

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

GIAC Securing Windows Certification
Practical Assignment v 3.2, Option 2

Implementing a Windows 2003 PKI from an Existing Windows 2000 Network

Authored by: Norman Christopher-Knight
November, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Table of Contents 2
Abstract 4
Chapter 1: Introduction 5
I. Assumptions and Expectations 5
II. Company Overview 5
III. Information Technology Infrastructure 6
IV. Public Key Infrastructure (PKI) Defined 6
V. Business and Technological Issues Driving PKI Adoption 7
i. Digital Signatures: 7
ii. Securing Communications 8
iii. Securing Data for Mobile Users 9
Chapter 2: PKI Design, Process, and Considerations 10
I. Defining Project Goals and Objectives 10
II. Defining and Identifying the Relevant Technologies and Terms 12
i. General Cryptography and Public Key Related Terms 12
ii. Microsoft Specific Cryptography and Public Key Related Terms 15
III. Decision Points: Windows 2000 Server vs. Windows Server 2003 16
i. Enhancements Indirectly Related to Public Key Infrastructure: 16
ii. Enhancements Directly Related to Public Key Infrastructure: 17
IV. Decision Points: Windows 2000 Professional vs. Windows XP Professional 20
V. Planning the Windows 2003 Active Directory Infrastructure 20
VI. Planning the Windows Server 2003 Based PKI 25
i. Certificate Policy and Practice Statements 25
ii. Installing the Root Certificate Authority 27
iii. Installing the Issuing Certificate Authorities 28
Chapter 3: PKI Implementation Details 30
I. Upgrading the Existing Windows 2000 Active Directory Domain 30
i. Verification of the Active Directory and DNS Infrastructure 30
ii. Pre-Installation Steps 31
iii. Active Directory Preparation 35
II. Installing the PKI Infrastructure 38
i. Installing the Root Certificate Authority 38
ii. Installing the Issuing Certificate Authorities: 55
iii. Locking Down the Certificate Authorities: 62
III. Certificate Management Implementation: 64
i. Implementing and Configuring a Version 2 Certificate Template 66
Chapter 4: Applications Leveraging the Public Key Infrastructure 72
I. Securing E-mail 72
i. Composing the Initial E-mail: 72
ii. Reading the Secured E-mails: 73
II. Digitally Signing a Word Document 75

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

III. Using the Encrypting File System 76

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

This paper will describe the process that one fictitious, medium-sized, organization took in deciding to move their Windows 2000 AD based domains to Windows Server 2003 and, subsequently, a 2003 based PKI. Furthermore, it will detail the steps they took to actually implement their plans.

The paper moves from overviews of relevant PKI technologies in Windows 2000, Windows XP, Windows Server 2003, and in general, to specific implementation details of the various services that the PKI will help support and secure.

After the implementation information, each of the services provided by the PKI will be tested and documented. Finally, some conclusions will be drawn. Appendices will serve to go into more detail about items that don't relate directly to the PKI technologies, but are relevant to the overall discussion.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Chapter 1: Introduction

I. Assumptions and Expectations

It is assumed that the reader has at least a moderate degree of familiarity with the general administration of Windows server environments and the terms and technologies involved as well as a basic understanding of what cryptography is.

Detailed explanations outside the scope of this paper will be referred to using Internet hyperlinks where possible.

II. Company Overview

Down the Tubes Incorporated (DTI) specializes in making and supplying toilet bowls and bathroom accessories. It is the 2nd largest supplier in North America and is trying to expand to other potential markets in Europe and Asia in the future. The company is headquartered in Calgary, Alberta, Canada and has offices in Vancouver, Toronto, and Houston (to have a presence in the lucrative U.S. market). Additionally, they currently own a manufacturing plant just outside Sao Paulo, Brazil. The organization was founded approximately 10 years ago in 1993. They have seen the most significant growth over the course of the last 6 years as they went from approximately 250 people in 1997 to over 1500 by 2003.

Much of DTI's growth can be attributed to the company becoming increasingly better at differentiating itself by incorporating innovative technologies into their wares. Several of their toilets, for example, have luxury features (very popular in executive bathrooms across corporate North America) incorporated into them such as heated seats, emergency lighting in case of power failure, etc. They, like many companies, have tried to embrace computer technologies and include them in their products as well. Certain models have an environmentally friendly feature which can automatically adjust the flow of water used for flushing by analyzing data from sensors within the bowl. DTI technicians can get diagnostic information using Bluetooth enabled PDA's or even over the Internet for more effective troubleshooting.

In addition to their core business of toilets, DTI also offers accessories that complement their merchandise or can be sold separately. These items include bathroom shelving units, scales, brushes, etc. This side of the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

business has grown to amount to just over 30% of their revenues and it is continuing to increase in significance.

III. Information Technology Infrastructure

The computer, network, and other technologies that DTI employs are managed by their Information Technology and Communications (ITC) group. The ITC has a wide range of responsibilities including the following:

- Desktops computers and laptops
- Servers
- Network infrastructure and equipment
- Phone system
- Printers and photocopiers

The core management and technical teams in the ITC group reside in Calgary office with smaller support groups located in the other offices and the Sao Paulo plant. Responsibility for network design, build standards, etc. all come from the Calgary group.

DTI has always managed to stay relatively current with modern technologies. Their approach to technological adoption is best described as moderately conservative. Typically, the ITC group will evaluate technology that it sees as being able to add value to the business with the intention that it will not be adopted wholesale until it has been in the market place for approximately 6 or more months. Following that pace, the ITC group had Windows 2000 deployed to over 90% of its servers, and over 75% of its desktops by second quarter of 2001.

Currently, DTI has a Windows 2000, Active Directory based domain infrastructure running in native mode. All of their servers have been updated to Service Pack 4 and the latest patches up to and including the patch described in Microsoft Security Bulletin MS03-039. They have also been a Microsoft Exchange shop and have been running the various versions since Exchange 5.0. The most recent Exchange version they are running is 2000 with SP3 and the latest hotfix rollup installed.

The ITC Desktop group is currently underway in a project to migrate their user's desktops to Windows XP from Windows 2000 Professional

IV. Public Key Infrastructure (PKI) Defined

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

It is important at this point to provide a very high level definition of what a PKI is. In essence it describes implementing an electronic infrastructure by which the identity of individuals and devices (such as computers, routers, etc.) can be verified by means of verifying credentials presented in the form of an electronic certificate to an authority or authorities trusted by multiple parties.

The certificate contains an entities' public key (the public key in PKI) which is closely related to another mechanism called a private key. Information encrypted or signed with one of the keys can only be verified or decrypted using the other.

In the case of DTI, they wish to implement a system on their network, leveraging functionality built into Windows Server 2003 and Windows 2000 and XP that will allow the ITC group to act as the trusted authority and distribute certificates to their users for reasons described next.

V. Business and Technological Issues Driving PKI Adoption

Although, over the last several years, the Information Technology and Communications (ITC) Group have identified the growing need for a PKI, resources are only now being made available for this project to become a reality. Upper management finally decided to provide budget for implementing a PKI after several key corporate executives read alarming articles on digital security in glossy, in-flight magazines, and their children's copies of PC Magazine. In light of the new found attention that security was receiving from upper management, the ITC group seized the opportunity to present the idea of the PKI implementation again.

The ITC group decided that, before entering the detailed design phase of the project or examining their options, they needed to identify the business and technological factors which would allow them to bring value to the company with this project. They identified the following:

i. Digital Signatures:

The ITC group has identified two specific scenarios in which digital signatures can be used.

1. Document Security: Currently, documents authorized by corporate officers and anyone else that need to provide a signature are still using paper based methods. As the company has grown over the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

last 6 years, various corporate services departments have begun experiencing difficulties in managing the voluminous amounts of paper that have been generated. The feeling now corporately is this would all be better managed via electronic means. Previous initiatives to move forms and other key documents to an exclusively electronic format have failed because of the need for key signatures.

2. Digital Signing of E-mail: It is almost mind numbing to consider how much business is conducted via e-mail in today's business and technological environment. DTI's corporate executives and sales force especially rely heavily on the flow of e-mail and often give and receive important business directives using the medium. ITC wants some way to minimize the risk of someone "spoofing" an e-mail from an important company officer. Such an event could have some negative, and far reaching consequences.

ii. Securing Communications

This is a critical consideration for the company. Currently, many systems have been implemented but not with complete security in mind. The ITC group recently appointed a new Chief Security Officer that has been extremely focused on mitigating the risks associated with inadequate security behind the firewall in addition to in front of it. The "Chief", as she is known, is well aware of the fact that most security vulnerabilities come from corporate insiders. That said; she is focused on improving the security of the communications on both sides of the firewall.

The ITC project team identified several areas under this particular security category that could benefit from the additional security provided by the implementation of a PKI corporately. They are as follows:

1. Administrative Network Communications: Network and System Administrators connecting to servers, routers, or other network devices for which they are responsible use a variety of tools to maintain them. Many of these tools were never designed with security in mind and pass credentials and other data in clear text over the network. ITC has implemented some security like restricting which workstations can access network devices such as routers.
2. Confidential Data Protection: Securing data classified as confidential in transit between authorized workstations and the appropriate servers can be as important as the security once the data has been stored at its final destination.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

iii. Securing Data for Mobile Users

As previously discussed, DTI has a significant number of mobile users that often take their laptops and other mobile devices to many locations within DTI owned offices, partner or client offices, and various public places. The requirement for mobility often necessitates storing what is often sensitive or confidential data on the mobile devices themselves.

In the highly competitive bathroom fixture and accessory industry, losing any intellectual property can have extremely negative effects on the company bottom line should a competitor get a hold of designs, confidential sales information, etc. It was clear to the ITC group that data security is a major factor in any decisions that they make regarding the implementation of a PKI.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Chapter 2: PKI Design, Process, and Considerations

I. Defining Project Goals and Objectives

The ITC group realized that, in order to deploy a "successful" PKI implementation, they had a significant amount of up front planning and research to do. They also realized that the project had the potential to be incredibly complex and that they would have to break it down into very small and more manageable elements to get the job done.

One of the first required elements was to define the goals and objectives for the project in the first place. In other words, they needed to determine what constituted a "successful" implementation.

Listed below are the objectives that they determined were most important in working towards the completion of the project. All of them are on some level closely tied to the others.

1. **Corporate Buy-in:** As with many information technology projects that have the potential to make some changes in the processes within a company, support from management on down the hierarchy is key. Without it, processes cannot be altered to incorporate new technologies in an effective manner nor will adequate resources, financial or otherwise, be available. For example, the digital signing of documents can, in the long run streamline the flow of documents within the organization. If users and management are not properly educated as to the pros and cons of the technology, they may go back to more "tried and true" methods.

2. **Perception Management:** During meetings held within the ITC group, some of the senior people with more experience in managing IT projects raised the issue of what they termed Perception Management. They defined it as communicating with the user and management community in such a way that it was clear to everyone, at least on a high level, the benefits and limitations of the PKI implementation and the business drivers for the project.

3. **Addressing the Business Issues:** As technology professionals, everyone on the team was conscious of the potential for getting carried away in the excitement of implementing new technology. The team wanted to be certain that no technology was implemented that was looking for a solution. In other words, any technology implemented shouldn't complicate the network environment needlessly and could be

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

justified from a cost or other business perspective. More specifically, any PKI technology that was used in the project should address one or more of DTI's issues (business and/or technical) that had been defined earlier.

4. **Manageability:** The end product of the project needed to be a PKI environment that could be rolled out and managed with relative ease from an ITC perspective. As with any technology, if a PKI is too difficult to manage, the full benefits of it will not be realized as many features simply will not be used. Difficulties in control can often strain IT department's human and financial resources.

5. **Transparency/Ease of Use:** It is a virtual certainty that if end users have to go through complicated procedures in order to get their certificates, digitally sign documents or e-mail's, etc., the buy-in discussed earlier will not happen and the technology will not be used. In short, the technology should complement, not complicate business activities.

6. **Cost Effectiveness:** While there are a number of justifiable reasons for implementing a PKI, consideration must always be given to keeping costs under control. There is a broad spectrum of both hardware and software related to a PKI on which an organization can spend its money. It is highly dependent on the company and its goals what combination will provide the most benefit for a reasonable cost.

7. **Limit the Initial Scope:** The project team, in performing their initial high level research, quickly realized that it would weaken the overall success if too many applications of the technology were attempted initially. They decided that they should focus on two or three core applications of the technology but design the PKI such that it could be expanded to others easily once ITC and the user community had many months or years of experience with the implementation. No amount of planning and testing can flush out all of the details like using a technology in a production environment everyday.

   There were three technologies that they decided early on to test.
   - **Digital signing of documents:** One of the major hurdles that have been restricting the use of electronic forms in the organization is the need for the ability to securely sign documents.
   - **Secure E-mail:** Which includes both digital signing and encryption.
   - **Encrypting File System:** The management of user encryption keys and the keys of recovery agents is much easier with a centrally managed PKI.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

II. Defining and Identifying the Relevant Technologies and Terms

Once the goals of the project were established, there was now a need to identify the specific PKI technologies that would address the business and technological drivers for the project that they defined earlier.

Many terms were reviewed in order for the PKI project team to be "on the same page" as everyone else when planning the roll out of this sweeping technology.

i. General Cryptography and Public Key Related Terms

1. **Cryptography:** PKI is based upon cryptographic techniques, so a somewhat formal definition of what exactly that means is required. Cryptography involves taking something that would be in normal readable text (referred to as plaintext) and converting it into coded text (also referred to as ciphertext). In order for someone to make sense of the ciphertext again, they must have the proper key in order to decrypt (decode) the text back into plaintext.

2. **Encryption Algorithm:** A method or mathematical formula for using a key or keys to encrypt plaintext data into ciphertext.

3. **Key:** A number based upon the binary system that is used to encrypt and/or decrypt the ciphertext. An mathematical algorithm of some sort using the key performs the actual encryption of the plaintext information. The number is generally referred by the number of bits it contains. The more bits in the key, the larger the number of possible combinations of zeros and ones if someone were to use a computer to try every combination until the right one was found. The more bits a key contains, the stronger it is said to be.

   For example a 128 bit key is far stronger than a 40 bit key. The reason is that the number of possible combinations increases by a power of 2 each time a bit is added.

   A 40 bit key would have 2^{40} = 1,099,511,627,776 different combinations. By contrast a 128 bit key would have 2^{128} = 3.4028 x 10^{38}.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4. **Secret Key:** This refers to a key that is used to both encrypt and decrypt plaintext into ciphertext. In the context of encrypted communications between two parties, the person(s) initiating the message would encrypt it using a particular key. The recipient on the other end would have to be aware of the exact key that was used in the first place in order to decrypt the message.

5. **Public and Private Keys:** Another method of encrypting plaintext is to use a set of two keys that are mathematically related to one another, but that you could not derive simply by knowing one of them and/or having the ciphertext. One key is kept private to the key holder while the public key is, naturally, public knowledge. Items encrypted by the public key can only be opened by the individual using the private key.

   This type of cryptography is leveraged in a Public Key Infrastructure and, more specifically, certificates used in a PKI.

6. **Hashing Function:** A mathematical technique which, when applied against a plaintext input, produces "a string of characters into a usually shorter fixed-length value or key which represents the original string". [1] This string is sometimes referred to as a message digest.

   Hashing is different from an encryption algorithm in that it is a one way operation. You do not "decrypt" the message digest in order to come up with the original text. Instead, hashes are often used as a means to verify whether or not some amount of data has changed. To provide an oversimplified example, if someone were to send a message and include the hash and disclose what hashing function was applied, the recipient should be able to apply the same function against the text he/she receives. If it is exactly the same as the included hash, then you know the message has not been altered in some way.

7. **Digital Signature:** An electronic means of asserting that a digital document, program, etc. was actually sent from a particular entity and that it was not modified on the way to the recipient. A hash of the message is encrypted with the sender's private key. The recipient on the other end of a communication can decrypt the message digest and then use the same hashing algorithm to on the message received to determine if it matches the encrypted hash or not.

   The fact that the hash could be decrypted using the public key is indicative of the message coming from the supposed sender. Applying

[1] "SearchDatabase.com Definitions." Hashing. March 12, 2002.
URL: http://searchdatabase.techtarget.com/sDefinition/0,,sid13_gci212230,00.html (November 5, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the hash algorithm against the message is the part of process that verifies its integrity.

8. **Secure Key Exchange:** This is an important concept in the world of cryptography and communications. Two entities needing to communicate using some kind of encryption algorithm generally need to be able to pass the keys they will use for their session (often called a session key) in a way that they cannot be intercepted in transit. Typically this involves the initiating end of the communication encrypting the session key with the recipients public key and sending it. The recipient then decrypts the session key with its private key and then communications can begin. Session keys (which are secret keys) are used often for performance reasons in digital communications.

9. **Certificate:** A certificate is a digital construct that combines an entity's public key with other information that represents or authenticates that entity. The term entity simply refers to the fact that a certificate can be used to represent a human being, a computer, router, company, etc.

   The certificate includes the digital signature of a higher authority (not God) called a certificate authority (CA). The presence of the CA's certificate helps validate the fact that the certificate is representative of the entity it's supposed to.

10. **Certificate Authority (CA):** A certificate authority or CA is an entity that is trusted to issue certificates to other entities. In other words, it is trusted to verify the identity of a person or thing and distribute a certificate to them accordingly also generating public and private keys for them. For example, if a certificate is presented as being for Bob Smith, the fact that it is digitally signed by the CA indicates that it indeed represents Bob Smith.

    Multiple certificate authorities can be used to form a trust hierarchy in which one CA acts as the top of the hierarchy (the root CA) and CAs lower in the chain trust it. They in turn can issue certificates to other CAs lower in the trust chain, to individual people or computers and other devices.

11. **Certificate Revocation List (CRL):** Over time and for various reasons, certificates representing someone's identity may become invalid. An employee may no longer work for a company and therefore should no longer be associated with the company CA in any way. CAs maintain lists of revoked certificates. Anyone attempting to validation a certificate needs to be able to check against this list. This list is, fittingly, called a Certificate Revocation List (CRL). The location of the CRL is included in a CAs certificate. This location is referred to as the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CRL distribution point or CDP. The CDP can be a file location, URL or Active Directory in the case of Microsoft Windows.

12. **Authority Information Access (AIA):** Validating an entity's certificate requires that the certificate of the CA which issued the certificate be examined as well. If the CA itself has an expired certificate or is not trusted, that will invalidate any certificates that have purportedly by issued by it. The information as to where a copy of the CAs certificate can be found is included in its certificate which, in turn, is included in certificates issued by it. This field is called the Authority Information Access or AIA. Like CRLs, it can be a file location, URL, or AD reference.

ii. Microsoft Specific Cryptography and Public Key Related Terms

Microsoft, as per usual, has their own terminology for a number of items related to their implementation of a public key infrastructure. The good thing is that, for the most part, it is consistent between Windows 2000 and Windows 2003. What follows is a brief primer on some of the terms and technologies that the ITC encountered while researching this project.

1. **CryptoAPI:** CryptoAPI is an application programming interface specific to Microsoft Windows that allows applications (third party or Microsoft) to take advantage of various cryptographic functions provided by CSPs or cryptographic service providers.

2. **Cryptographic Service Provider (CSP):** These are either hardware or software modules that provide core cryptographic functions such as supporting particular encryption algorithms or devices such as smart cards. Again these can be programmatically accessed by using the CryptoAPI interfaces.

3. **Stand-Alone Certificate Authority:** This refers to a Windows 2000 or Windows 2003 based server running Certificate Services that does not leverage the Active Directory and does not even have to be installed on a server which is a member of a domain. There are two types of these CAs

    a. **Stand-Alone Root Certificate Authority:** A stand-alone CA not integrated with AD that will self sign its own certificate and is intended to act as the root in a CA trust hierarchy.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

b. **Stand-Alone Subordinate Certificate Authority:** A stand-alone CA that will have it's CA certificate issued by another CA higher in the trust hierarchy.

4. **Enterprise Certificate Authority:** These types of CAs must be members of an Active Directory domain and are fully integrated with it. They too are Windows 2000 or 2003 servers running Certificate Services. Similar to the stand-alone CAs, there are two types of enterprise CAs.
   a. **Enterprise Root Certificate Authority:** An enterprise CA that will self sign its own CA certificate and act as the root of the trust hierarchy.
   b. **Enterprise Subordinate Certificate Authority:** An enterprise CA that will get it's CA certificate from a CA higher in the trust hierarchy.

5. **Certificate Template:** Starting with Windows 2000, Microsoft based certificate authorities could use what are known as templates. These templates can only be used with enterprise CAs as they are stored in the Active Directory. They define what kind of certificates can be issued by an enterprise CA and specific properties of the templates such as their purpose, encryption key lengths, etc. Windows 2003 makes significant changes to what can be done with templates.

III. Decision Points: Windows 2000 Server vs. Windows Server 2003

The ITC group had a number of reasons in deciding to migrate their servers to Windows Server 2003 that extended beyond the PKI project. That said; there were additional reasons that they decided to wait until they had rolled out 2003 to all domain controllers and upgraded their domain to Windows 2003 functionality before moving ahead.

The following is a description of the direct and indirect reasons why ITC decided to follow the path that it did.

i. Enhancements Indirectly Related to Public Key Infrastructure:

Windows 2003 includes some enhancements to security which, in the long run will make the job of the server administrators easier whether they are managing a certificate authority or not. Some of these include:

1. **Secure by Default:** This Microsoft catch phrase simply refers to the fact that in a default install of Windows Server 2003

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

permissions, generally speaking are much more restrictive than a Windows 2000 default installation. NTFS file and share permissions are set to the Everyone group having read permissions instead of full control for one important instance of this new security posture.

Many services are not installed by default or are more locked down if they are. The most notable example is Internet Information Services (IIS). Windows 2000 installed it by default with most of its components such as dynamic web pages. This left many people, experienced administrators or not vulnerable to numerous exploits that took advantage of the lax default security. 2003 does not install IIS by default and, when it is installed, it can only server dynamic web pages.

2. **Active Directory Improvements:** There have been a number of small improvements to AD that make it easier to manage than 2000. There are some performance improvements over slow links for example. More important to the ITC team was the ability for AD in 2003 to replicate data between domain partitions. Particularly DNS information. In Windows 2000, DNS information integrated with AD would only replicate between domain controllers (DCs) in the same domain. Setting up name resolution for other AD domains involved setting up zone transfers and forwarders for the right servers. In 2003, once a zone is set up, it can replicate throughout the entire forest reducing the complexity of the DNS structure which is critical to AD and therefore critical to the PKI project.

3. **Group Policy Management:** In Windows 2000, group policy (GP) was a major advance but difficult to manage in large environments. It was challenging to determine exactly what the effects of a GP change at one point in the AD hierarchy of organizational units would have on users and computers further down or at other points where the policy was linked. 2003 includes resultant set of policy (RSoP) features that allow administrators to model what will happen in the effect of a change or to better determine the effects of an existing change. Group policy is important to the PKI project.

ii. **Enhancements Directly Related to Public Key Infrastructure:**

Windows 2003 introduces a number of enhancements to the public key infrastructure technologies that were present in Windows 2000.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

These improvements will make it far easier for the ITC group to implement and manage the PKI over time.

1. **User Auto-Enrollment:** In Windows 2000 computers could be automatically enrolled for certificates that would be used for things such as SSL enabled intranet web sites, etc. Users had to be manually enrolled either by administrators or by sending them to web enrollment pages which, even if they were provided with instructions, would inevitably lead to mistakes in chosing the right options, etc.

   Windows 2003 builds on the auto-enrollment functionality by allowing users to auto-enroll. Furthermore, they can be automatically request and be issued a certificate or the certificate requests can be approved by an administrator. Users can be enrolled for certificates based on ACLs of existing AD groups. This is the number one feature that caught the attention of PKI project members doing their initial research.

2. **Version 2 Certificate Templates:** The user auto-enrollment functionality is made possible primarily by the use of version 2 templates. In fact, auto-enrollment will not work without them. These can be modified in numerous ways to fit the needs of the organization. The key length, certificate purpose, validity and renewal purposes, issuance requirements, etc can be modified as needed.

   Certificate templates in a Windows 2000 environment by contrast could not be modified. There was a fixed number of them for specific purposes. New version 2 templates can be created as needed. Additionally, old certificates can be automatically superceded by version 2 templates.

3. **Key Recovery and Archiving:** The only data recovery features of the Windows 2000 PKI was the encrypting file system (EFS) recovery agent for recovering encrypted data on NTFS volumes. Archiving user or computer private keys was not possible. Windows 2003 on the other hand does allow this possibility when used in conjunction with version 2 templates. Under carefully secured conditions, this can reduce the possibility that data may become irrevocably lost if a user loses their private key or leaves the company and there is encrypted data.

   This feature also negates the need to have an Exchange 2000 Key Management Server (KMS) which essentially provided the same service for secure e-mail purposes. Windows 2003 will allow all

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PKI related activities to be more centrally managed in a common infrastructure.

4. **Delta Certificate Revocation Lists:** This term described CRLs that contain only the changes in revoked certificates since the last full CRL publication. Since many workers can come and go from DTI over time, this feature was another key differentiator for the ITC PKI project members. It will allow clients to be able to download and cache much smaller CRLs which can be published more frequently as a result of their smaller size. Only Windows XP and 2003 computers can recognize and work with delta CRLs.

5. **Qualified Subordination:** Although ITC did not envision initially taking advantage of this feature, they possibly could in the future. This capability allows a parent CA to restrict exactly what a subordinate CA can do. Name constraints, which "restrict the valid range of names permitted or excluded by the CA and its subordinates"[2] are one example of the possible restrictions. Others include limiting the length of the trust hierarchy path (basic constraints) and application policies which determine what certificates can be used for.

6. **Command Line Support:** Certutil, a command line tool which can perform most functions done through the Certification Authority Microsoft Management Console (MMC) snap-in, and many that it can't, exists in Windows 2000. Functionality from the DSSTORE utility has been incorporated into the tool as well. Previously DSSTORE, only available in the Windows 2000 Resource Kit tools, was needed to publish stand-alone CA information into AD. Now, this can be done using the certutil –dspublish command.

   Many other tools, previously unsupported and available only in Resource Kits, have been included with the operating system and fully supported. See the command line help for more information.

[2] Cross, David"PKI Enhancements in Windows XP Professional and Windows Server 2003." Qualified Subordination. July , 2001.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/Plan/PKIEnh.asp (November 4, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

IV. Decision Points: Windows 2000 Professional vs. Windows XP Professional

It was clear early on that Windows XP would be the preferred platform to be able to provide DTI's users with a easily managed and used PKI. In typical Microsoft fashion, the more compelling features of Windows 2003's PKI are only, or best, supported by Windows XP as a desktop OS. The deciding factors are below.

1. **Certificate Auto-enrollment:** Users can only auto-enroll and take advantage of the other automatic features afforded by the use of version 2 templates if Windows XP is used on the client or they are logging on to a Windows Server 2003 system which is unlikely (unless it is a Terminal Server). Windows 2000 users, if need be, can obtain a version 2 based template by using the web enrollment pages in Certificate Services.

2. **Encrypting File System Enhancements:** EFS was first introduced with Windows 2000 and made the process of encrypting a file as simple as selecting an attribute checkbox. That said, XP makes a number of improvements to EFS that had been on the wish list of Windows 2000 users of the technology.

   First of all, the Offline files cache can now be encrypted. Offline files is a technology that allows a user to locally cache server based files and keep them in synch. This is very useful for laptop users who are often mobile and disconnected from the network. If the laptop is lost or stolen, potentially sensitive data can be protected.

   Multiple users can now be added so that an encrypted file can be accessed by them as well. One thing to keep in mind is that only individual users, not groups, can be added.

3. **Delta Certificate Revocation Lists:** Only Windows XP and 2003 systems can recognize and use delta CRLs. Being able to use the deltas can allow for more frequent CRL publishing and a reduced chance that a certificate will be taken to be valid when, in fact, it is not.

V. Planning the Windows 2003 Active Directory Infrastructure

Planned Windows network infrastructure in this context indicates any changes or additions to the Windows server design and Active Directory infrastructure to implement and accommodate the PKI project.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In order to take advantage of many of the 2003 features, ITC knew they would first need to implement 2003 domain controllers in the forest. Many of the features new to 2003 such as V2 templates, delta CRLs, etc are most useful or are only available in a fully 2003 based domain. Additionally, there are DNS changes which could help the overall AD infrastructure such as the ability to replicate DNS zones (in AD integrated DNS zones) to every domain controller in the forest.

It was clear that the ITC group wanted to completely roll out Windows Server 2003 to their AD infrastructure before going forward with the rest of their plans for the PKI. More accurately, they needed to replace the Windows 2000 DCs with 2003 DCs and raise the forest functional level (described later) to the Windows Server 2003 level. What follows is an overview of their plans.

1. **Verify DNS Infrastructure and Active Directory Replication Stability:** The first thing to be done prior to attempting any actions with the existing AD implementation is to verify that:
    a. DNS is functioning properly company wide and all registrations for all domain controllers exist.
    b. That replication is functioning properly across the enterprise. Any schema or domain changes need to be able to reach all domain controllers.
    c. Group policies are consistent and replicated everywhere they need to be.

    There are a number of changes that occur to the AD infrastructure upon adding a Windows 2003 domain controller into the forest. That said, before embarking on any project that makes changes to the forest schema, adds groups, or in any other way, relies on or manipulates AD, it is always wise to verify that there are no replication, DNS, group policy, or other problems before making the changes. You can then be assured that all the necessary information will available to all sites in the enterprise.

2. **Verify that all of the Windows 2000 domain controllers in the existing AD environment are running a minimum of Service Pack 4:** There are a few important factors of note with this particular requirement.
    a. Microsoft recommends installing at least Service Pack 3 on all Windows 2000 DCs that will participate in a domain with Windows 2003 DCs.[3] There are a number of updates that avoid some potentially serious replication issues. Microsoft Knowledge Base article 331161 discusses this issue in depth and is available at the

[3] "How to Upgrade Windows 2000 Domain Controllers to Windows Server 2003." Microsoft Knowledge Base 325379. July 30th, 2003. http://support.microsoft.com/default.aspx?scid=kb;en-us;325379&Product=exch2k (November 2, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

following URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;331161

b. The Windows 2003 admin tools by default sign and encrypt all of the LDAP traffic they generate.[4] See Microsoft Knowledge Base article 325465 for more information. The URL is: http://support.microsoft.com/default.aspx?kbid=325465

c. The most obvious reason for implementing the latest service pack is to gain the benefits of all the included bug and security fixes.

3. **Backup up all existing Windows 2000 DCs:** More specifically, the system state which, on domain controllers, includes the AD database and log files.

4. **Update the Secretary, houseIdentifier, and labeledURI Attributes:** This is an extremely important step as DTI has been running Exchange 2000 in its AD environment. Exchange introduces non RFC (2798) compliant versions of these attributes that can result in what are known as "mangled" attributes.[5] Essentially, some conflicts can occur between the existing attributes and the ones that would be introduced as a result of running ADprep /forestprep (described later). Exchange 2000 uses the same LDAPDisplayName as the ones defined for the LDAP InetOrgPerson object class described in RFC 2798. For more information regarding the InetOrgPerson, read RFC 2798 from the Internet Engineering Task Force (IETF) website at http://www.ietf.org/rfc/rfc2798.txt?number=2798.

   The Microsoft Knowledge Base articles 314649 and 325379 describe a method of using an LDIFDE file to update these attributes prior to running ADprep /forestprep and avoiding the mangled attribute problem. Alternatively, these attributes can also be modified by using the ADSI Edit utility from the Windows Support Tools.

5. **Prepare the Existing Windows 2000 Forest and Domains:** Windows 2003 introduces some changes to the AD schema. Additionally, once these changes are introduced, certain AD objects and their associated security descriptors must also be updated.

   These tasks are carried out using the ADprep tool. As its name implies, this command line tool, located in the i386 directory of the Windows 2003 installation media, prepares the AD forest and each of the domains with

[4] "Windows 2000 Domain Controllers Require SP3 or Later When Using Windows Server 2003 Administration Tool." Microsoft Knowledge Base 325465. September 22nd, 2003. http://support.microsoft.com/default.aspx?kbid=325465 (November 2, 2003)

[5] "Windows Server 2003 ADPREP Command Causes Mangled Attributes in Windows 2000 Forests That Contain Exchange 2000 Servers." Microsoft Knowledge Base 314649. July 1st, 2003. http://support.microsoft.com/?ID=314649 (November 2, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the necessary changes to properly introduce Windows 2003 domain controllers. There are two commands that should be run in the following order.

a. **ADprep /forestprep:** It updates the existing Windows 2000 AD schema with the Windows 2003 version (from version 13 to version 30 [6]). The following requirements must be met in order to be able to run this tool and update the schema.

- This command must be run from the AD forest's schema master. The schema master is a forest specific role in which only one server can be used to update the AD schema
- The user running the command must a member of Schema Admins group.
- The user must also be a member of the Enterprise Admins group.

All schema changes should be replicated throughout the entire forest before proceeding to the next step. The ITC group will most likely implement this change over a weekend and allow 2 to 3 days before attempting the next step. This will ensure all necessary replication has taken place.

In addition to extending the schema, the forestprep command also adjusts security descriptors in the configuration container and creates some new objects and attributes there as well.[7] This is mainly for enabling some new functionality for the Resultant Set of Policy (RSoP) tool. It allows an administrator to see actual group policy results detailing which settings were inherited from specific group policy objects or what-if analysis.

b. **ADprep /domainprep:** This tool updates AD objects and their associated access control entries (ACEs) for each domain in which it is run. This command should be run in each domain in the forest into which Windows 2003 DCs will be introduced. The following are requirements that must be met in order to be able to execute and complete this command.

- The changes introduced by the ADprep /forestprep command must have been run and fully replicated throughout the forest.

[6] Deuby, Sean. "Windows Server 2003 Command Line Utilities" Windows & .NET Magazine April 2003 (2003): 81- 82.

[7] "Microsoft Windows 2000: Upgrading Domains to .NET Server." Microsoft Support Webcasts. February 18th, 2003.
URL: http://support.microsoft.com/default.aspx?scid=/servicedesks/webcasts/en/wc021803/wct021803.asp (November 17, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- This command should be run from the server serving as the Infrastructure master in each domain. The Infrastructure Master manages object references across domains.8
- The user running the command must a member of the Domain Admins group for the domain or the Enterprise Admins group.

  The domainprep switch adds new security descriptors to the content in the SYSVOL and to objects in the domain naming context. These changes allow the Enterprise Domain Controllers group to be able to read group policies in any domain in the forest. Again, this is for RSoP processing.

6. **Replace all Windows 2000 Domain Controllers with Windows Server 2003 Domain Controllers:** Normally, the ITC group avoids doing operating system upgrades in place (installing new operating systems over existing ones on servers or workstations). This is especially true of server operating systems. The rationale for this is that you can avoid a number of potentially undesirable consequences of upgrading.
   a. Often applications that were once installed on a system leave remnants of the software installation despite having an uninstall program. This can include files, registry changes, permissions changes, etc. By doing a clean installation, you do not have to be concerned about what was once on the system.
   b. You avoid bringing forward any potentially insecure settings. These include settings on files and folders, in the registry, or in the local policies of the system. This consideration is made all the more important by the fact that Windows Server 2003 installs with many more services turned off by default, and tighter security descriptors on objects when compared with default installations of Windows 2000.
   c. Closely related to the item above, any incorrectly configured settings, whether related to security or not will not be brought forward to the newly installed operating system.
   d. Provided that the server has had the hard disks reformatted and the operating system freshly installed, the need for defragmentation of the hard drives is eliminated. Furthermore, if an existing DC has a somewhat fragmented page file, a third party utility would be required to deal with this. The built in Windows 2000 defragmentation utility cannot do this.

      ITC will build fresh installs of Windows Server 2003 on new hardware and perform rolling upgrades of the existing Windows 2000 DCs. Once a Windows 2000 DC is replaced by a new

[8]"Windows 2000 FSMO Roles." Microsoft Knowledge Base 197132. October 10th, 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132 (November 2, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Windows 2003 DC, the hardware is reformatted and used to replace another Windows 2000 DC.

7. **Change the Domain and Forest Functional Levels to Windows Server 2003:** Functional Levels describe an updated concept to that of mixed and native mode domains when discussing Windows 2000 and Windows NT 4.0 domain controllers. Microsoft must now account for the fact that there are more possible upgrade scenarios now versus when Windows 2000 was first introduced early in 2000.

   Once the first Windows 2003 server is introduced into a domain in the forest, the domain functional level will be Windows 2000 native mode. The forest functional level will be Windows 2000 as well. A more complete discussion of functional levels can be found in the appendix, "Upgrading a Windows 2000 Active Directory to Windows Server 2003". That said, in order to gain the full set of additional benefits that Windows 2003's AD brings to the table, you must get raise the forest level to Windows 2003. Fortunately, since they did not need to rename a domain, DTI decided that they could wait until all DCs in the entire forest were running Windows 2003. That way, all they would have to do is upgrade the functional level to Windows Server 2003 and the functional level for all domains in the forest would be upgraded to Windows Server 2003.[9]

8. **Perform the initial set of checks over again:** It bears repeating again that any replication, DNS, or group policy issues should be resolved as soon as possible before proceeding further.

9. **Replicate the Forest Root and Child DNS Zones to All DCs:** In Windows 2000, AD integrated DNS zones (which have been used in the Windows 2000 AD infrastructure) were limited to replicating to DCs in their own domain. An AD forest at the Windows Server 2003 functional level can replicate DNS domains to any domain controller in the forest. This is a great advantage as ITC no longer has to strategically designate some DNS servers in both the DTIROOT.NET and the DTI.DTIROOT.NET domains as secondary name servers for the other domain.

VI. Planning the Windows Server 2003 Based PKI

i. Certificate Policy and Practice Statements

The ITC group thought that they should start off with Certificate Policy and Practice Statements which would guide the design of the PKI project. A

[9] Minasi, Mark. "Mastering Windows Server 2003". San Francisco: Sybex Inc., 2003. 599

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Certificate Policy (CP) statement is a high level document that indicates the policies associated with the PKI in general. Some of the things outlined include:

1. Legal disclaimers.
2. Who can and cannot acquire certificates. In line with DTI's security policy, only employees, and business partners could get certificates.
3. The certificate purposes which the organization supports. The primary purposes would be digital signing, secure e-mail, encryption, and authentication. This is the same for employees and business partners with the exception of encryption. ITC decided that since business partners don't get laptops, there isn't a need for someone outside the company to encrypt data that potentially could be difficult or impossible to retrieve.
4. Archival and recovery of keys. Encryption keys will be archived and accessible only by high level ITC staff in very limited numbers. This will be to avoid potentially losing data due to encrypted information with lost or deleted keys.
5. Enrollment policies. ITC has settled upon auto-enrollment for users and even business partners. DTI already has strict security guidelines and policies for when employees start and their classification within their company For example all employees have criminal background checks and their identities are cross referenced through a number of different government and private organizations before they are issued accounts and/or made members of particular groups. Access to certificate templates will be done on the basis of groups.
6. Revocation policies. At DTI certificates will be revoked when an employee or partner leaves the company, if it is suspected that an existing key has been somehow compromised. A new key will be issued or if an existing key is somehow modified (in which case the old certificate will be superceded).

A Certificate Practice Statement (CPS) is a lower level document that, in the case of DTI, covers very specific details on how different types of CAs will be managed. There was a CPS prepared for each type of CA the ITC group identified they would need. These were a root CA, issuing CAs, and high security issuing CAs.

Items the CPS covers include:

1. All CAs will run on hardware of with at least a 2 Ghz processor and 1 GB or RAM.
2. The key lengths for the various CAs. Root CAs are to have 4096 bit keys, issuing CAs and high security issuing CAs each can have 2048 bit keys.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Who can administer what CAs. 3 or 4 senior ITC staff can administer the root CA. Another small group can administer the high security CAs. and a third larger set, perhaps of Domain Admins can administer the general issuing CAs.
4. Certificate validity. Root CA is 10 years, issuing CAs and high security CAs are 3 years.
5. No CA should be installed on a domain controller. If a server with both those roles be compromised, that would effectively taint DTI's primary authentication infrastructure.
6. Employee certificate validity. Employees including executives have lifetimes of 1 year. Business partners, 3 months.
7. Certificate key lengths. Employees and business partners 1024 bits, executives 2048.
8. Executive certificates should only be available on high security CAs.

ii. Installing the Root Certificate Authority

Much of the success for the project, in the immediate future and over time, hinges on preparing the root CA properly. All certificates issued depend on the security and validity of the root CA in order for them to be considered valid as well.

1. The root CA will be named DTI Root CA. It will be installed as a stand-alone root CA and only be a member of a workgroup. Making it a member of the domain would result in authentication problems for the server since ITC will keep this server offline most of the time except when it is time to publish AIA or CRL information. Only Windows 2003 Standard server is required. Windows 2003 Enterprise Edition is only needed for the enhanced support for version 2 templates and auto-enrollment.

2. CRL and AIA information will be published to the Active Directory and to a special website on the company's intranet.

3. A special batch file will be created so that DTI Root CA will synchronize time with the PDC emulator role holder in the root domain which is DTIROOT.NET.

4. A CAPolicy.inf file will be used for the root CA. This file details some configuration options that will apply to the root CA's certificate itself and other certificates it issues after the fact.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5. Web enrollment support will not be installed as offline requests can be handled by the Certification Authority MMC snap-in now where it could not be in Windows 2000.

6. The certificate database and logs will be stored on separate disk arrays just like the ITC group manages other database related applications.

7. After the installation of the root CA, the certificate will be verified to ensure that all desired parameters have been met. Examples include

8. Once DTI Root CA's certificate is verified, then the CRL and AIA information will be configured to publish to the Active Directory and the intranet web site. The CRL interval will be set to 6 months as the need to publish information more frequently will be practically non-existent as it will be offline and only issue certificates for other CAs.

9. The validity period for issued certificates will be set. Normally, this is only one year so it must be changed. The maximum will be set to 5 years.

10. Once everything is in place, the AIA and CRL information will be published to both AD and the intranet.

11. Finally, DTI Root CA will have a system state backup performed and this will be burned to a CD and stored in a vault.

iii. Installing the Issuing Certificate Authorities

The installation for these CAs will be similar to that of the root CA except that these servers will always be online serving requests. The general steps will be as follows.

1. Each CA will be installed using Windows Server 2003 Enterprise Edition in the root domain. Only this version supports version 2 templates. The primary reason the root was chosen for the installation was that it was deemed more secure. There were a very small number of people within the ITC group that were Enterprise Admins or Domain Admins in the root. This made it much easier to assign permissions only to those who needed them later on

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2. A CAPolicy.inf will be used for each of the issuing CAs as well.

3. Web enrollment will be installed on one issuing CA to facilitate any Windows 2000 servers that cannot be upgraded right away but still may need a certificate. Some web servers which require SSL connections will not be able to be upgraded immediately since they are running some sensitive applications that need to be tested on Windows 2003. Windows 2000 can get version 2 template certificates through web enrollment.

4. When the CAs are being installed, a certificate request file (.REQ) will be generated and submitted to the root for manual approval.

5. Publishing CRL and AIA information to Active Directory is automatic for enterprise CAs. However, the HTTP publication location will be changed to the local intranet.

6. Once the certificate request is approved by the root CA, it will be installed in order to be able to start the Certificate Services. Otherwise, the CA will not operate.

7. Verify the CRL and delta CRL publishing intervals. These will be configured using the CAPolicy.inf files but should be double checked.

8. Verify the certificate chain using the PKI Health Tool from the Windows Server 2003 Resource Kit tools.

9. Lock down the CA by changing default permissions and applying standard lockdown template.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Chapter 3: PKI Implementation Details

I. Upgrading the Existing Windows 2000 Active Directory Domain

i. Verification of the Active Directory and DNS Infrastructure

ITC determined during their planning phase that the first thing that needed to be done was to ensure that any problems with the AD, DNS, and group policy infrastructure be identified and resolved before attempting to introduce any Windows 2003 DCs into their environment.

The ITC group made use of a number of command line tools that can be used for creating scripts for checking AD replication, domain controller health, group policy consistency, etc. A batch file was created that could be run from all the domain controllers and the results examined.

Essentially, the batch file runs DCdiag which itself runs a battery of tests to determine if domain controllers has registered properly with DNS, knows about the operations master roles (also known as FSMOs), etc. Additionally, it runs checks on the networking set up of the machine (via netdiag), and checks group policy object consistency (via GPOtool)

The listing below details the batch file that was run. For a detailed explanation of the function of each line and the tools used, see the Upgrading to Windows Server 2003 appendix.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
MD L:\ADCheck
L:
CD\
CD ADCheck

netdiag /l

dcdiag /c /e /v /f:L:\ADCheck\DCdiag.txt
dcdiag /TEST:DcPromo /DnsDomain:DTI.DTIROOT.NET /ReplicaDC
/f:L:\ADCheck\DCPromoROOT.txt
REM dcdiag /TEST:DcPromo /DnsDomain:DTIROOT.NET /ReplicaDC
/f:L:\ADCheck\DCPromoDTI.txt
dcdiag /TEST:RegisterInDNS /DnsDomain:DTI.DTIROOT.NET /f:L:\ADCheck\DCRegRoot.txt
REM dcdiag /TEST:RegisterInDNS /DnsDomain:DTIROOT.NET /f:L:\ADCheck\DCRegDTI.txt

netdom query DC > L:\ADcheck\DomainControllers.txt
netdom query fsmo > L:\ADcheck\FSMO.txt
netdom query trust > L:\ADcheck\DomainTrusts.txt

gpotool /verbose > L:\ADcheck\GPOverify.txt
```

Listing 3-1: CheckAD.bat script the ITC project members used in verifying AD replication, DC DNS registrations, and FSMO roles.

Most of these tools assume that at least the Windows Support Tools are installed from the Support\Tools directory of the Windows 2003 installation media. Run SUPTOOLS.MSI to start the installation.

ii. Pre-Installation Steps

1. **Installed Windows 2003 Servers in a Workgroup:** These servers would be subsequently promoted to domain controllers in the root domain and replace the existing Windows 2000 DCs. The installs were performed according to the server standards for DTI.

2. **Determined Service Pack Level of Domain Controllers:** The ITC group wanted to ensure that all domain controllers were running their corporate standard of Windows 2000 Service Pack 4. In addition to the regular and security related hotfixes that the service pack provides, there were also a number of features included that would aid in maintaining compatibility and manageability of the various DCs running either Windows 2000 or 2003. This is discussed in more detail in the planning portion of this document.

3. **Added Network Admins to the Schema Admins Group:** DTI maintains an empty Schema Admins group in order to mitigate the possibility of unwittingly making changes to their AD schema. Some software packages do make changes to the AD schema which, in a Windows 2000 environment, cannot be reversed. The administrative

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

accounts of the network administrators performing the install were added in preparation.

An administrator must be a member of this group in order to make changes to the AD schema. This is not the only requirement however.

The Schema Admins group is located in the User container of the root domain in the forest.

4. **Set Schema FSMO Role Holder to be Allow Schema Updates:** In Microsoft parlance, FSMO stands for Flexible Single Master Operations. This term refers to the fact that although AD follows a replication model in which most changes can be made connected to any domain controller, some types of updates are better suited to being assigned to one particular server.

   DTI-RT001 was the schema FSMO role holder for DTI's AD forest which simply means that this was the only domain controller in DTI's forest from which any schema updates could occur. An additional step that was made was to enable schema updates to occur from that machine. This was accomplished by running editing the registry at the following location:

   HKEY LOCAL MACHINE\System\Current Control Set\Services\NTDS\Parameters

   A REG_DWORD value was added called "Schema Update Allowed" with a value (decimal or hex) of 1. When it needs to be disabled, set the value to 0.

5. **Took Steps to Avoid Exchange 2000 "Mangled Attribute" Problem:** As described earlier in the Windows 2003 upgrade planning section of this document, Exchange 2000 makes three, non-RFC 2798 compliant changes to the AD schema. The ITC group needed to update these attributes before running the ADPREP utility in order to avoid problems. Specifically they:
   a. Viewed the Existing Attributes: This was done using the Active Directory Schema MMC tool from the Windows 2000 Support Tools. After the Support Tools were loaded (by running SETUP.EXE from the Support\Tools directory on the Windows 2000 installation media), the tool was added to the management MMC.

      To view the Secretary, houseIdentifier, and labeledURI attributes expand the Schema MMC and click on the Attributes

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

node. In the right hand pane will be a listing of all the attributes defined in AD. Typing the name of the attribute you wish to view will take you to it. Right or double clicking the attribute will open its properties. The LDAPDisplayName which was to be changed is displayed at the top of the property window as Figure 3-1 below shows.

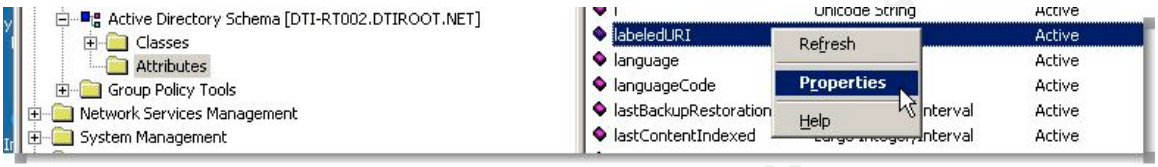


Figure 3-1: Active Directory Schema tool highlighting the labeledURI attribute.

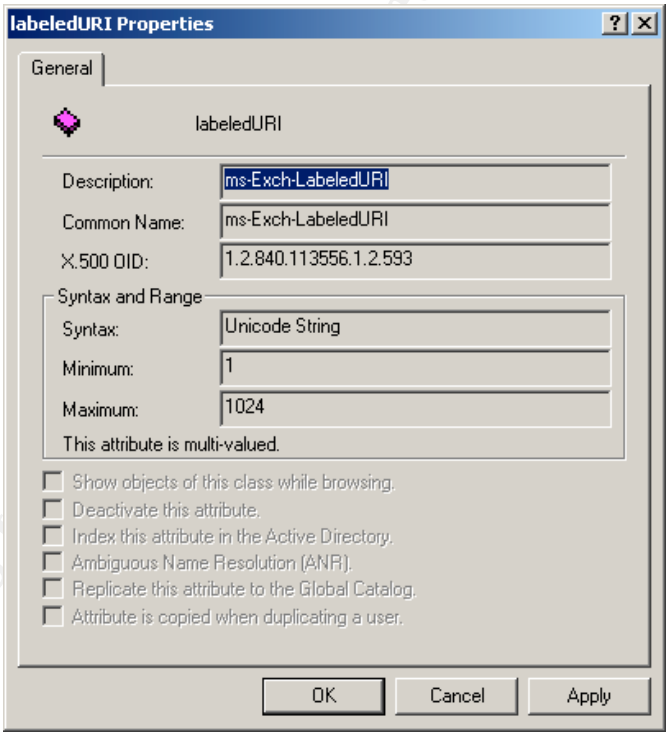


Figure 3-2: The labeledURI attribute properties before changing the LDAPDisplayName which maps to the Name field (the top most label to the right of the pink object in the property window above) for these attributes.

b. **Updated Existing Non RFC 2798 Compliant Schema Attributes:** Using ADSI Edit on DTI-RT001 (the Schema

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Master for their Windows 2000 AD domain), the Secretary, houseIdentifier, and labeledURI attributes LDAPDisplayNames were updated to avoid conflicting with what would be installed when running the ADPREP /forestprep command. Table 1 below shows the old names and what they were changed to in accordance with Microsoft Knowledge Base article 314649.

	Attribute Common Name (CN)	Exchange 2000 Attribute LDAPDisplayName	Non-Conflicting Attribute LDAPDisplayName (Changed To)
1.	ms-Exch-Assistant-Name	Secretary	msExchAssistantName
2.	ms-Exch-House-Identifier	houseIdentifier	msExchHouseIdentifier
3.	ms-Exch-LabeledURI	labeledURI	msExchLabeledURI

Table 3-1: The attributes above were created because Exchange 2000 was introduced to the domain. The LDAPDisplayNames needed to be changed to avoid conflicting with InetOrgPerson attributes introduced by the ADPREP /forestprep AD preparation tool.

The ITC group used the ADSI Edit tool on DTI-RT001 (the Schema Master for DTI's Windows 2000 AD forest) to make the changes to the LDAPDisplayNames. The following is a description of how to accomplish the same task. When editing the registry, care and attention is a 10 on a scale of 10 most important things when making server changes. By comparison, caution when editing the schema is most likely a 40 on that same scale. Accidentally adding or deleting the wrong thing can potentially cause serious problems which may replicate to every domain controller in your forest.

- Log on to the Schema Master server for your AD forest. You must log on as a user who is a member of the Schema Admins group.
- Go to the Start menu and then go to Programs\Windows 2000 Support Tools\Tools\ADSI Edit
- If the Schema naming context is not displayed when you expand the ADSI Edit object in the MMC, right click ADSI Edit and select Connect.
- When the Connection window appears, select Schema from the Naming Context drop down list box.
- Leave the Computer portion on the default setting with the last radial button selected.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Click OK to complete the operation.
- The Schema object should now appear in ADSI Edit. Expand it and click on the CN=Schema,CN=Configuration,DC=<Domain Name>,DC=<Domain Name>. For example, the same object in the DTI forest is: CN=Schema,CN=Configuration,DC=DTIROOT,DC=NET
- In the right hand pane should be a listing of all the schema attributes. Type the following: CN=<name of attribute you wish to modify>. In the case of ms-Exch-Assistant-Name, you would type: CN=ms-Exch-Assistant-Name.
- Right click the attribute and select Properties from the menu.
- In the drop down list box for selecting which properties to view (top), select Mandatory. In the list box for the specific property (bottom), pick LDAPDisplayName.
- Type the new name in the Edit Attribute field and then click the Set button. You will see the value you entered in the Value field (which cannot directly be edited).
- Click OK to save the change.
- Repeat the last 5 steps for any other attributes to be modified.
- Allow changes ample time to replicate to all the other domain controllers in the forest before proceeding.

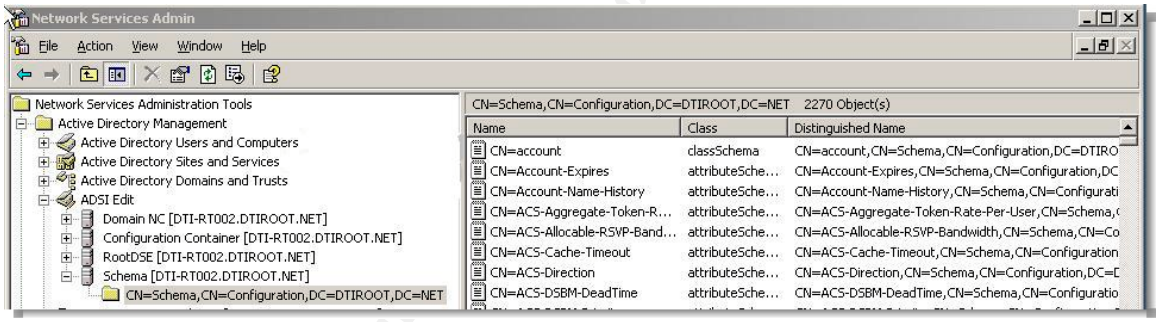


Figure 3-3: Picture of the ADSI Edit utility with the Schema naming context expanded to reveal the attributes in the right hand pane of the MMC.

NOTE: ADSI Edit is a tool which allows you to take a low level look at the Active Directory and should therefore in the toolkit of any administrator managing AD. There are at least 2 additional AD contexts (the Schema context was already added in the example above) that should be added to the tool. They are the Domain NC and Configuration Container. See the appendix for more information.

iii. Active Directory Preparation

Once the project team was certain that they had properly addressed the Exchange 2000 attribute issue, they were ready to move on to preparing AD for the introduction of Windows 2003 DCs.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. **ADPREP /forestprep:** ITC first ran the ADprep /forestprep command from DTI-RT001.

   With the Windows Server 2003 CD in the CD-ROM drive, they went to a command prompt and ran the command below. ITC always assigns CD-ROMs to the R: drive letter.

   R:\i386\ADprep /forestprep

```
R:\I386>adprep /forestPrep

ADPREP WARNING:

Before running adprep, all Windows 2000 domain controllers in the forest should be upgraded to Windo
ws 2000 Service Pack 1 (SP1) with QFE 265089, or to Windows 2000 SP2 (or later).

QFE 265089 (included in Windows 2000 SP2 and later) is required to prevent potential domain controll
er corruption.

For more information about preparing your forest and domain see KB article Q331161 at http://support
.microsoft.com.

[User Action]
If ALL your existing Windows 2000 domain controllers meet this requirement, type C and then press EN
TER to continue. Otherwise, type any other key and press ENTER to quit.



c
Opened Connection to DTI-RT001
SSPI Bind succeeded
Current Schema Version is 13
Upgrading schema to version 30
Connecting to "DTI-RT001"
Logging in as current user using SSPI
Importing directory from file "C:\WINNT\system32\sch14.ldf"
Loading entries.....................................................................................
.....................
111 entries modified successfully.

The command has completed successfully
Adprep successfully updated the forest-wide information.
```

Listing 3-2: Partial listing of ADprep /forestprep screen output. Note the reference to the current and post upgrade schema versions. Some lines have been removed in order to make the listing more compact and readable.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

a. **Verified ForestPrep Changes:** To verify that the changes indeed took place, they made use of, once again, the ADSI Edit utility. In order to do this:

- Launched ADSIEdit.msc
- Expanded the Configuration naming context.
- Observed whether or not the CN=ForestUpdates container had been created.[10]
- By clicking on the ForestUpdates container or by expanding it, see if there is a CN=Windows2003Update container (in the right hand pane or as a sub-container of ForestUpdates).[8]

NOTE: The "Microsoft Windows Server 2003 Deployment Guide: Designing and Deploying Directory and Security Services" book incorrectly (as of this writing) indicates that the container under the ForestUpdates container to look for is called "CN=Windows2003Upgrade" in Chapter 9. Do not be concerned if, in your testing, you do not see this exact container.

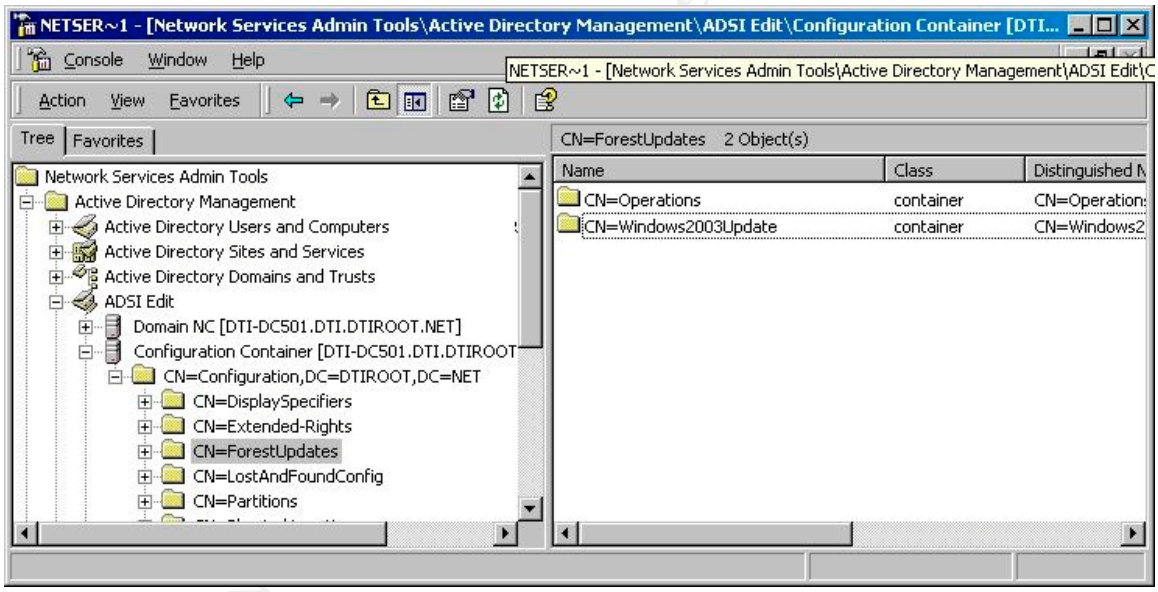


Figure 3-4: Confirming the successful installation of the changes made by Adprep /forestprep by looking for the Windows2003Update object under the ForestUpdates container in ADSI Edit.

b. **Verified Changes Propagated to Other DCs:** By connecting to other DCs in other sites and using ADSI Edit to look at the Configuration container, ITC was able to determine that the changes had replicated to them as well.

[10] Microsoft Corporation. "Microsoft Windows Server 2003 Deployment Kit: Designing and Deploying Directory and Security Services". United States of America:
Microsoft Corporation., 2003. 380

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2. **ADPREP /domainprep:** Once the Adprep /forestprep schema changes had replicated to all of the other DCs in the forest, then this command was run in both of DTI's domains. First in the root domain (DTIROOT.NET) and then the child of the root (DTI.DTIROOT.NET).
    a. **Verified DomainPrep Changes:** ITC ran ADSI Edit and went into the Doman NC container.
    - From there they expanded the DC=DTIROOT,DC=COM object.
    - Expanded CN=Ssytem
    - Expanded CN=DomainUpdates
    - Observed that CN=Windows2003Update was in the right hand pane.

    b. **Verified Changes Propogated to Other DCs:** They used the same technique as was used after the Adprep /forestprep command ran.

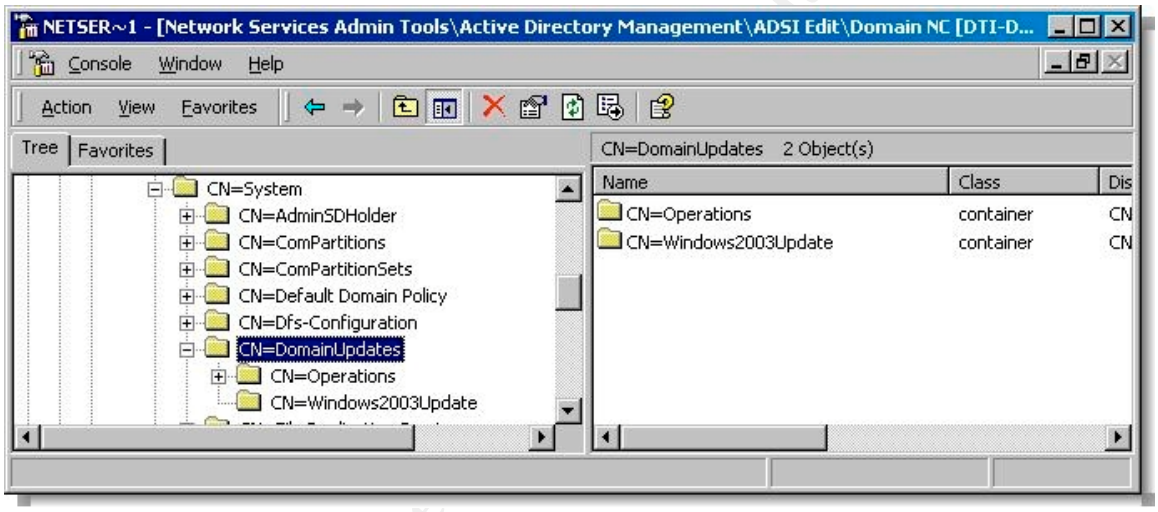


Figure 3-5: Confirming the successful installation of the changes made by Adprep /domainprep by looking for the Windows2003Update object under the DomainUpdates container in ADSI Edit.

II. Installing the PKI Infrastructure

i. Installing the Root Certificate Authority

With the successful upgrade of DTI's Active Directory forest to the Windows Server 2003 Functional Level, the ITC group could now proceed with the implementation of the PKI infrastructure itself.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

DTI decided upon a two-tiered certificate authority (CA) architecture. They also decided upon an offline root CA for the reasons outlined earlier in the design chapter.

The first piece of the structure to be installed was the root certificate authority (CA). They proceeded as follows:

1. **Installed a Windows Server 2003 Server into DTI-RAWKGRP Workgroup:** The root CA will be offline and therefore must be installed in a workgroup configuration. The ITC group decided on the name DTI-RAWKGRP although any would have done.

2. **Configured CAPolicy.inf File and Copied to the %SYSTEMROOT% Directory:** The CAPolicy.inf file was a critical step to the overall PKI installation procedure as it specifies blank CRL and AIA distribution point fields for the root. If the CAPolicy.inf file was not used, the CRL and AIA distribution points would be set to local directories on the RootCA which could never be resolved by any of the subordinate CAs to which it would be issuing tickets since the root would be offline the majority of the time. Listing 3-3 shows the contents of the file used for the Root CA. In addition to the CRLDistributionPoint and AuthorityInformationAccess fields, the other items, as defined in the certificate practices statement for the organization is as follows.
    a. **RenewalKeyLength=4096:** The Root CA is probably the most important server in the CA hierarchy. Should it ever somehow become compromised, the entire hierarchy below it would be compromised as well. That said, the ITC group decided that the root should have very strong encryption keys, but not so long that it would risk the interoperability potential down the road with partner certificate authorities. The "Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure" white paper on Microsoft TechNet states.

       "It is recommended that the key length does not exceed 4096 bits because this is the maximum interoperable key length with most programs and PKI providers. The renewal key length must not be shorter than the key length that you chose during the CA installation procedure."[11]
    b. **RenewalValidityPeriod=Years:** This line defines the period of time the CA uses in determining the length of time a CA certificate

[11] "Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure." Appendix B: Parameters for a Three Tier CA Topology.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp (November 12, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

which has been renewed will be considered valid. In this case, the root CA determines this value in years. Other valid periods include days or months.

c. **RenewalValidityPeriodUnits=10:** The actual amount of time periods (defined above) the certificate of the CA will be valid for upon renewal. As defined by this CApolicy.inf, the renewed certificate will be valid for 10 years. This amount of time is considered valid since the CA is unlikely to become compromised during that period of time due to a long key length and the fact that it is offline most of the time.

```
[Version]
Signature= "$Windows NT$"

[Certsrv_Server]
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=10

[CRLDistributionPoint]

[AuthorityInformationAccess]
```

Listing 3-3: Contents of the CAPolicy.inf file used to install the DTI Root CA.

3. **Set Time Synchronization:** Normally, in a Windows 2003 or 2003 forest, time is synchronized between all forest members. Since DTI Root CA will be offline and never actually join a windows domain, time synchronization is somewhat of a concern. A batch file was created which simply ran the following command and restarted the Windows Time service (w32tm):

   w32tm /config /update /manualpeerlist:tick.usno.navy.mil

   The process synchronized the time of DTI Root CA with that of a time server on the Internet. The same one used by DTI's AD forest.

4. **Installed Certificate Services from Add/Remove Programs:** Certificate services was installed by launching Add/Remove programs from the Control Panel and selecting the Certificate Services checkbox in the Add/Remove Windows Components section.
   a. By default, both the Certificate Services CA and Certificate Services Web Enrollment Support modules were selected. These can be observed by clicking Details with Certicate Services highlighted. Both of these needed to be installed. Once Next was clicked a warning message pointing out the fact that the name and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

domain membership of the server cannot be changed as it could invalidate certificates that it will subsequently issue.

b. The table below has the settings which were filled in and the values which DTI used during the installation. Of particular importance were the values used on the Public and Private Key pair portion of the wizard as these are the values that are assigned to the self signed ticket the root will generate.

- ITC learned that they needed to take particular care in moving between the Public and Private Key Pair portion of the installation wizard and other screens. The key length box resets itself to 2048 instead of the desired 4096 each time they went back to it.
- The distinguished name field also became blank when someone would navigate away from the CA Identifying information screen and then went back.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CA Install Wizard Screen	Property Name	Value Entered
CA Type	CA Type	Stand-alone root CA
CA Type	Use custom settings to generate the key pair and CA certificate	Ensured the box was checked.
Public and Private Key Pair	CSP	Microsoft Strong Cryptographic Provider
Public and Private Key Pair	Hash algorithm	SHA-1
Public and Private Key Pair	Key length	4096
Public and Private Key Pair	Allow this CSP to interact with desktop	Checkbox cleared (default)
CA Identifying Information	Common name for this CA	DTI Root CA
CA Identifying Information	Distinguished name suffix	DC=DTIROOT,DC=NET
CA Identifying Information	Validity Period	10 years
Certificate Database Settings	Certificate Database	D:\Certlog
Certificate Database Settings	Certificate Logs	L:\Certlog
Certificate Database Settings	Shared Folder	D:\CAConfig
Confirmation Box	Confirming location of certificate database files	Clicked Yes to continue.
Warning Dialog Box	Warning that web enrollment will not work without IIS being installed (which it was not).	Clicked OK to continue.

©SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

©SANS Institute 2004, Author retains full rights.

Table 3-2: Properties of the CA install wizard and the values that the ITC group entered when installing certificate services on the root CA.

5. The ITC group did not initially install IIS on the Root CA server because they forgot that Windows 2003 does not install IIS by default unlike Windows 2000. Therefore, they had to go back into Add/Remove programs and add the Windows 2003 default of IIS. In order for the web

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

enrollment pages to work however, an additional step had to be taken using the certutil tool in order for the web enrollment web pages to be generated. The command certutil –vroot was run.

a. Web enrollment pages were tested by going to http://localhost/certsrv in Internet Explorer.
b. Certutil is a command line tool that can perform numerous PKI related functions. Details on its usage can be found in Chapter 3

6. **Root CA certificate Verified**:
   a. The Certificate Authority snap-in was added to the Network Services management MMC.
   b. All configured parameters were confirmed to be present in the certificate. Administrators went into the properties of the DTI Root CA object in the Certificate Authority snap-in. On the General tab of the properties window was a button to "View Certificate". On the General and Details tabs, the settings below could be verified. This is not a complete list of all the certificate details. Only those related to what was configured during the install of the CA.

- **Common Name:** DTI Root CA. This appears on the General tab as well as the Subject field on the Details tab of the root CA's certificate.
- **Issuer:** In this case, because it was a root CA, the issuer was itself. This is on the General tab and the Issuer field on the Details tab of the CA's certificate.
- **Validity Dates:** The date which the certificate became valid and the date which it will become invalid. This information is on the General tab and the Valid From and Valid To fields on the Details tab of the CA's certificate.
- **Cryptographic Service Provider (CSP):** Project members selected the default of the Microsoft Strong Cryptographic Provider. This appears on the General tab of the CA properties when opened from the Certificate Authority MMC snap-in.
- **Signature Algorithm (Hash):** SHA-1 had been selected. This appears on the Details tab of the CA's certificate in the Signature Algorithm field.
- **Public Key (Key Length):** 4096 bits was chosen. This appears on the Details tab of the CA's certificate in the Public Key field.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Figure 3-6: Certificate of the DTI Root CA, General tab.

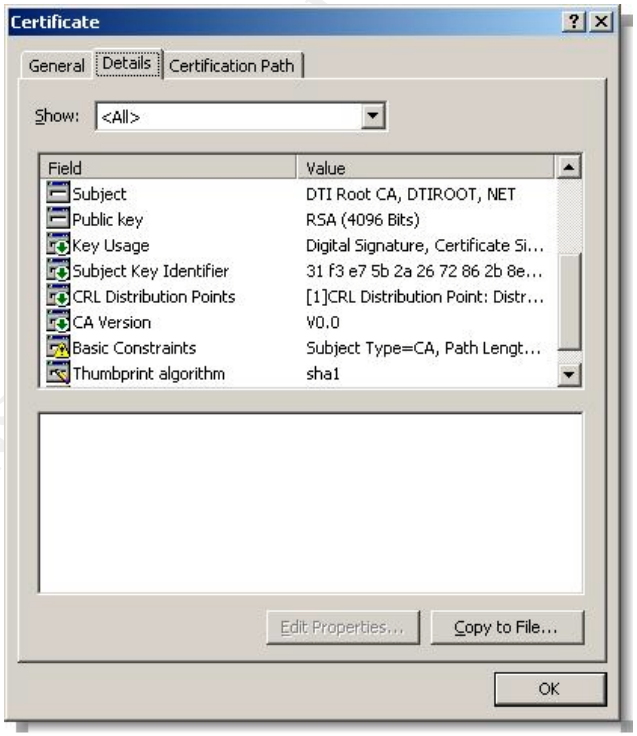


Figure 3-7: Certificate of the DTI Root CA, Details tab.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7. **AD Namespace Mapped to Root CA's Registry:** This will aid in being able to publish the CRL and AIA information to AD since this does not happen automatically with an offline CA. AD was selected as the primary vehicle for delivering this information since there will be predominantly Windows based domain clients using the PKI.
    a. Using the CertUtil utility, a registry key on the DTI Root CA computer was mapped to use Active Directory. This would normally been done automatically on Enterprise CAs, but since this CA is a stand-alone which will never join a domain and be offline, it must be specifically configured. See Listing 3-4 below for the specific syntax used and screen output. It is important that this been done before any certificates are issued.
    b. Stopped and started the CertSvc service for the change to take effect.

```
C:\>certutil -setreg ca\dsconfigdn cn=Configuration,DC=DTIROOT,DC=NET
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\DTI Root CA\dsconfigdn:

New Value:
  dsconfigdn REG_SZ = cn=Configuration,DC=DTIROOT,DC=NET
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

Listing 3-4: CertUtil command used to map a key in the CA's registry to the Configuration container in DTI's root domain (DTIROOT.NET). The purpose was so that DTI Root CA could publish its AIA and CDP information to the Active Directory.

8. **Configured DTI Root CA AIA and CRL Distribution Points**: Another vital step that need to be performed before the issuance of any certificates was to specifically configure the AIA and CRL distribution points. As previously stated, it is important to do this because clients verifying certificates up the chain of trust must be able to retrieve this information. The procedure was as follows:
    a. Using the Certificate Authority MMC, the Root CA administrators went into the properties for DTI Root CA and then went to the Extensions tab. This is where the CRL Distribution Points (CDP) and Authority Information Access (AIA) information is configured.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

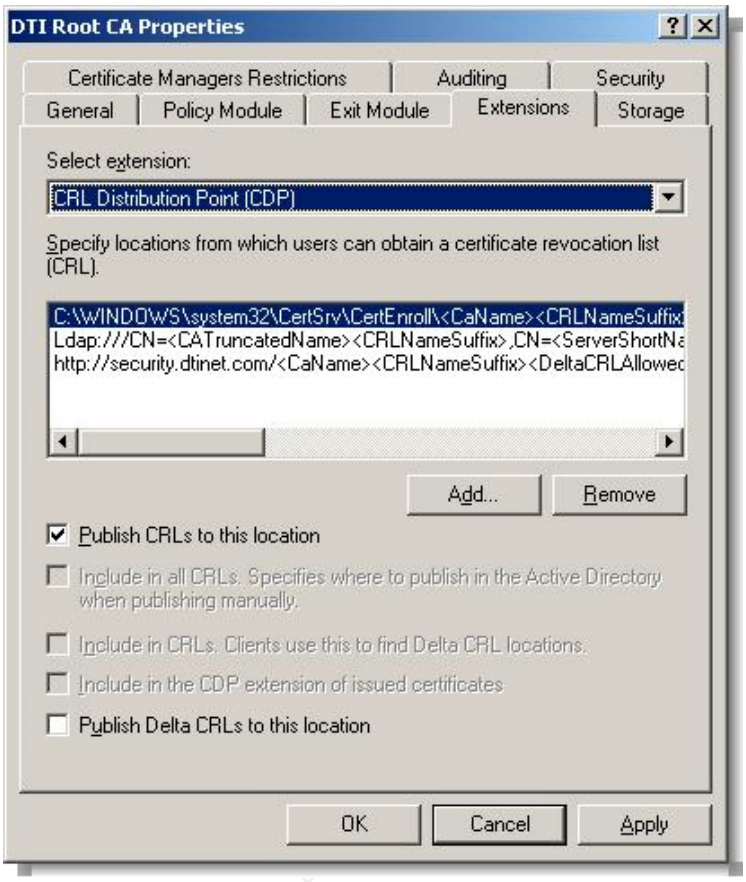


Figure 3-8: Extensions tab of the DTI Root CA properties. The CDP and AIA information for the CA can be configured using this interface.

b. In the Select extension drop down list box, CRL Distribution Point (CDP) was selected. All other paths except for the local path, which the CA uses when validating certificates prior to them being issued to others.[12]
c. The following table is from the Best Practices for Implementing a Windows Server 2003 Public Key Infrastructure guide on Microsoft TechNet. It contains the CDP information that the ITC group used for the root CA. Note that in DTI's case the LDAP URL is listed first followed by HTTP. This reflects the fact that the majority of the clients accessing this information will be Windows 2000 or XP and will be using Active Directory. HTTP has been included for future

[12] "Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure." Offline Root CA Configuration.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp (November 12, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

uses such as using certificates with routers or non Windows based operating systems.

	CRL Access Protocol	CRL Distribution Point	
	Default File Location	C:\Windows\System32\CertSrv\CertEnroll\%3%8%9.crl	
	LDAP	LDAP:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10	
	HTTP	http://security.dtinet.com/%3%8%9.crl	

Table 3-2: CDP used for the DTI Root CA.[13] LDAP is listed before HTTP since most of DTI's clients needing this information will be domain members accessing Active Directory. The HTTP location was set up by the ITC project team specifically for CRL and AIA publications.

The symbols included in the URL are known as replacement tokens which act as wildcards for abstracting certain aspects of CA configuration. Thus the URLs in Table 3-3 could be used for other CAs with minimal modification, if any. These tokens can be used in the scenario they have been for configuring the CA properties on the Extensions tab or in a CAPolicy.inf file. They are denoted by the % symbol followed by a number. In the context of Windows Server 2003, the replacement tokens used in Table 3-3 refer to the following:

- **%3** The name of the CA. Also known as CaName.
- **%6** The AD configuration container location. For DTI, this would be CN=Configuration,DC=DTIROOT,DC=NET
- **%7** Refers to the sanitized name of the CA. It is limited to no more than 32 characters. See Listing 3-5
- **%8** The CRLNameSuffix which, according the Windows Server 2003 documentation, "Inserts a name suffix at the end of the file name when publishing a CRL to a file or URL location". [14]

[13] "Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure." Offline Root CA Configuration.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp (November 12, 2003)

[14] "Windows Server 2003 Product Documentation." Manage Certificate Revocation.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_csprocs_cdp.asp (November 16, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- **%10** CDPObjectClass OID or object identifier. See Figure 3-9.

```
Exit module count: 1
CA name: DTI Root CA
Sanitized CA short name (DS name): DTI Root CA
CA type: 3 -- Stand-alone Root CA
    ENUM_STANDALONE_ROOTCA -- 3
CA cert count: 1
KRA cert count: 0
KRA cert used count: 0
CA cert[0]: 3 -- Valid
CA cert version[0]: 0 -- V0.0
CA cert verify status[0]: 0
CRL[0]: 3 -- Valid
CRL Publish Status[0]: 0x45 (69)
    CPF_BASE -- 1
    CPF_COMPLETE -- 4
    CPF_MANUAL -- 40 (64)
DNS Name: DTI-RA001.DTI.DTIROOT.NET
Advanced Server: 1
CertUtil: -CAInfo command completed successfully.
```

Listing 3-5: Output from successfully running the certutil –cainfo command against DTI's Root CA. Note the inclusion of the sanitized name for the CA.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

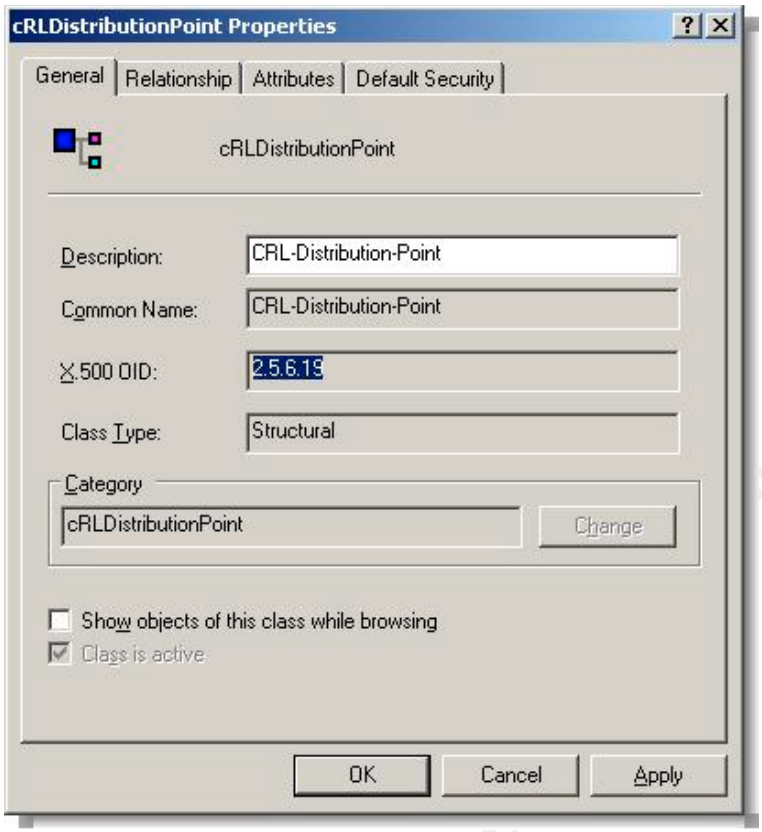


Figure 3-9: The CDPObjectClass object ID as viewed through the AD Schema MMC on DTI-RT002 (the new Schema Master for DTI's AD forest).

Table 3-4 specifies the options that were selected for a given CRL publication location.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	CDP Property	Default File Location	HTTP	LDAP
	Publish CRLs to this location	Selected		**Cleared**
	Include in all CRLs			**Selected**
	Include in CRLs		Cleared	**Selected**
	Include in the CDP extension of issued certificates		Selected	**Selected**
	Publish delta CRLs to this location	**Cleared**		**Cleared**

Table 3-4: Properties the ITC group selected for each CRL distribution point.[15] A blank cell indicates that this option would normally be greyed out in the interface and not applicable to that particular CDP location. A cell with Cleared in it means that the root CA administrators purposely cleared this check box or left it empty. Finally, a cell with Selected in it means that administrators intentionally configured this setting or left it on by default.

The ITC group researched this particular set of settings in the Best Practices for Implementing a Windows Server 2003 Public Key Infrastructure document. They concluded that the settings above were applicable to their PKI model. Below are the reasons why they set each of the CDP properties the way they did.

- **Publish CRLs to this location:** Used by CA. This setting means the CA will automatically publish CRLs to this location. In this situation the root CA will normally be offline and therefore not be able to do this. HTTP is not automatically published to and therefore this option is not applicable.
- **Include in all CRLs:** Used by CA. This is an AD related property which is why it is not applicable to the file location or HTTP. It specifies the location in AD where the CRL will be published when done manually. Any publishing of the CRL from the root CA will be done manually since it will normally be kept offline and only brought online for these purposes.
- **Include in CRLs:** Used by certificate clients. Clients will use this information to determine if there are any delta CRLs and, if so, their location.

[15] "Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure." Offline Root CA Configuration.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp (November 16, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- **Include in the CDP extension of issue certificates:** Used by clients. It indicates the location of the CRL distribution points (CDP). This is extremely important for any clients to perform revocation checking regardless of whether they are retrieving the information from AD or the intranet via HTTP.
- **Publish delta CRLs to this location:** Used by CA. As previously discussed, there is no need for delta CRLs to be used by the root CA because of the low number of certificates that it directly issues (only to issuing CAs in the DTI trust hierarchy) and the infrequent revocation (every 3 years for an issuing CA to expire or if ITC determines the need to revoke one sooner which is unlikely). If there were delta CRLs being used, then the CA would use the URLs selected to publish this information.

d. When applying their changes by clicking on the Apply button, they had to click Yes when prompted about restarting Certificate Services.

9. In the Select extension drop down list box, Authority Information Access (AIA) were selected. All other paths except for the local path, which the CA uses, were cleared.

AIA Access Protocol	AIA Distribution Point
Default File Location	C:\Windows\System32\CertSrv\CertEnroll\%1_%3%4.crt
LDAP	LDAP:///CN=%7%,CN=AIA,CN=Public Key Services,CN=Services,%6%11
HTTP	http://security.dtinet.com/%1_%3%4.crt

Table 3-5: CDP used for the DTI Root CA.[16] LDAP is listed before HTTP since most of DTI's clients needing this information will be domain members accessing Active Directory.

There are some replacement tokens included here which were not discussed in the CRL configuration. They are:

- **%1** ServerDNSName. The DNS name of the server. In this case DTI-RA001.DTI.DTIROOT.NET.
- **%4** CertificateName which is the renewal extension of the certification authority.
- **%11** CAObjectClass which refers to the object ID or OID.

[16] "Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure." Offline Root CA Configuration.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp (November 12, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The only property set for each of the URLS is the "Include in the AIA extension of issued certificate". This is used by clients to retrieve the CA's certificate. Clients will use LDAP first since most of them will be AD aware. This is used in verifying the certificate trust chain. HTTP is available for any non-Windows clients that may eventually be enrolled in the PKI.

Include in the online certificate status protocol (OCSP) extension is a setting that bears mentioning. Although it is not selected it may be at some point in the future. OCSP is a protocol that provides *real-time* access to the CRL of a CA. No windows platforms have built-in support an OCSP cryptographic service provider (CSP) but there are third party ones available. The ITC team will be looking at this more closely once the initial roll out of the PKI is complete.

10. **Set CRL publishing interval to 6 months:** The PKI project team members decided that this was a reasonable amount of time to publish a full CRL to the distribution point since the CA will not have to revoke many certificates due to the fact that the root CA will only issue to the issuing CAs. Furthermore, configuring delta CRLs would also not be necessary due to the low volume of certificates the root will issue directly and the infrequency of expired or revoked certificates. The bottom line is that few resources are required to publish the CRL or download the entire CRL to clients.

    In order to set the CRL publishing interval, the following steps were performed.

    a. Launched the Certificate Authority MMC and expanded the DTI Root CA object.
    b. Went into the properties of the Revoked Certificates node.
    c. On the CRL Publishing Parameters tab, they selected 6 months from the CRL Publication Interval drop down list box.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

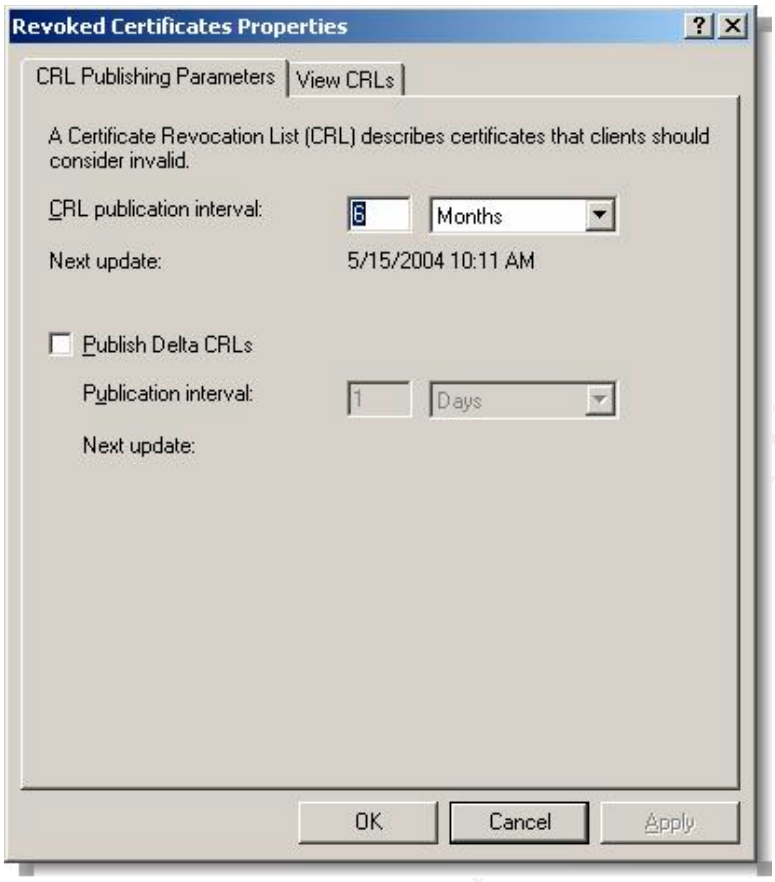


Figure 3-10: Properties of the Revoked Certificates node in the Certification Authority MMC snap-in. In the case of the DTI Root CA, the CRL publication interval was set to 6 months.

11. **Set Validity for Issued Certificates:** This step set the default validity for certificates issued by DTI Root CA. The default otherwise is only 1 year. Different validity dates can be set for v2 templates (discussed later).

    If this was set in the CAPolicy.inf file, it would only have been valid for the certificate of the root CA itself.

    a. **ValidityPeriod:** The measure of time that will be used to measure how long certificates the CA issues remain valid. In this case ITC used Years. Other possible values include days or months.
    - Ran certutil –setreg ca\ ValidityPeriod "Years"

    b. **ValidityPeriodUnits:** The number of units of the ValidityPeriod for which the issued certificates will remain valid. In this situation, 5 was selected. So certificates issued by DTI Root CA will be valid for a period of 5 years.
    - Ran certutil –setreg ca\ValidityPeriodUnits 5

    c. After both commands were run the Certificate Services service was restarted.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

12. **Published CRL and AIA Information:** After the CA was properly configured, it was time to publish the CRLs and AIA information to AD and to the security.DTINET.com intranet site so that clients, including issuing CAs, would be able to retrieve this information. ITC proceeded as follows:
    a. **Published the CRL to AD:** They launched the Certification Authority MMC, right clicked the Revoked Certificates node and from the All Tasks menu option selected Publish. Alternatively, the certutil –dspublish –f command could have been used.
    b. **Published the AIA to AD:** The oft used CertUtil tool was pressed into service once again. ITC decided that this was the best method of distributing the AIA to client machines. Then it would be available forest wide instead of them having to set a group policy in both the root and child domains to set it up a a Trusted Root Certification Authority
    - Certutil –dspublish –f DTI-RA001.DTI.DTIROOT.NET_DTI Root CA.crt RootCA
    c. **Published CRL and AIA to Intranet:** The CRT file for the root certificate and the crl were simply copied to the intranet web server from the default locations on the file system
13. **Backed up System State of CA:** The system state of the CA was backed up and burned to a CD which was then put in a vault.

ii. Installing the Issuing Certificate Authorities:

Once the root CA was installed and properly configured, it was time to set up the issuing CAs. These will be the CAs which will distribute certificates to the computers and users in DTI's forest.

The most significant difference between the install of the issuing CAs versus the root install is these were made members of the an Active Directory domain. This results in a somewhat easier set up than that of the root as many things are automatically configured and published to the Active Directory.

1. **Installed a Windows 2003 Enterprise Server as Member of the Root Domain:** As before, once the certificate services were installed, the name of the server nor domain membership could be changed. Since it was the intention that this become an enterprise CA, it had to be made a member of a domain in the forest. The primary reason the root was chosen for the installation was that it was deemed more secure. There were a very small number of people within the ITC group that were Enterprise Admins or Domain Admins in the root. This made it much easier to assign permissions only to those who needed them later on.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Enterprise server was selected in this instance because of the identified need to use version 2 templates and auto-enrollment both of which are only supported on Enterprise edition. This is just as Windows 2000 Advanced Server was required for computer autoenrollment. Both Windows 2000 Server and Windows Server 2003 Standard only support version 1 certificate templates when installed as Enterprise CAs.

2. **Configured CAPolicy.inf File and Copied to the %SYSTEMROOT% Directory:** The CAPolicy.inf file is an important step in this installation too as it is a way that the certificate practices can be implemented easily and consistently across installed issuing CAs. Listing 3-6 shows the CAPolicy.inf that was used for the issuing CAs. Explanations will be given where the policy differs from that used by the root CA.
   a. **Policy Statement Extension:** This section, referred to in Windows 2000 CAPolicy.inf files as the [CAPolicy] section defined the various issuer statements that can be included with certificates when they are issued. DTI's policy has been published to a website on their intranet. DTINET.com The specific policy defined is DTICertPolicy.
   b. **DTICertPolicy:** The first line under this section defines the OID or object identifier for the policy. This must be defined for each of the policies. The URL portion, of course, points to the web page where the policy statement is located on DTI's intranet.
   c. **RenewalKeyLength=2048:** The lower key length will improve performance when issuing certificates as these servers will have far more certificates to issue than the root CA.
   d. RenewalValidityPeriod=Years:
   e. **RenewalValidityPeriodUnits=3:** As defined by this CApolicy.inf, a renewed issuing CAcertificate will be valid for 3 years. The chances of the CAs key becoming compromised is much more possible for issuing CAs because they are always online and the key length of their privates keys is much shorter.
   f. **CRLPeriod=Days:** The measure of time that will be used to measure how often the CRL will be published. Days were selected since certificates will be issued and revoked often as people come and go and network accounts are created or remove for business partners, employees, etc.
   g. **CRLPeriodUnits:** The number of CRLPeriods before the next CRL is published. The ITC project team settled on 3 days as a reasonable amount of time.
   h. **CRLDeltaPeriod=Hours:** The measure of time that will be used to measure how often the delta CRL will be published. Since this is often much smaller than the full CRL, less resources are required to publish it more often. For Windows clients that can use Delta CRLs (as of this writing, only Windows XP and Windows Server

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2003), if a certificate is revoked during a particular day, this change will be picked up during the client's revocation checking process.

i. **CRLDeltaPeriodUnits:** The number of CRLDeltaPeriods used to determine how often to publish delta CRLs. DTI selected 12 so delta CRLs will be published every 12 hours.

```
[Version]
Signature= "$Windows NT$"

[PolicyStatementExtension]
Policies=DTICertPolicy

[DTICertPolicy]
OID=1.5.6.1.1.1.5002.1000.1.1.1.1
URL="http://security.dtinet.com/certpol.html"

[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=3
CRLPeriod=Days
CRLPeriodUnits=3
CRLDeltaPeriod=Hours
CRLDeltaPeriodUnits=12
```

Listing 3-6: CAPolicy.inf file used for DTI's issuing CAs.

3. **Time Syncrhonization:** Since issuing CAs will be servers in the root domain, they will automatically synchronize with the PDC emulator in the root which is DTI-RT002.

4. **Installed Certificate Services from Add/Remove Programs:** Used the default of both the Certificate Services themselves and the Web Enrollment support. The table below details the settings and options that were selected during the CA portion of the installation.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CA Install Wizard Screen	Property Name	Value Entered
CA Type	CA Type	Enterprise subordinate CA
CA Type	Use custom settings to generate the key pair and CA certificate	Ensured the box was checked.
Public and Private Key Pair	CSP	Microsoft Strong Cryptographic Provider
Public and Private Key Pair	Hash algorithm	SHA-1
Public and Private Key Pair	Key length	2048
Public and Private Key Pair	Allow this CSP to interact with desktop	Checkbox cleared (default)
CA Identifying Information	Common name for this CA	Issuing CA X where X is a number starting from 1 of the CA.
CA Identifying Information	Distinguished name suffix	DC=DTIROOT,DC=NET
CA Identifying Information	Validity Period	Greyed out stating 'Determined by parent CA". This then is 5 years as configured on DTI Root CA.
Certificate Database Settings	Certificate Database	D:\Certlog
Certificate Database Settings	Certificate Logs	L:\Certlog
Certificate Database Settings	Shared Folder	D:\CAConfig
Confirmation Box	Confirming location of certificate database files	Clicked Yes to continue.
CA Certificate Request	Save the request to a file	Use default file name or save to <Server Name>.req
Warning Dialog Box	Warning that web enrollment will not work without IIS being installed (which it was not).	Clicked OK to continue.
Warning Dialog Box	Warning that installation is not complete until certificate request file is approved by parent CA	Clicked OK to continue.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table 3-5: Properties of the Certificate Services install wizard and the values the ITC group entered when installing them on the issuing CAs.

NOTE: When saving the request files or subsequently issued certificates, the files are saved on floppies, transported and used wherever they need to go. The files are deleted when no longer need, then the floppy disks destroyed.

5. ITC did not install IIS on the issuing CAs. Although it is in their plans to roll out certificates to non Windows systems such as routers and switches, they have opted to install IIS only when needed.

6. **Certificate Approved by DTI Root CA:** The .REQ files were taken to the root CA on floppy disk and the certificates issued as follows:
   a. Logged into DTI Root CA a member of the ITC Root CA Admins group.
   b. Launched the Certification Authority snap-in. Right clicked the name DTI Root CA and selected All Tasks\Submit New Request. Browsed to the file and then clicked Open. The request now appeared in the Pending Requests node.
   c. The pending request was viewed in the Pending Requests folder, right clicked, and All Tasks\Issue selected from the menu.
   d. The certificates would now appear under the Issued Certificates node. Going into the properties and moving to the Details tab would allow both verification of the desired settings (see the table above for details on the key lengths, server name, etc.) and the ability to save the certificate back to floppy. To save the certificate, click on the Copy to File button. Using the defaults was sufficient for transferring back to an issuing CA.
   e. Installed the certificate on the issuing CA by using the the Certification Authority snap-in. Right clicking the node with the name of the CA and selecting Install CA Certificate from the menu. They had to change the Files of type drop down list box to X.509 before they could see the file on the floppy. Finally, they clicked Open.

      Before this was done, the Certificate Services service would not start. To start they right clicked the name of the CA and then selected All Tasks\Start Service from the menu.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

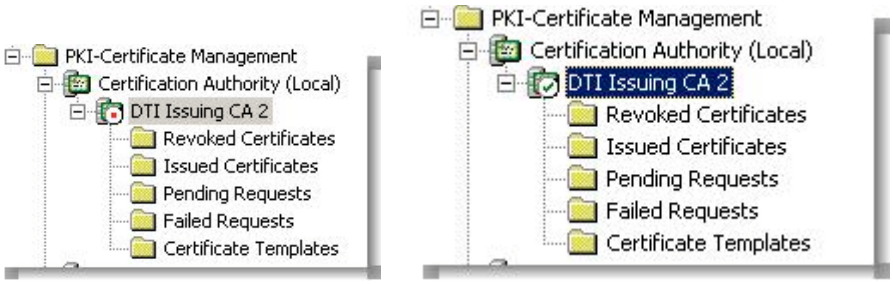


Figure 3-11: Certification snap-in showing Certificate services before and after CA certificate was installed.

7. **Publishing CRL and AIA Information:** For the most part, the defaults can be taken here, especially with respect to installing into the Active Directory. However, the only change that was made was the HTTP address since IIS is not being installed on the issuing CA servers for the time being.

   The HTTP value was set to http://security.dtinet.com/%3%8%9.crl or %1_%3%4.crt for CRLs and AIAs respectively.

   The properties for the AIA information was set exactly the same as it was for the root CA with no OCSP protocol configuration. However, there are some differences between issuing CAs and the root since the issuing servers are always online with regards to CRLs and are publishing delta CRLs.

	CDP Property	Default File Location	HTTP	LDAP
	Publish CRLs to this location	Selected		**Selected**
	Include in all CRLs			**Selected**
	Include in CRLs		Selected	**Selected**
	Include in the CDP extension of issued certificates		Selected	**Selected**
	Publish delta CRLs to this location	**Selected**		**Selected**

Table 3-6: Properties the ITC group selected for each CRL distribution point for issuing CAs. A blank cell indicates that this option would normally be greyed out in the interface and not applicable to that particular

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CDP location. A cell with Cleared in it means that the root CA administrators purposely cleared this check box or left it empty. Finally, a cell with Selected in it means that administrators intentionally configured this setting or left it on by default.

8. **Verified CRL Publishing Interval:** Using the Certification Authority MMC, administrators went into the Revoked Certificate properties and saw that CRLs were to be published every 3 days and delta CRLs were to be published every 12 hours.

9. **Verified the Certificate Chain:** This was performed to ensure that no clients would encounter errors trying to verify the chain. This was done using the PKI Health Tool from the Windows Server 2003 Resource Kit. The tool will verify all the CDP and AIA paths for the entire chain of CAs up to the root just as a client would and display that information graphically. After installing the Resource Kit, ITC added the tool to the PKI-Certificate Management portion of their Network Services Admin MMC. It appears simply as Enterprise PKI.

iii. Locking Down the Certificate Authorities:

Since these servers are amongst the most sensitive in the company, special measures have been taken to lock down these computers and make them more resistant to compromise.

1. **Changing the Default CA Permissions:** Using the Certification Authority MMC and going into the Security tab of each CA's properties, the default groups and permissions were removed and replaced with the groups seen in Figure 3-12.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

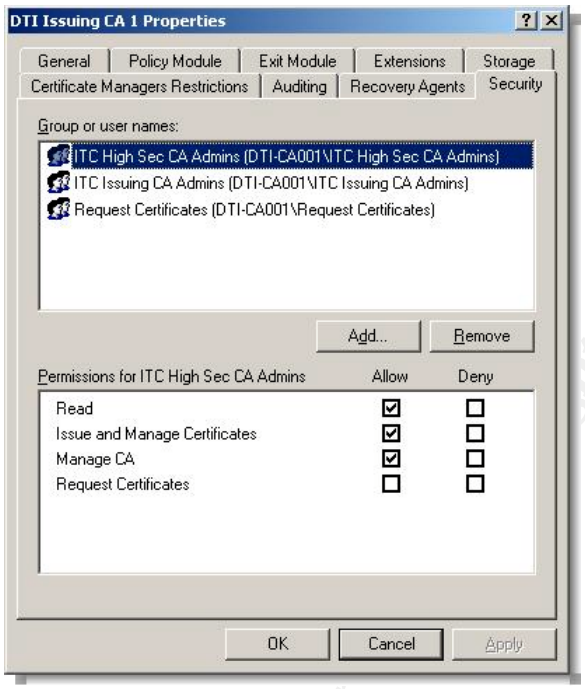


Figure 3-12: The permissions set by the CA administrators on the issuing CAs. The groups are local groups on each CA to which domain global groups have been added.

a. ITC High Sec CA Admins: A universal group which has only 3 senior ITC group members in it including the CIO. These are the only people that can issue certain templates deemed to need higher security as well as all others. They can also administer the Enterprise CAs.
b. ITC Issuing CA Admins: Also a universal group which contains 4 ITC members. There are no members from the High Sec group in this one. They can issue all template except those deemed high security. They can only issue CAs not deemed high security.
c. Request Certificates: A universal group with only the permissions to do just that; request certificates. This does not include the Everyone or Authenticated users groups. Only the Domain Users groups from both the parent and root domains, DTI Business Partners, and the Domain Computers groups from domains are members.

   On high security CAs, only the DTI Executives are members of the Request Certificates group and only the ITC High Sec Admins can administer the CAs. Table 3-7 lists the local groups and their permissions on each type of CA.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

On DTI Root CA, the members of the ITC High Sec CA Admins had to have local accounts created for each of them since that computer is not on a domain. Every certificate issued must be approved manually by one of the administrators.

	Local Security Group	Permissions on Issuing CAs	Permissions on High Security Issuing CAs	Permissions on DTI Root CA
	ITC High Sec CA Admins	Read, Issue and Manage Certificates, Manage CA	Read, Issue and Manage Certificates, Manage CA	**Read, Issue and Manage Certificates, Manage CA**
	ITC Issuing CA Admins	Read, Issue and Manage Certificates, Manage CA		
	Request Certificates	**Read, Request Certificates**	**Read, Request Certificates**	

Table 3-7: Each local group that has permissions on all types of CA. Each permission is separated with a coma.

2. **Applying Security Templates:** Security templates were used to further lock down the computers on which the CAs resided. The same template used on DTI Root CA was imported into the Certificate Authorities group policy for the Enterprise CAs. Since universal groups were used on all CAs, no special modifications had to be made to any group related policies.

III. Certificate Management Implementation:

The ITC group decided upon a certificate deployment and revocation strategy that leverages the auto-enrollment capabilities of Windows Server 2003 and Windows XP on client computers. The strategy for the management of certificate templates then, as discussed earlier, is that for each template they would need, they will create a new version 2 template based certificate from existing ones. The rationale being that they can have more control over the design of the certificates and ensure that their needs were met.

Some team members expressed concern that some users and servers could not immediately benefit from the PKI implementation until they were upgraded from Windows 2000 Professional and Server to XP and 2003 respectively. This was a legitimate concern because, while the ITC desktop group was already well into the process of migrating their

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

users to Windows XP, there was still at least two or three months remaining in that project. As far as the servers were concerned it would be six months to a year before some of those were upgraded. For example, the ITC messaging team was still evaluating Exchange 2003 and was not moving to it for a minimum of six months to a year. Exchange 2000 cannot be directly installed onto a Windows Server 2003 server (although it can exist in a fully Windows 2003 based domain).

In order to address this, two issuing CAs in the Calgary and Toronto offices were installed with IIS and the web enrollment pages so that Windows 2000 users can use this distribution method of requesting version 2 certificates as the only prerequisite for making this kind of request is that Windows 2000 must be running a minimum of Service Pack 2.[17] All Windows 2000 machines (workstations or servers) on DTI's network were running Service Pack 4. Users logging on at a Windows XP workstation would get automatically enrolled for one of the new certificates and could then use them from their Windows 2000 workstations. If the certificate were to change for some reason later on, the user would either have to use the Web Enrollment pages again to get a new certificate or log on to a Windows XP machine in order for it to happen automatically.

Servers needing specific templates, such as the intranet servers, and still running Windows 2000 will use version 1 templates and will have those superceded by newer version 2 templates when they are migrated to Windows 2003. As previously stated, ITC will perform fresh installs on servers rather than upgrading.

The project team, early on, identified one particularly special certificate template need during their planning for the DTI's executive team. Current corporate policy dictates that certain documents such as pay raises, corporate policies, etc. need to be signed by someone at the corporate executive level. Therefore, they have decided to create a special template that only corporate executives could obtain. People verifying signatures would have to also ensure that a certificate of this level was used in order to validate the document.

Other templates identified as being needed during the planning stages are described in Table 3-8 below. Note that only

[17] "Implementing and Administering Certificate Templates in Windows Server 2003." Administering Version 2 Templates: The Security Tab. 2003
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/ws03crtm.asp (November 10, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Template Name	Type	Certificate Purpose	Created from Template	Supercedes	Who Can Enroll
	DTI User	Version 2	EFS, secure e-mail, authentication	**User**	**User**	**General DTI user population**
	DTI Executive	Version 2	EFS, secure e-mail, authentication	**User**	**User**	**Only users who are members of the DTI Executives group. They are explicitly denied from enrolling for a regular user certificate.**
	DTI Computer	Version 2	Encryption, server authentication	**Computer**	**Computer**	**Most servers and administrative workstations**
	DTI Web Server	Version 2	Encryption, server authentication	**Web Server**	**Web Server**	**Server who are member of the DTI Web Servers group. This group is explicitly denied from enrolling for the Web Servers version 1 certificate.**
	Web Servers	Version 1	Encryption, server authentication			**Windows 2000 servers who are members of the DTI Web Servers – W2K group.**
	DTI EFS Recovery Agent	Version 2	File recovery	**EFS Recovery Agent**	**EFS Recovery Agent**	**Members of the ITC Data Recovery group.**
	Key Recovery Agent	**Versio n 2**	**Encryption**			**Users who are members of the ITC Data Recovery group.**

Table 3-8: Indicates the certificates the ITC group used in the initial roll out of their PKI. Blank cells in any particular column indicate that particular item is not applicable. If a certificate is of type version 2 and it has a blank "Created from Template" cell, it means that it was a new template added when upgrading to the Windows 2003 schema.

i. Implementing and Configuring a Version 2 Certificate Template

In Table 3-8, one can see there were a number of templates which the ITC group implemented during the PKI rollout. Most of their strategy hinged on setting up version 2 templates so it is important to walk through the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

configuration of one to understand how they are being managed. This section will go through the steps used to create the DTI Executives certificate. Similar management techniques were applied to the other version 2 templates created.

1. **Managing the Templates for Particular CA Roles:** The DTI Executives certificate is only available on a high security issuing CA. On all of the CAs however, any certificates for which a CA was not supposed to responsible were removed by going into the Certificate Templates node of the Certification Authority and deleting them. In the case of the DTI Executives template, it had to be created and then added to the CA.

2. **Creating the Version 2 Template:** Using the Certificate Templates snap-in, the procedure was as follows:
    a. Right clicked the User (version 1) template and selected Duplicate from the menu.
    b. **On the General Tab:**
        - The template display name, which appears in the Certification Authority and Certificate Templates MMCs was set to DTI Executives.
        - The template name automatically became DTIExecutives (no space). Note the space was removed automatically based on the name typed into the display name. This name could have been changed if needed. This is the name that will appear in the CN=Certificate Templates,CN=Public Key Services,CN=Services,DC=DTIROOT,DC=NET container.[18]
        - Validity period was left at the defaults of one year. The default renewal period of six weeks means that the certificate will be renewed six weeks before it is due to expire.
        - Publish certificate in the Active Directory was the default based on the User template and this, obviously was and should have been left. Certificate templates will allow users to automatically reenroll should the template change for some reason (such as to change validity times, change the purposes, etc). This option was left intact.
    c. **On the Request Handling Tab:**
        - The purpose of the certificate was left at Signature and Encryption which means that it can be used for EFS, digital signing, etc.

[18] "Implementing and Administering Certificate Templates in Windows Server 2003." Administering Version 2 Templates: The General Tab. 2003
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/ws03crtm.asp (November 10, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Archive subject's encryption private key was selected. This was selected since many of the executive team have or were to be getting Windows XP laptops on which they would most likely encrypt data. Should they leave the company or encounter any problems not being able to access their private key, the members of the ITC Data Recovery group would be able to retrieve the users encryption key to decrypt the data. The three elements necessary to enable key archiving and recovery were present. First, key recovery certificates must have been issued to recovery agents, the certificate must allow the key to be archived and the CA itself was configured to allow key recovery.
- The key was set to 2048 bits to make these very important certificates harder to break. Especially considering the fact that the certificates are still only valid for one year like the normal Users template.
- Enroll subject without requiring any user input was the default and left this way. As alluded to earlier, DTI has very strict security policies regarding who can become a member of the DTI Executives group. That being the case, ITC deemed it best to make it as simple as possible and never have to make any special effort to acquire their certificates other than logging onto a Windows XP machine.
- Cryptographic service providers (CSPs) were left at their default since these are also supported on client machines. Should a CSP that it not supported on a client be chosen, then auto enrollment will fail.

d. **On the Subject Name Tab:** The default option for building the name from the fully distinguished name from Active Directory was retained. Include e-mail name in subject was also chosen (since this certificate can be used for secure e-mail). The alternate subject names options using the e-mail name and the user principal name (UPN), a way of uniquely identifying a user object by means of name which resembles an SMTP e-mail address, were selected.
e. **On the Superceded Templates Tab:** The User, DTI Users, Basic EFS certificates were selected. Should a DTI Executive be enrolled for any of these such as, for example, before they received a promotion to executive status, the DTI Executive will replace either or these certificates through the re-enrollment process. The EFS certificate is included to ensure that the newly issued certificate is the one used for any EFS encryption operations.
f. **On the Security Tab:** Displayed in Figure 3-13 there are three global groups configured. It is recommended that global groups rather than domain local or machine local groups be used in

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

assigning permissions to templates as they are stored in the configuration container in Active Directory. The ITC group did encounter some problems with users being unable to enumerate the certificates and, therefore, being unable to autoenroll because they tried using local groups on the CAs. They have opted to use global groups on the issuing CAs as well since they encountered difficulties with this too using local groups.

Note the Cert Publishers global group (which CAs in a particular domain are added to) must have at least Read permissions on a certificate for it to be able to offer the template to users who have the necessary rights. The DTI Executives group has Read, Enroll, and Autoenroll which are all necessary to be able to autoenroll for this certificate. Finally, the ITC High Sec CA Admins group only has Read and Write permissions which is sufficient for that group to be able to modify the template and assign permissions, but they cannot enroll for this certificate manually or automatically.

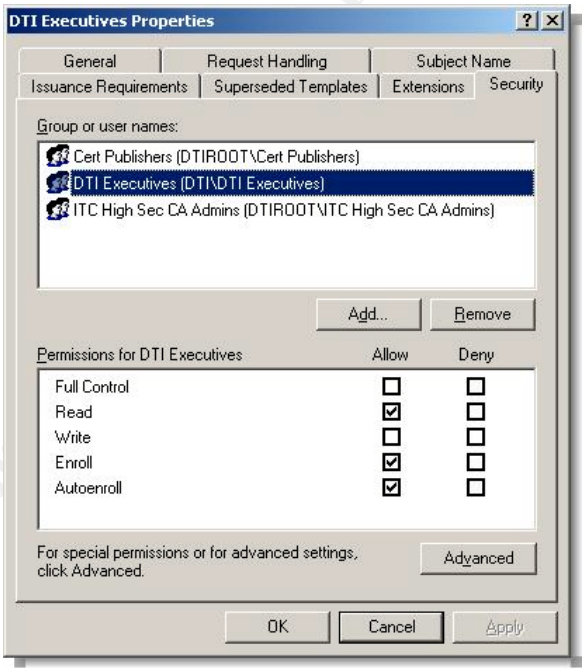


Figure 3-13: Permissions on the DTI Executives version 2 certificate. Note the DTI Executives group has the Read, Enroll, and Autoenroll permissions which are all necessary to enable autoenrollment for this certificate.

g. **On the Remaining Tabs:** None of the options on the Issuance Requirements or Extensions tabs were changed. For more details about the options on these tabs, see the "Implementing

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and Administering Certificate Templates in Windows Server 2003" whitepaper at the following URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/ws03crtm.asp

The other certificate templates were configured using similar permissions techniques and configurations. Once certificates were enabled for the appropriate CAs and replication was allowed enough time, minimal enrollment issues were encountered. The most important thing was to ensure that clients had the Read permission on the certificate templates or they were unable to "see" them in AD and subsequently enroll using them.

One item of extreme importance to note is the fact that the project team encountered an issue in which users in the DTI child domain could not autoenroll for certificates even when setting permissions using the proper global groups and rights. Some research on the Microsoft Knowledge Base led them to article 219059. Essentially, the article indicated that the Cert Publishers group from the DTIROOT domain in which the CAs were installed did not have the permission to read or write to the userCertificate attribute of users in the DTI child domain.

The circumstances the article describes were not exact in that both the root and child domain existed before the introduction of any enterprise CAs yet the root's Cert Publishers global group still did not have these rights. The first workaround the article suggests, to add the CAs from the root into the child's Cert Publishers group did not work because of the fact that global groups can only have members from their own domains. The option to change the group type on Cert Publishers was greyed out as well.

The second solution to delegate the right to the root Cert Publishers group did work using the Delegate Control wizard applied at the top of the DTI.DTIROOT.NET domain only to User objects (which also set it for computer accounts as well). For more information on Microsoft Knowledge Base article 219059, use the URL below: http://support.microsoft.com/default.aspx?scid=kb;[LN];219059

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

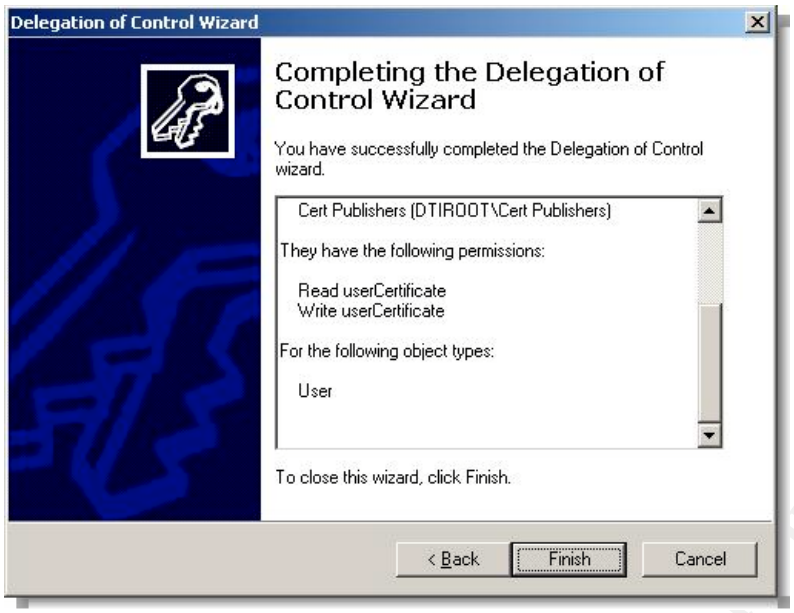


Figure 3-14: Final page of the Delegation of Control Wizard used in giving the Cert Publishers group read and write permissions to the userCertificate attribute on accounts in the DTI.DTIROOT.NET child domain.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Chapter 4: Applications Leveraging the Public Key Infrastructure

The ITC PKI project group decided to limit the scope and focus on applying the PKI infrastructure to specific applications of the technology while keeping the design flexible enough that it could be expanded at a later date once some real world production experience had been gained.

The applications of the technology they decided upon are:

1. **Digital signing of documents:** One of the major hurdles that have been restricting the use of electronic forms in the organization is the need for the ability to securely sign documents.
2. **Secure E-mail:** Which includes both digital signing and encryption.
3. **Encrypting File System:** The management of user encryption keys and the keys of recovery agents is much easier with a centrally managed PKI.

Once the certificates had been deployed to a number of user and computer accounts, it was time to actually test them being used with the various applications with which they would be used by the user community.

I. Securing E-mail

The term secure e-mail in the context of this discussion involves the ability to either digitally sign a message, encrypt it, or both.

Two of the people who were initially auto-enrolled for certificates were two executives. Bill Ellison (President and CEO) and Larry Gates (Chairman and Chief Technologist). Both members of the DTI Executives group.

The test was to have Bill send a signed message to Larry and then Larry would reply with both a signed and encrypted response. Since the message was being sent to Bill, only he should be able to read it, despite an administrator, having rights to his mailbox.

i. Composing the Initial E-mail:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Using Outlook 2002 as their e-mail package, the procedure was as follows:

1. Larry started a new mail message and went to the View\Options menu. In the Message Options window, he clicked on the Security Settings button.
2. In the Security Properties windows, Bill selected the Add digital signature to this message option which automatically selects the Send this message as clear text signed option.
3. In the Security Settings section he clicked on the Change Settings button. This was done mainly to verify that his certificate was "visible" to Outlook. The default options were selected based on what was supported by Windows XP. Recall that digitally signing a document or e-mail involves encrypting a hash of the message. That is why the hash algorithm and encryption algorithm are needed despite the fact that Bill is not encrypting the entire message.

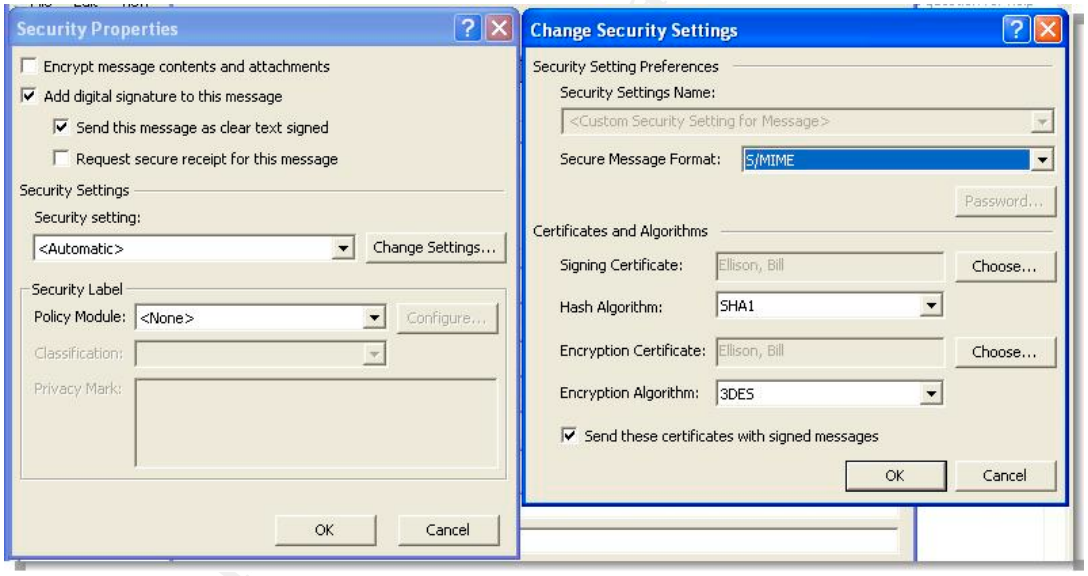


Figure 4-1: Security Properties and Change Security Settings windows in Microsoft Outlook 2002. Note that in the Signing Certificate and Encryption Certificate windows, Ellison, Bill appears and is greyed out. This means that it is the only available certificate for this function on the machine at the moment.

4. Bill clicked OK in the windows he had open in order to save his changes. He then sent the message to Larry Gates.

ii. Reading the Secured E-mails:

1. Larry Gates opened Outlook 2002 on his Windows XP based laptop and opened Bills e-mail message. In the top right hand corner was a red ribbon icon as shown in Figure 4-2. This indicated that the message was signed. Just below the Subject line in the message was

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

a line showing the e-mail address of the person who signed the message. This information is pulled from the certificate and it is why it is important to include that information in AD based certificates such as DTI Executives. Double clicking the red ribbon icon allowed Larry to verify the signature or, more specifically, the certificate used to sign the message. All green check marks indicate that

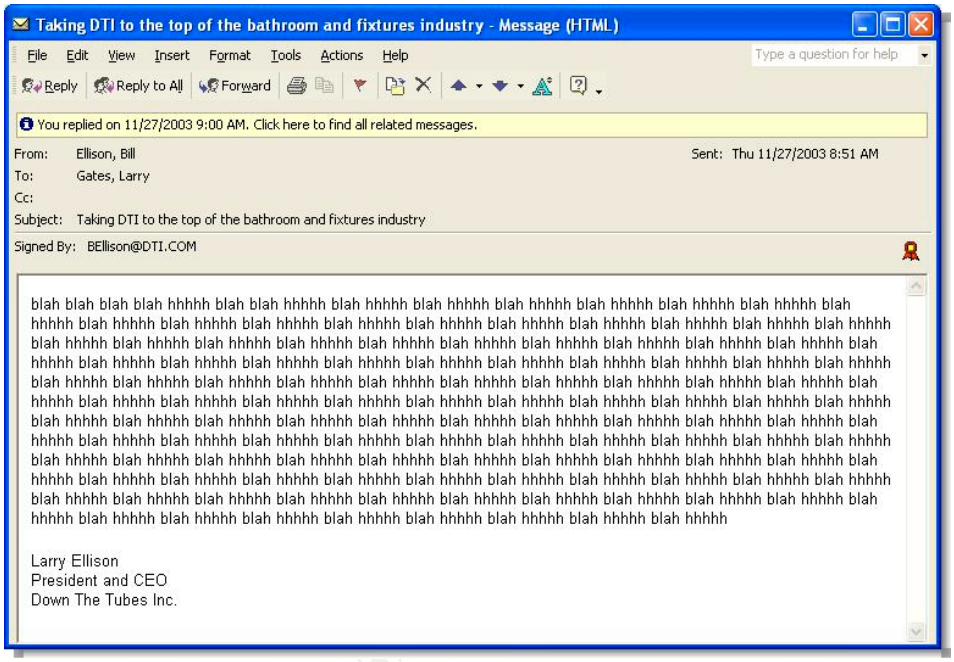
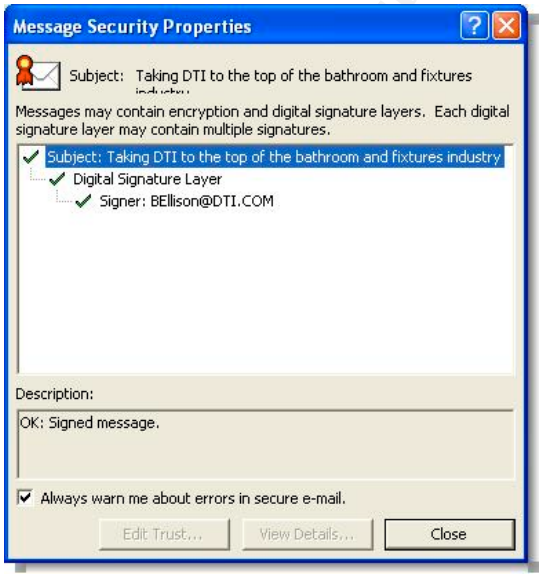


Figure 4-2: Signed message from Bill Ellison. Note the red ribbon icon in right hand corner above the message window and the "Signed By:" section under the Subject line. Double clicking the red ribbon will allow one to verify the certificate. See Figure 4-3.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figure 4-3: Message Security Properties window that opens when the red ribbon signature icon is double clicked.

2. Larry then composed a reply. He opened the Security Properties window and not only selected the Add digital signature to this message option and its default setting, but the other two as well. The Encrypt message contents and attachments option will encrypt the entire message so that only the recipient with his private key can read its contents. Even and administrator with full rights to the mailbox could not read the message. The Request secure receipt for this message option sends a read receipt back which is signed by the recipient. When this message is received, the red signature icon is available so that it can be verified that the intended recipient did in fact get the message.
3. Bill opened the reply with no issue from his laptop.
4. An administrator opened Bill Ellison's mailbox and attempted to read Larry's reply. He could not and received an error message shown in Figure 4-4.

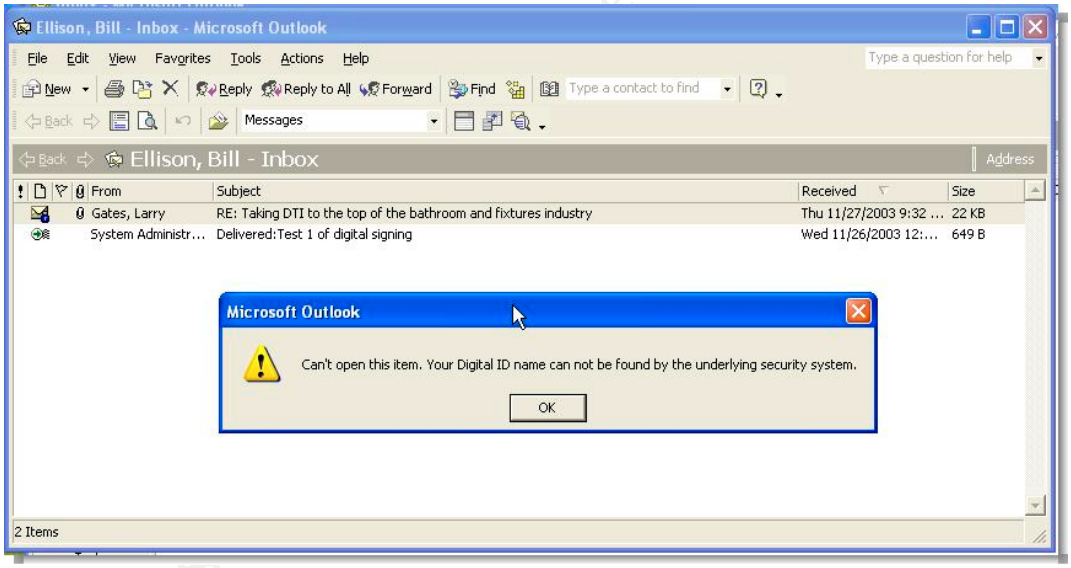


Figure 4-4: Error message received by an e-mail administrator attempting to read an e-mail encrypted for Bill Ellison. Only Bill with his private key could decrypt the message.

II. Digitally Signing a Word Document

The next set of tests involved digitally signing a Word document. On a shared network drive, Larry Gates created a Word document called Test Doc 1.doc.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Larry went to the Tool\Options menu. Then he clicked on the Security tab.
2. He then clicked on the Digital Signatures button. In the Digital Signature windows, he clicked Add. He was then able to view his certificate as shown in Figure 4-5.

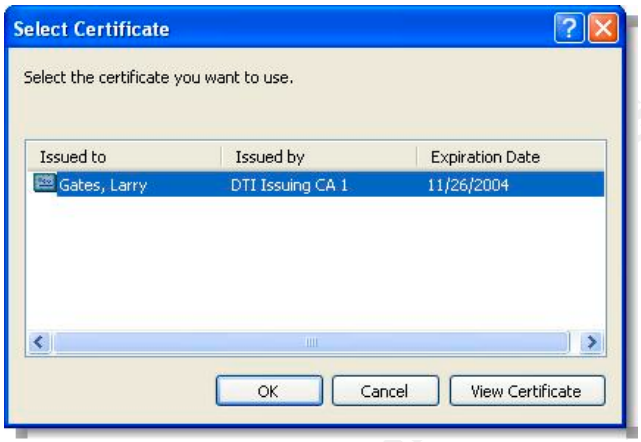


Figure 4-5: The Select Certificate window where Larry has the opportunity to select his certificate to sign his document with.

3. Larry clicked OK to save his changes in all the windows that were opened.
4. Bill Ellison then open the document and went to the Digital Signatures windows to view the signer's certificate (in this case Larry Gates) and verify that it is indeed his.

III. Using the Encrypting File System

The Encrypting Files System (EFS) allows users to be able to encrypt documents locally on their computers should unauthorized people gain access to the hard disk. The ITC groups strategy for their users is to have their laptop users use one particular folder on their hard disks to encrypt documents as this can resolve some potential insecurities. Additionally, they also want Windows XP laptop users (which ultimately will be all laptop users) to encrypt their Offline files cache. This was not possible in Windows 2000.

The ITC project team wanted to test users ability to encrypt files using their CA issued certificate and the ability of a member of the ITC Data Recovery groups ability to decrypt them.

1. Larry Gates was kind enough to accommodate this test. He created a directory on the hard disk of his laptop called Secured

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Info. He then went into the properties of the folder and clicked on the Advanced button.

2. The Advanced Attributes window opened. Checking the Encrypt contents to secure data option will encrypt that folder and anything that gets added to it after that fact. This is done to avoid documents existing on the hard drive before being encrypted since the unencrypted files could possibly be recovered using a disk editor.

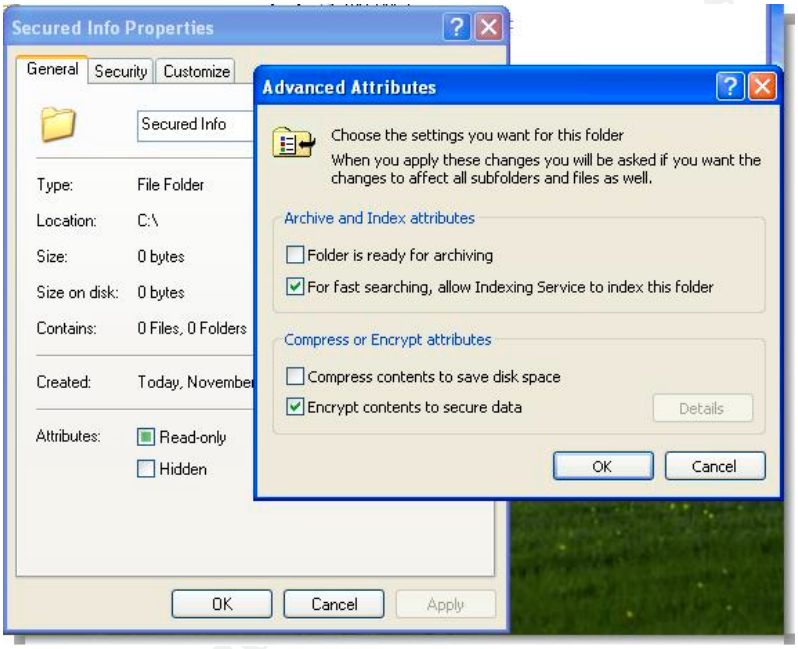


Figure 4-6: The Advanced Attribute properties of the Secured Info folder. Checking of the Encrypt contents to secure data option will encrypt that folder and anything subsequently added to it. Once this is done. Going back to the Advanced Attributes and clicking on Details will allow additional *individual* users to be added.

3. Larry then added a Word document to the folder called Test Doc 2.doc. Examining the Advanced Properties of that file revealed that it too was encrypted.
4. Checking Larry's certificate store showed that the only certificate available was the one issued by DTI Issuing CA 1.
5. Logging on as Bill Ellison to Larry's laptop revealed that Bill could not open the file. Going into the Secured Info folder and double clicking Test Doc 2.doc only yielded the error message displayed in Figure 4-7.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Figure 4-7: Error message yielded when Bill Ellison attempted to open a Word document previously encrypted by Larry Gates despite having the necessary NTFS permissions.

6. Logging on as an administrator with the DTI EFS Recovery Agent certificate allowed the encryption property to be changed and the file decrypted so it could be read. The agent had to be added as one to the group policy for the domain before this would work.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Conclusions

Rolling out a public key infrastructure requires extreme amounts of patience and planning. The planning paid off in minimizing the problems the project team encountered during and after the completion of the initial phase.

The ITC group will evaluate and document how the day to day operation proceed over the next few months and, once the Windows XP migration is over, possibly implement more PKI applications.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

List of References

1. “SearchDatabase.com Definitions.“ Hashing. March 12, 2002.
URL: http://searchdatabase.techtarget.com/sDefinition/0,,sid13_gci212230,00.html (November 5, 2003)

2. Cross, David“PKI Enhancements in Windows XP Professional and Windows Server 2003.“ Qualified Subordination. July , 2001.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/Plan/PKIEnh.asp (November 4, 2003)

3. “How to Upgrade Windows 2000 Domain Controllers to Windows Server 2003.“ Microsoft Knowledge Base 325379. July 30th, 2003.
http://support.microsoft.com/default.aspx?scid=kb;en-us;325379&Product=exch2k (November 2, 2003)

4. “Windows 2000 Domain Controllers Require SP3 or Later When Using Windows Server 2003 Administration Tool.” Microsoft Knowledge Base 325465. September 22nd, 2003.
http://support.microsoft.com/default.aspx?kbid=325465 (November 2, 2003)

5. “Windows Server 2003 ADPREP Command Causes Mangled Attributes in Windows 2000 Forests That Contain Exchange 2000 Servers.“ Microsoft Knowledge Base 314649. July 1st, 2003.
http://support.microsoft.com/?ID=314649 (November 2, 2003)

6. Deuby, Sean. "Windows Server 2003 Command Line Utilities" Windows & .NET Magazine April 2003 (2003): 81- 82.

7. “Microsoft Windows 2000: Upgrading Domains to .NET Server.“ Microsoft Support Webcasts. February 18th, 2003.
URL:
http://support.microsoft.com/default.aspx?scid=/servicedesks/webcasts/en/wc021803/wct021803.asp (November 17, 2003)

8. “Windows 2000 FSMO Roles.“ Microsoft Knowledge Base 197132. October 10th, 2002.
URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;197132 (November 2, 2003)

9. Minasi, Mark. “Mastering Windows Server 2003”. San Francisco:
Sybex Inc., 2003. 599

10. Microsoft Corporation. “Microsoft Windows Server 2003 Deployment Kit: Designing and Deploying Directory and Security Services”. United States of America:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Microsoft Corporation., 2003. 380

11. “Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure.“ Appendix B: Parameters for a Three Tier CA Topology.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp (November 12, 2003)

12. “Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure.“ Offline Root CA Configuration.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp (November 12, 2003)

13. “Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure.“ Offline Root CA Configuration.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp (November 12, 2003)

14. “Windows Server 2003 Product Documentation.“ Manage Certificate Revocation.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_csprocs_cdp.asp (November 16, 2003)

15. “Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure.“ Offline Root CA Configuration.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp (November 16, 2003)

16. “Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure.“ Offline Root CA Configuration.
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws3PKIBP.asp (November 12, 2003)

17. “Implementing and Administering Certificate Templates in Windows Server 2003.“ Administering Version 2 Templates: The Security Tab. 2003
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/ws03crtm.asp (November 10, 2003)

18. “Implementing and Administering Certificate Templates in Windows Server 2003.“ Administering Version 2 Templates: The General Tab. 2003
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/ws03crtm.asp (November 10, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.