Realtime
publishers

The Shortcut Guide™ *To*

Subject Alternative Name Certificates

sponsored by

VeriSign®

Mike Danseglio

Copyright Statement

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.

This sponsored eBook is valid until June 30, 2011.

Chapter 4: Planning and Implementing a SAN-Enabled Certificate Strategy

Chapter 1 reviewed the basics of certificates, establishing definitions for certificates and related technologies and processes. With this foundation, we explored the more technical and complex topic of subject alternative name (SAN) certificates. Chapter 2 pressed on to discuss the details of a SAN certificate. This discussion included examining the appropriate public key cryptography standards (PKCS) and comparing data between SAN and non-SAN certificates. That chapter wrapped up by comparing SAN certificates to wildcard certificates to show the distinction between two somewhat similar objects.

Chapter 3 focused on the business aspects of certificates, and SAN certificates in particular. We saw how the proper use of a 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 are clearly advantageous to single-purpose certificates in many organizations. We also saw that the use of a SAN certificate is highly efficient over time, as it is easier to maintain than a large number of specialized certificates.

In this final chapter, we will get back to the technical details by going through typical SAN-specific public key infrastructure (PKI) scenarios in detail. Many of the sections in this chapter will enable you to take direct action to start using SAN certificates.

Quick Reminder About SAN Certificate Use

We've thoroughly examined the flexibility of the SAN certificate in previous chapters. As a quick reminder, a SAN certificate is a single PKI certificate that allows multiple DNS namespaces to use it for authentication and secure communications. It does so by listing the DNS namespaces in the *subject alternative name* field. For example, a company might own the following namespaces:

- www.example.com
- www.example.net
- www.new-example.com
- www.example.org
- www.newyork.example.org

Normally, a PKI certificate specifies a single namespace where it is valid. By using the subject alternative name field, a SAN certificate can be valid for all of the listed namespaces.

Aside from the subject alternative name field, a SAN certificate is identical to any other PKI certificate. It still contains the same information all other certificates contain, including public key, root certification authority (CA), key usage, and so on. Many applications that properly use PKI certificates can use a SAN certificate without any problem. However, as we'll see, an application that is specifically designed to exploit the power of SAN certificates can be very effective and efficient.

Planning for SAN Certificates

Planning a certificate strategy using SAN certificates differs significantly from a single-use certificate strategy. Before we begin to look at implementation details, we should take a brief look at how the certificate planning differs. As you'll see, the result is that plans can be greatly simplified.

Because SAN certificates are more flexible than single-instance certificates, in general, we can plan to obtain fewer certificates and use those certificates in multiple locations. For example, we can show how a company might secure its Internet-facing servers with a series of certificates in a typical PKI deployment (see Figure 4.1).

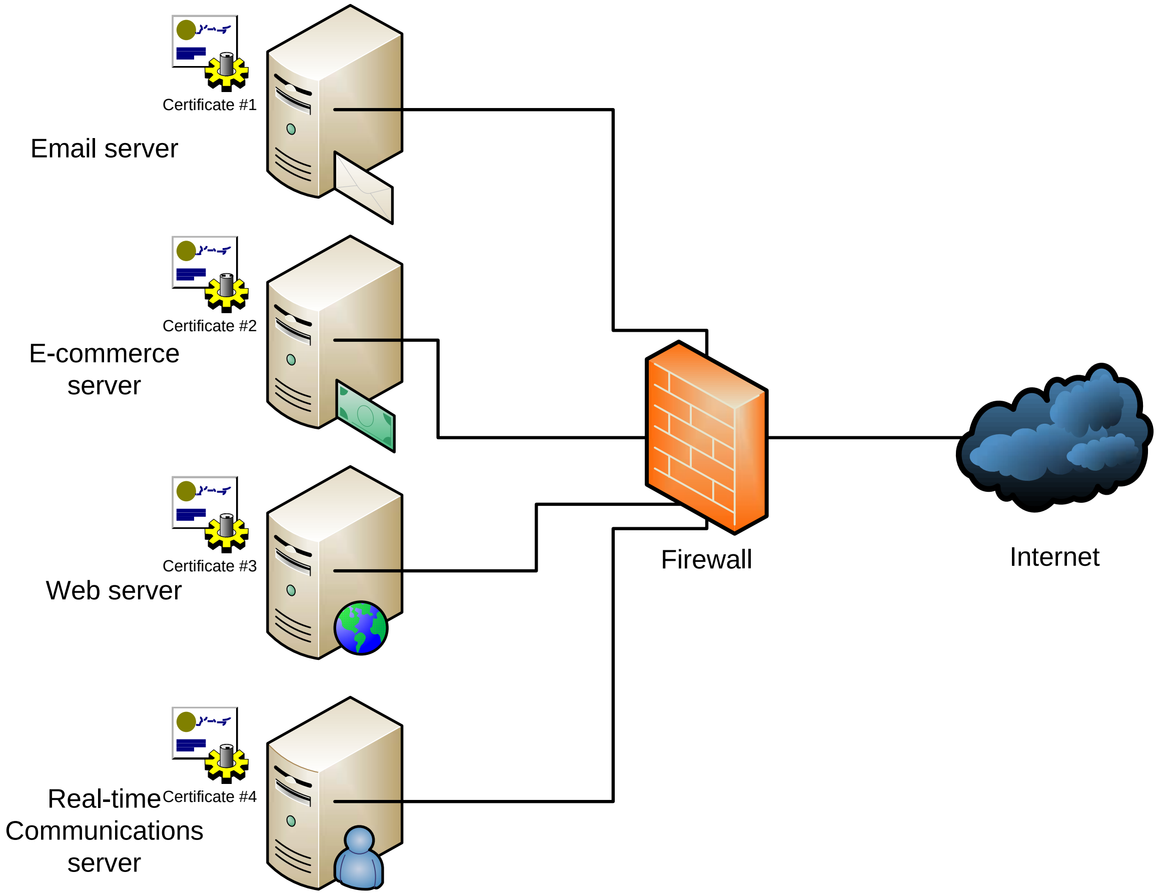

Figure 4.1: A typical Internet-facing PKI deployment.

As we can see, this deployment has four servers, one of each, that will serve as our server archetypes:

- Email server
- E-commerce server
- Web server
- Real-time Communications (RTC) server

You can see from the certificates that there are four specific certificates deployed. There is a different certificate on each system, and that certificate is unique to that server's identity and key usage. Note that for space and clarity, I have not listed each system's DNS name in the diagram; as an example, the names might conform to Table 4.1.

Server Role	Server DNS Names
Email server	Example.com Autodiscover.example.com Owa.example.com
E-commerce server	payments.example.com
Web server	www.example.com www.example.net www.example.org www.acquisition.com (an acquired company)
RTC server	Olm.example.com Rtc.example.com

Table 4.1: Example DNS names by server role.

Now let's look at the same deployment using a SAN certificate; you'll quickly see the difference.

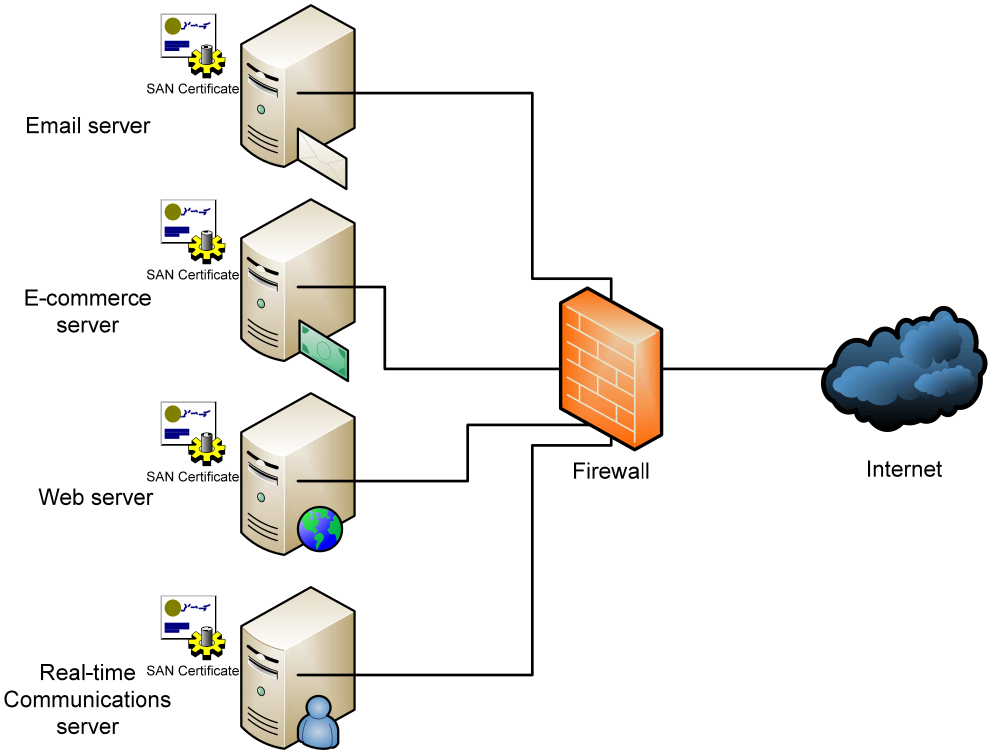

Figure 4.2: Using a single SAN certificate on multiple servers.

We're using the same certificate on all four systems. We examined the benefits of using the same certificate in multiple locations in Chapters 2 and 3, so you should recall that there are a number of reasons that this configuration is desirable.

To make this simplified configuration happen, we have to properly plan the PKI deployment. Most of the existing best practices for PKI planning apply to the use of SAN certificates. This actually makes the proper use of SAN certificates much easier. The most significant difference comes in the use of applications that either require or provide additional functionality when using a SAN certificate. Let's take a look at that planning element.

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.

Planning PKI Applications

There are dozens of categories of PKI-enabled applications, and easily hundreds of individual applications within those categories. So how do we know the best way to plan for each of them? The important aspect of planning PKI applications for SAN certificates is in understanding how each application uses PKI.

For example, let's take a look at email. Email volume, message complexity, security, reliability, and improved services and features have significantly increased over time. As a result, the load on email servers has increased. Today, very few organizations have a single email server. And most email servers and clients support PKI-centric encryption based on long-established standards and practices, such as secure sockets layer (SSL) for secure Web communications and IP Security (IPSec) for secure networking. In fact, in many organizations, the majority of certificates are usually deployed for secure communications.

More specifically, Microsoft's Exchange 2007 messaging server and Office Outlook 2007 client support SAN certificates to enable the deployment of a single, multi-use certificate in several locations. We'll look at these in more depth later in this chapter.

The crux of this section is that you need to examine each service in your organization that supports PKI and determine whether it supports SAN certificates. At the time of this writing, only a few newer applications support them despite the fact that the *subject alternative name* field has been defined for years. For example, no version of Microsoft Exchange prior to 2007 supports SAN certificates. The older versions of Exchange only looked at the *common name* portion of the *subject* field. No matter what the subject alternative name field contained, it was ignored. Thus, although you could theoretically use a SAN certificate for that application, it would certainly not work as you would expect it to.

In general, the applications that support SAN certificates are the ones where it makes good sense. As I mentioned earlier, the applications that use distributed services over a number of servers and locations are the most likely to support SAN certificates. Single-instance applications that utilize only one server for their service, such as phone switching applications or network gateways, are less likely to support multiple DNS namespaces per certificate simply because they have no need to do so.

How to Determine Whether an Application Supports SAN Certificates

You need to understand how to determine whether a given application will work properly with SAN certificates. It makes no sense to pursue a SAN certificate infrastructure if your applications will not support it. In fact, there is even the potential (albeit small) for a SAN certificate to break your existing services.

In general, there are three possible ways that an application will deal with a SAN certificate:

- The application will honor the subject alternative name and consider all names within the field valid. Thus, SAN certificates will work as expected on this application.
- The application will ignore the subject alternative name field and examine only the common name portion of the subject field to determine the valid subject name. Although a SAN certificate will work with this application, the alternative names will not work. You will still need separate certificates for separate namespaces.
- The application will consider the certificate invalid because it cannot understand or process the subject alternative name field. You will have to obtain and use a standard certificate without the SAN field.

The fastest and most authoritative method for determining which of these three ways the application will deal with a SAN certificate is to ask the software manufacturer. Check their Web site, read their documentation, or talk to a sales or technical support representative. If their application supports PKI (and if it doesn't, you're already barking up the wrong tree), they will probably understand your question and have a ready answer for you.

If the software manufacturer is unable to provide an authoritative answer, you will probably have to test it yourself. Assuming you already have the software deployed in your organization, you may be able to test the certificate in your live systems during downtime or on a hot-swap server. However, that isn't always a good approach. As a general rule, functional and compatibility tests like this should be done with offline systems to prevent any issues from affecting the production network.

A common software testing and verification method is to obtain an evaluation copy of the intended software and try out a SAN certificate on a test installation. Most large software vendors are more than happy to provide evaluation or test copies for this exact purpose. For example, Microsoft provides 120-day evaluation copies of most of its server technologies including Windows Server 2003, Windows Server 2008, Exchange Server 2007, and Office Live Communications Server.

Virtualized Testing

Most organizations are trying to do more with less these days. As a result, many dedicated test environments are being scaled back or eliminated. However, technology advances have made testing much easier with limited resources.

You've undoubtedly heard of solutions such as VMware Workstation and Microsoft's Virtual PC or Virtual Server products. These products allow you to run a virtual environment within another system at reasonable performance and system resource investments. If you're doing basic PKI testing, such as testing to ensure proper SAN certificate support, there is probably no reason to set up a large test architecture. You should be able to obtain evaluation copies of both the operating system (OS) and application, install them in a virtual environment, and test away. If you also use managed PKI or a third-party CA, you can often obtain a limited-lifetime test certificate to validate the technology before you buy the actual certificate.

Although virtual environment testing does not replace the need for full-scale testing prior to enterprise-wide deployment, it can very handily serve the purpose of validating behavior and applicability of SAN certificates.

Once you've got the test environment up and running, you should use the SAN certificate extensively to ensure that the same level of functionality exists with both a regular and a SAN certificate. Because this chapter focuses on PKI and not software testing, I will not provide an exhaustive testing methodology. There are numerous books and articles on the subject. You should use whatever methodology you find most effective for your software and your situation.

Using SAN Certificates in Your Environment

Once you've determined that your application supports the subject alternative name field of certificates, you are ready to begin planning for deployment. This process can be lengthy or short, expensive or cheap, simple or difficult. It will all depend on the plan developed prior to the deployment.

Based on my experience, few organizations will consider taking a rip-and-replace approach of replacing all existing certificates with the new SAN certificate. Unless there is a massive redeployment or some other event that requires certificate reinstallation across the systems, the new certificate will most likely be deployed to replace existing certificates as they expire. This will gradually put the single SAN certificate into use throughout the system.

The gradual replacement of certificates has several benefits:

- Making the most use of existing certificates
- Limiting exposure of the new certificate in case of compatibility issues
- Conserving IT resource expenditure by avoiding a single reengineering event

There are also several drawbacks of this approach:

- Continuing to support the complex multiple-certificate configuration
- Losing validity time of the new SAN certificate
- Missing out on potential SAN-enabled functionality of the applications

In general, you should consider the rip-and-replace strategy to replace existing certificates with the new SAN certificate if there are other factors that contribute to the need to perform operations on all servers. The factors that might cause you to conduct a rip-and-replace operation include:

- Extended server maintenance on all servers
- Broad server hardware or software upgrades
- Additional functionality added by deploying the SAN certificate
- Application intolerance of a mixed certificate environment (in other words, the application will not work unless all certificates are consistent)

If one or more of these factors applies to your environment, consider the rip-and-replace strategy. Otherwise, I recommend that you plan to replace existing certificates as they expire or as maintenance is conducted on each server.

The Danger of a Massive Certificate Deployment

On the surface, the rip-and-replace massive deployment of a new certificate seems like a great idea. Get it all over with at one time. But it can also be a dangerous venture. If your testing was not thorough, there might be deployment or compatibility issues with the new certificate. It may not work in the production systems. And without a fallback plan, you might find yourself unable to provide core services such as email and messaging. So before performing this type of deployment, ensure that you have thoroughly researched and tested the configuration and have a fallback plan of some type in case of disaster.

Example: Using SAN Certificates with Microsoft Exchange 2007

Microsoft Exchange 2007 supports PKI certificates for a variety of purposes:

- Secure email communication
- Remote procedure call (RPC) over hypertext transfer protocol (HTTP)
- Outlook Web Access (OWA)
- Various email transport protocols including SMTP and POP3

Many of these services will work with a standard certificate (assuming it is properly configured). As we've discussed, the use of multiple DNS namespaces with a single certificate is the principle benefit of a SAN certificate. With email systems in general, they are often deployed to serve more than one namespace, such as example.com, example.org, and exchange.example.com. Wildcard certificates might suffice for some of the convergent namespaces, but for a combination of .org and .com addresses, a SAN certificate is required. A wildcard certificate cannot span multiple root domain names.

There is a useful new feature in Microsoft Exchange 2007 called Autodiscover. This feature encapsulates new functionality of Exchange. It also provides a great deal of existing functionality that relies on Autodiscover. The features that require Autodiscover to work properly are:

- Auto Account Setup (a new service that provides automatic account detection and profile creation)
- Availability (the free/busy service)
- Offline Address Book (OAB)
- Out of Office
- Exchange Unified Messaging

Microsoft Exchange 2007's Autodiscover feature requires a SAN certificate to work properly. Because Exchange uses certificates for several reasons already, the only change from the PKI side is that the certificate can no longer be a standalone certificate. It must be a SAN certificate.

By default, Microsoft Exchange 2007 deploys a self-signed certificate when it is installed. The self-signed certificate can provide basic functionality for limited organizations, but it is not flexible enough for most organizations. In fact, it will not be trusted by clients by default. Adding a self-signed certificate to each client's Trusted Root Certification Authorities container can be very difficult to deploy and manage (and will not work for many types of clients). It is simply not realistic to try to do so.

As a result, you will want to remove that self-signed Exchange certificate and install a CA-issued SAN certificate that chains to a trusted root. In this configuration, you have to manage only the server-side certificate and not worry about the client configuration in most cases.

Previous Versions of Microsoft Exchange

It is worth calling out that the support for SAN certificates is new for Microsoft Exchange 2007. Previous versions did not cleanly support or require this certificate type like the current version does. Although it is possible to use SAN certificates in previous versions, it is tricky and less than optimal to do so. Thus, this section is specific in mentioning the version of Exchange repeatedly. If you're using a previous version of Exchange, this guidance does not apply.

Let's take a look at how to request a certificate from Microsoft Exchange 2007.

Requesting a SAN Certificate from Microsoft Exchange 2007

This process assumes that you already have Exchange 2007 installed. We will use functionality from the Exchange software to generate the certificate request, as other software may not properly form a SAN-enabled certificate request.

We'll use the Exchange Management Shell to create a certificate request at the command line. Although a bit cumbersome, it is the only way to ensure that the certificate request is complete and properly configured. As of the time of this writing, there is no user interface (UI) method for requesting a SAN certificate because there is no interface for adding the domain names that go in the subject alternative name field.

For this example, we will use the details provided in Table 4.2.

Field	Data
Certificate friendly name	Microsoft Exchange SAN Certificate
Primary domain name (CN)	Example.com
Secondary domain names	Autodiscover.example.com www.example.com
PKI key size	2048 bits

Subject name	C=com
	O=requestor
	CN=example.com

Mail services for certificate	IIS, POP3, SMTP
Certificate request path and file name	C:\ExchangeSANCert.txt
Issued certificate path and file name	C:\IssuedExchangeSANCert.p7b

Table 4.2: Microsoft Exchange 2007 SAN certificate request example details.

To create the request, follow these steps on the server running Exchange 2007:

1. Click **Start**, then **All Programs**, next **Microsoft Exchange Server 2007**, and then click **Exchange Management Shell**. The Exchange Management Shell command-line window will open.
2. Type the following command:

```
New-ExchangeCertificate -DomainName example.com,
autodiscover.example.com, www.example.com -FriendlyName "Microsoft
Exchange SAN Certificate" -GenerateRequest:$True -Keysize 2048 -path
c:\ExchangeSANCert.txt -PrivateKeyExportable:$true -SubjectName
"c=com, o=Requestor, CN=example.com"
```

This two-step process will result in a certificate request saved in the file **C:\ExchangeSANCert.txt**.

Installing an Issued SAN Certificate in Microsoft Exchange 2007

The next step is having the certificate issued. This is normally done by sending the saved request file to a CA (internal or external) and completing the certification process as described in Chapter 3. At the end of the process, the CA will sign and issue the certificate and most likely send a copy to you in a p7b file.

Once you have the certificate, it is a simple process to install it. Just follow these steps on the server running Exchange 2007:

1. Click **Start**, then **All Programs**, next **Microsoft Exchange Server 2007**, and then click **Exchange Management Shell**. The Exchange Management Shell command-line window will open.
2. Type this command:

```
Import-ExchangeCertificate –Path c:\IssuedExchangeSANCert.p7b |
Enable-ExchangeCertificate –Services IIS, POP, SMTP
```

This process will import the signed certificate from the p7b file back into the server. Because the server where this command is run is the same one where the certificate request was made, the private key for this certificate is already loaded and is automatically associated with the newly signed certificate. The result is a signed certificate and its associated private key both loaded into the computer.

Note

If the exported p7b file was password-protected, step 2 in the previous procedure would require the addition of the following parameter, where *password* is the password specified by the certificate issuer:

```
-Password password
```

Post-Installation Tasks

Once the certificate has been installed, the first thing you should do is conduct functional tests to ensure that the certificate works properly. For the example in this section, appropriate tests might include using PKI-enabled features by performing these user-focused tasks for each of the subject alternative name domains:

- Access a mailbox through OWA from a Web browser
- Configure a new email Microsoft Office Outlook 2007 client and confirm that Autodiscover populates the configuration
- Schedule a meeting to ensure that the Free/Busy Service is functioning

Once these tests are successfully completed, you should back up the certificate and private key. Take care to ensure you make a complete backup by testing it on another system, then store the backup in a reliable and secure location. If the backup is compromised by an attacker, the attacker will have the private key for your messaging infrastructure (and possibly much more). If the backup is lost or damaged, and your original key is also lost, the cost and difficulty in having a new certificate issued and can be significant.

Example: Using SAN Certificates with Microsoft Office Communications Server 2007

SAN certificates are required for proper operation of Microsoft Office Communications Server 2007. This isn't a matter of convenience or best practice. It actually is a requirement. With SAN certificates, the Office Communications Server 2007 environment does not work.

Compared with the Exchange processes, however, the operational processes for requesting and installing the certificates are amazingly simple. In fact, it's a wizard that comes up by default when you run the management console. The wizard generates your SAN certificate request automatically. Your only task is to send the request to the issuing CA and then install the returned certificate by double-clicking it. Really, that's all there is to it!

SAN Operation and Maintenance

SAN operation and maintenance is discussed extensively in Chapter 3. As a brief reminder, certificates require very little attention during their lifetime. For the most part, once you've installed and verified the configuration of a PKI-enabled application, it will work until one of a small number of issues occurs:

- The private key is compromised on one of your servers
- The root issuing certificate's private key is compromised
- The certificate revocation list (CRL) is compromised or is unreachable
- The certificate expires

When one of these issues occurs, you should quickly address it. The most common issue that you'll face is certificate expiration. PKI vendors understand this, and today many of them are recommending 2- to 3-year certificate validity periods to help minimize the impact of expiring certificates.

Summary

The first two chapters covered PKI and certificates in technical detail. Chapter 3 departed from that type of content by focusing on the business aspects of certificates, and SAN certificates in particular. In this chapter, we looked at applied use of the SAN certificates. We discussed various planning techniques and details, and provided specific recommendations and guidelines for which approaches are appropriate for each situation. We then explored Microsoft Exchange 2007's use of certificates in some depth and showed specifically how it can be configured with a SAN certificate.

Throughout this series, you have seen the benefits of SAN certificates. Not only are they required for a number of advanced PKI-based applications, they also simplify your IT infrastructure and can lower the cost of certificate ownership and management. Although some managed PKI vendors do charge more for SAN certificates, you now understand their value and how to calculate whether to make an investment.

Download Additional eBooks from Realtime Nexus!