent certain data. Non-repudiation ensures that the recipient of data can prove that the sender sent the data, usually at a specific time, to provide accountability in case the sender later claims ignorance or inaccuracy.
- Data security—The information that you exchange with the entity is secure from eavesdropping by third parties. All data between you is kept secret.

As you can see, certification is a very important element of today's business landscape. The services it provides are not optional—they are critical elements of nearly every business transaction.

Summary

The previous two chapters covered PKI and certificates in some technical detail. This chapter departed from that type of content by focusing on the business aspects of certificates, and SAN certificates in particular.

The SAN certificate can be a powerful business tool. It can save a great deal of money during the request and issuance phases, which is where the initial PKI investment is most closely scrutinized. We looked at the ROI and showed how SAN certificates have a tremendous value, especially where required for specific applications or scenarios. We also saw that the use of a SAN certificate can be efficient over time, as it is relatively easy to maintain.

In the next chapter, we will get back to the technical details by going through some typical SAN-specific PKI scenarios. Many of the sections explored in this chapter, especially planning, will be expanded upon in the next chapter so that you can take direct action to start using SAN certificates.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.