Global Information Assurance Certification Paper

Securing Windows 2000 With Security Templates: Focussing on Windows 2000 Smart Card Logon and Windows 2000 Certificate Services

By Malcolm Cook

Securing Windows GCNT Practical Assignment
v3.0 (August 2001)
Option 2 - Securing Windows 2000 With Se curity Templates

Table of Contents

1. Scope

The focus of this paper will be directed towards Windows 2000 Cer tificate Services with the goal to securely enroll users for smart card logon (and subsequently those users should be able to log onto our domain). The base platform will be Windows 2000 Advanced Server with Service Pack 2 installed. Certificate Services will be installed once the server has been promoted to a domain controller, and a security template, supplied by Microsoft, will be installed over this. Then the system will be analyzed for any potential flaws or weaknesses, particularly those pertaining to Windows 2000 Certificates Services and Windows 2000 Smart Card Logon and the security of the overall system.

The security template that will be analyzed forthwith will be the (heavily modified) Highly Secure Domain Controller template (hisecdc.inf) co mbined with the default Windows 2000 and Domain Controller templates (a combination of templates that can be re -installed which match the "out of the box" settings). These come by default when the server is installed, which is part of the reason why they were chosen. The default "out of the box" templates take care of a lot of registry permissions and file permissions so it is important that these be reapplied before our template is applied (which will no doubt be modified to suit our purposes).

1.1 Requirements

Before we delve into the details of security templates it might be pertinent to briefly look at what we want to secure:

1. Firstly we want to secure our logon process. Adding smart cards into the system adds a lot more security over password -based logons, provided the issuing system is also secure.
2. Access to the domain controller along with all of its resources like user accounts, IIS, certificate services (along with access to your CA's all important private key) will need to be secured using appr opriate policies, permissions and roles.
3. Access to the smart card issuing station (in this case the same domain controller, but delegation could have been used to separate them) and the important enrollment agent digital identity (again with another important of private key).

The level of security required would be medium to high given the fact that the target audience will most likely be small to medium sized organizations. While a lot of what will be discussed could be applied to larger organizations, they would have to take into account that their will only be a single root CA used for issuing the smart cards, and in an ideal world you would one or two more tiers in the CA hierarchy.

Additional third party hardware and software was required to enable s mart card enrollment to take place. The TrustedNet Connect smart card suite will be used which comes with a smart card based CSP (a necessity with all W2K smart card logon domains) and can make use of any PC/SC enabled reader

(in this case a GemPC410). The smart card that was used was a Multos 4 smart card (with the TrustedNet Digital ID application loaded), which has been highly rated in terms of the application loading and chip security (at least in Australia). The actual smart card and software chosen is not really that relevant to the discussion involving security templates and will not be analyzed in any great detail, apart from being used for visualization purposes.

1.2 Reasoning

The reason why this particular checklist was chosen was more due to the absence of a template particularly geared towards Certificate Services, smart card enrollment and smart card logon, rather than it being particularly suited to the details entered into previously. There were several checklists available from the NSA with regard to Certificate Services and IIS, but as these were not provided as part of the NSA's security template it was felt that they might be best used as a reference when trying to improve on the Highly Secure Domain Controller template provided.

There is another reason for using the NSA's template as a reference and not a basis for the template that will be used and that is while the NSA may have a high reputation in the security industry, they also have a reputation for somewhat looking after there own self interests rather than benefiting the security industry as a whole (this might be only from an international perspective). Thus their reputation for delivering independently sound security advice has yet to be proven on a world scale.

The reason for choosing certificate services, smart card enrollment and smart card logon to examine specifically was due to the author's familiarity in this area, and the pursuit of knowledge in learning how to roll these services out securely while maintaining functionality and relative ease of use.

Smart cards in particular have an illusive quality about them. They have a reputation for providing high security (through two factor authentication) when deployed effectively, but likewise have a reputation for being extremely difficult to roll out and deploy within an organization. Unfortunately computers never come with smart card readers by default and thus do we not only have to issue users with one extra hardware device, but two. Then there is the added complexity of deploying them effectively with an appropriate security policy (both on the domain and in general). All up the costs of rolling out smart card based authentication systems have usually been left to organizations like banks and their customers where they have no choice but to secure there systems, but now with many services being installed by default on Windows 2000 systems (and ideas such as plug and play which sometimes actually work) the cost of administering these systems is dropping, which can offset the cost of the smart card readers and smart cards themselves.

All it will take for smart card uptake to be accelerated is for the awareness of the security benefits to be greatly increased and thus this is one of the prime reasons why this particular slant on this topic has been chosen.

1.3 Expectations

Once the appropriate components have been installed and we have installed the Highly Secure Domain Controller template, one would expect some of our requirements to be addressed. However as the accoun t operator groups permission may need to be expanded to allow access to the CA private key and appropriate certificate templates (when enrolling for enrollment agent certificates and issuing users smart cards) this may cause the need for the template to be modified. Some of what will be changed will be driven by common sense, but the "Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services", published by the NSA, will also be extensively used as a reference (part icularly when they recommend something that differs from setting set by the template or those which exist by default). Various utilities, provided by Microsoft (such as secedit.exe, Security Configuration and Analysis snap -in and Fazam), will be used to track changes to the group policy and security policy before and after the template has been installed and also when manual changes are made to the system. These manual changes will hopefully be able to be added to the template to improve its usefulness wh en applied to a domain where smart cards will be predominately used.

Let us break down the expectations into something quantifiable:

- One group should have the permission to issue smart cards and create user account
- Minimum number of password based accoun ts
- Restricted use of the CA private key (only enable smart card logon certificate template and enrollment agent certificate template)
- Enforcement of smart card removal behavior on all machines within the domain
- Administration of the server (apart from user creation and smart card enrollment) should be able to be performed with an account which uses a smart card to logon

Looking at it from a human perspective at minimum we need:

- One person to administer the system – will be issued a smart card once the domain has been fully installed
- One person to create user accounts and issue smart cards – will need to logon using a password
- One or more authenticated smart card logon users – will be issued with smart cards once the domain has been fully installed

1.4 Tasks

The following tasks summarize the process that will be required to get the domain into a usable state:

1. *Install the domain controller*

   This task will begin with installation of the Windows 2000 Advanced Server operating system. Before we perform anyth ing useful, like install Active

Directory, we must have networking installed on the machine. This can be achieved without a network (or network card) by installing the Microsoft Loop-back Adapter. Once we have configured the server we can begin with the promotion of the server to a domain controller, which involves the installation of Active Directory and other sundry items.

2. Install the Windows 2000 Service Pack 2
This must be installed at this stage to enable the high encryption pack to be available for the creation of the CA keys. It might be necessary to install this after the next step to ensure that any additional files that are installed are likewise updated (this will be done as a precaution).

3. Install the Enterprise CA
It is important to install the CA after the domain controller has been promoted to a domain controller, so that the option of installing it as an enterprise CA exists. It is also important to note that once this step has been completed we cannot change the domain or computer name w ithout re-installation as the CA certificate will contain hard coded information about your domain (such as the internet location of the CRL to name one). We can re-install Service Pack 2 to ensure that all the files have been updated.

4. Apply manual steps
Here we can set our CA policy appropriately with the subtraction and edition of relevant certificate templates, and attaching appropriate permissions to those templates for our account operators group. We can use secedit.exe and Fazam to monitor any chan ges to our security policy or group policy in an effort to make any manual changes automated at a later time.

5. Apply security template(s).
This is where the fun begins. We will install the template that we have chosen (though it will be heavily analyzed a nd modified before hand). We can use secedit.exe to monitor the changes to our security policy to see that the template is being installed correctly.

6. Create an account operator user
The account operators will be the only users to remain password only. Their role will be to create user accounts, issue smart cards and add machines to the domain

7. Create a new domain administrator user
The domain administrator will be created and issued with a smart card. The pre-existing administrator will have their passw ord changed and archived away in a vault.

8. Add and enroll users as necessary
This step is optional and will take place numerous times over the lifetime of the domain.

9. Add machines to domain as necessary
This step is also optional and will take place numer ous times over the lifetime of the domain.

After the security templates have been applied testing can begin and will be described later (with appropriate screen shots).

2. Analysis
Firstly lets analyze the security settings that are configured by the Hi ghly Secure Domain Controller template:

2.1 Account Policies - Password Policies
The password policy may not be as important in our domain as smart cards will predominately be used for logon, and the pass phrase policy for the card is handled by the on-card application. But as a few user accounts will still be setup to use passwords for purposes of issuing the smart cards and also for disaster recovery purposes we will quickly discuss the settings that are suggested by the template:

- Minimum password age set to 2 days and a maximum age set to 42 days
- Minimum password length set to 8 characters
- Password complexity set to enabled
- Password history size set to 24
- Require logon to change password set to disabled
- Clear text password set to disabled

The one setting that stands out here as inadequate would be password length. As very few user accounts will be using passwords, but those accounts that are will be performing some vital operations, the password length should be increased. The setting recommended by the NSA is a minimum of 12 characters, but as these passwords will not be used a lot it would be even more preferable to increase the minimum to 14 which is the highest it can be set to.

Password age and password history settings should be sufficient cons idering the accounts in question will not be used in high volumes, and thus changing the passwords about once a month should be secure enough provided the length and complexity of the passwords is high. Also the reversible encryption setting being switche d off (Clear text password setting) is also a necessity and thus should be left as is. These settings were even more stringent than those recommended by the NSA and thus there is no compelling reason to alter them.

It is interesting to note that the NSA provide an alternate password complexity filter (ENPASFLT.DLL used in place of Microsoft's PASSFILT.DLL) and the addition of this to any system may improve the overall security of your users that make use of passwords.

2.2 Account Policies – Lockout Policies

The lockout policies are more important considering these settings will effect both the smart card users and the limited number of passwords users. As the smart cards have their own lockout and unblock settings this can provide a safeguard from potential hackers trying to exploit weaknesses of your every day user account settings. Also we can afford to be more prudent considering the minority of password users there will be in the system. The settings provided by the template are:

- Bad logon attempt lockout count set to 5 times
- Reset lockout count set to 30 minutes
- Lockout duration set not set (means administrator must unlock account)

As the smart cards that are being used for this paper will become blocked after five incorrect attempts, the lockout count settings seems appropriate, however it must be noted that other cards may have different on-card settings and it may be wise to synchronize these settings so when the card needs to be unblocked the user account will need to be unlocked also to avoid confusion.

At a first look the reset lockout count might be a bit low for the environment we are dealing with, but on further inspection the NSA recommends this value to be lower than what is set by the template and thus it will remain untouched for now.

Of more concern is the lockout duration setting which would require an administrator to manually unlock a user account should it become blocked. The NSA has flagged this as a potential "denial of service attack" target and thus we will change this setting to 30 to bring it inline with our reset lockout setting.

2.3 Account Policies – Kerberos Policies

What came as a surprise was the absence of any kerberos policy settings. Given the fact that smart cards and kerberos will be utilized in unison by our domain it would be wise to delve further into what these settings default to and whether they can be improved upon.

After further investigation the default settings were uncovered:

- Enforce user logon restrictions set to enabled
- Maximum lifetime for service ticket set to 600 minutes
- Maximum lifetime for user ticket 10 hours
- Maximum lifetime for user ticket removal set to 7 days
- Maximum tolerance for computer clock synchronization set to 5 minutes

These default settings matches the settings recommended by the NSA, with the difference being they are set explicitly in the NSA template (and thus would be corrected should they have been changed by an administrator or

previously applied template). The preference would be to apply them explicitly and thus rule out the possibility that the system might be weakened if they had been changed previously.

2.4 Local Policies – Audit Policy

For this domain hard disk space (and processor and memory for that matter) is not considered to be at a premium. Taking this into consideration lets look at the settings that the template provides us with:

- Audit all account logon events
- Audit all account management
- Audit all directory service access
- Audit all logon events
- Audit all object access
- Audit all policy change
- Audit all privilege use
- Audit all system events
- Do not audit process tracking

Auditing nearly everything possible may require a lot of storage medium to be made available, and also a frequent and reliable backup system. It would also be wise for administrators of the system to track the amount of processor and disk space that is being used up so these audit settings can be catered for without a degradation of performance of your critical domain services.

Having said all this if the logs are not checked at all, either manually or using an automated script, then their value diminishes somewhat, as any errors will only be picked up on if a user or administrator physically using your domain notices them.

2.5 Local Policies – User Rights Assignment

The absence of settings under this heading was a mild concern, but having experienced the same dilemma with the Kerberos Policy it was clear that a raft of default settings were being relied upon by the template in question. To make things a bit more explicit the default settings should really be added to the template (with appropriate comments in case they needed to be removed).

There are many settings under this heading, and as there are too many to go into great detail we will only discuss the default settings that differ from what the NSA recommends (as a reference point) and any that would affect the issuance and use of smart cards within our domain. One things that was noticed when perusing the NSA's recommendation was the absence of any settings assigned to the Server Operators group, and quite a few default settings will allow the Server Operators group rights where Administrators are also granted that right. In our domain we assume that users will only be added to the Server Operators group if they are required to perform these administrative functions and the differences in these rights assignments in particular will not be discussed beyond this point.

Access this computer from the network is the first on the list and the first one that the NSA recommends a setting that differs from the default. They recommend that the Administrators and Authenticated Users groups be allowed to access this the domain controller where as it is defaulted to allow the Everyone group (among others). It would be tempting to side with ca ution on this setting and include the NSA's recommendation but obviously it would be wise to check that this does not effect functionality for the users of our domain. It is also noted that a couple of accounts potentially used by IIS are assigned this right and as IIS is only used locally for certificate services in our domain these account will be left untouched to simplify the template.

Add workstation to domain is defaulted to allow the Authenticated Users group this right, whereas the NSA recommends that they should not have this right. As Administrators and Account Operators have the inherent ability to achieve the functionality granted by this right then there is no real need for the Authenticated Users group to have this right, so they the templa te should really be changed to cater for this.

Bypass traverse checking is another setting that differs. The NSA recommends that only the Authenticated Users group be assigned this right, whereas the default is for the Everyone group to be given this rig ht. The inclination would be to go with caution and side with the NSA on this setting and change the template accordingly.

Change the system time also differs, with the NSA giving the Administrators group this right, whereas the default being the Adminis trators, Server Operators, LocalService and NetworkService groups. Being allowed to change the time could affect the logon settings, particularly the hours a users is allowed to be logged on, and possibly kerberos ticket lifetimes (though we would have to analyze the kerberos protocol to be sure on this one). On the flipside if we were to require the system clock to be synced with a hardware device or timestamp server (via a third party application) we may very well need the default rights assignment for this to be possible. Given the fact that our domain is already making use of hardware devices (i.e. smart cards) and may very well be rolling out other third party hardware modules for purposes of unblocking smart cards and cryptographic acceleration the inclination would by to leave the settings the way they are. Lets also face the fact that resetting the system time using a boot disk, or by shorting the battery on the domain controllers motherboard would not be a difficult task unless extra physical security measures were installed (which is beyond the scope of this paper but bears mentioning).

Debug Programs is assigned by default to the Administrators group, whereas the NSA recommends that either no one or possible the Developers group (if there is such a beast) by assigned this right. The NSA is partially correct on this front; Administrators are not Developers and should not be debugging sensitive services, which may contain cryptographic keys hidden within memory. In fact even Developers should no t be given this right except in their own test domain (where they will obviously be domain administrators and be able to assign it to themselves).

Log on as batch job is by default assigns the accounts IUSR_STARBUG and IWAM_STARGBUG this right, whereas th e NSA recommends this right be removed. As the IIS service on this machine will only be locally servicing the certificate server on this machine it might be wise not to make any specific changes from the default to simplify the template somewhat.

Log on locally by default allows a bunch of administrative operator groups to log onto the domain controller, whereas the NSA recommends only the Administrators group. We side with the extra granularity this provides our domains administrative users and stick wi th the default so appropriate users can be assigned different administrative duties.

Remove computer from docking station is a right given be default to administrators, whereas the NSA recommends denying this right to everyone. If we were to run this dom ain controller on a laptop (which would be highly irregular unless it was used for test or demo purposes) then the Administrators group should be given this right one would have thought and thus the default shall be left untouched.

Shut down the system , see *Log on locally* above.

There were a whole host of user rights settings where the default it virtually what the NSA recommends so overall very few real changes need to be made here (apart from making all the default settings explicit as mentioned at the start of this section). Obviously we will need to analyze any changes that were made to the default and verify that this does not pose any denial of service problems for our domain's users.

2.6 Local Policies – Security Options

There are quite a few sett ings that are set by the template and again we will only discuss relevant settings (i.e. ones which might effect smart card users or ones which differ from the settings recommended by the NSA).

Amount of idle time required before disconnecting session is set to 15 minutes by the template, but is recommended to be 30 minutes by the NSA. The only disadvantage that can be seen by having a smaller value will be the extra network traffic it takes for the client to renegotiate a session. Taking this into consideration we will stick with the smaller value, as our network will not have many machines connected to it and thus the network load should not be significant.

Audit the access of global system objects is disabled by the template, but the settings is enabl ed by NSA recommendation. To remain consistent with our statements made earlier, we are assuming we have unlimited access to audit storage media (though in reality we might have to cut back should disk space and backups become a problem) so we will side w ith NSA on this one and enable this setting. This will also apply to *Audit use of Backup and Restore privilege*.

Digitally sign client communications (always) and *Digitally sign server communications (always)* have been enabled by the template but are dis able by NSA recommendation. We will try to stick with the template on this one as our network will be running in a controlled environment and thus our SMB client and SMB server should be able to sign all SMB communications without a problem.

Disable Media Auto-play is a new setting proposed by the NSA (they recommend all drives be disabled and give the registry settings that will achieve this) and it should be implemented on our system as it makes good common sense, and thus should be added to the existin g template.

Secure Channel: Digitally encrypt or sign secure channel data (always) is enabled in the template that we are using, but the NSA recommend this be disabled so domain controllers which do not support this feature will still function. In our ne twork all domain controllers will support this feature and thus this setting should be enabled for the added security, which it provides.

Secure Channel: Require strong (Windows 2000 or later) session key is also enabled in the template but is disabled by the NSA checklist. Again as our domain controllers, now and in the future, will be installed with Service Pack 2 for Windows 2000, which should upgrade the encryption available to enable this feature, and thus it should be reasonable to enable this featu re.

Shutdown down system immediately if unable to log security audits is disabled by the template but enabled by the NSA checklist. As we have put an emphasis on logging a large amount of domain controller activity it would be wise to enable this featur e as not to compromise a potentially critical part of our system (as security audits may identify an attack on the system if analyzed correctly).

Smart card removal behavior is set to force logoff by the template but is set to lock workstation by the NSA checklist. Having worked with this setting first hand in the past it might be a bit over the top to log the administrator off the domain controller if the smart card is removed as he or she could be in the middle of some critical updates to the system (an d it might not be a good idea to chance leaving the domain controller is an unknown state). Thus we will change the template to use the lock workstation setting.

Unsigned driver installation behavior and *unsigned non-driver installation behavior* have differing settings in the template than the NSA checklist settings. The NSA recommends to warn but allow installation, which also seems like the most common sense setting given the frustrations that it can cause not being able to install unsigned drivers (ev en though they may have been thoroughly tested), and thus we will change the template to match this.

2.7 Domain Policies – Security Options

The NSA checklist sets three settings in this section. The most important of these is *Automatically log off users when logon time expires*, which is enabled. This should be added to our template. Also it would be nice if we

could add smart card removal behavior in this section. We may need to make this change manually and analyze the change to the system using seced it.exe and hopefully be able to add this setting to the template.

2.8 Event Log Settings

The settings for the template in question vary greatly from those recommended by the NSA, with the NSA setting the maximum log sizes to full, which seems to be the best option for maximum security. The NSA also recommends manual retention of all event logs and enables shutting down of the computer when the security audit log is full. All of these recommendations seem more secure than those set in the template and thus they will all be changed to match.

2.9 Restricted Groups

The NSA recommends that the Power Users be added to the restricted group and that group should have no members. This seems feasible, as it was not envisaged that any user will be a member of the power users group, so adding this to the template should not pose any problems.

Given that this is the case we do not have to be as stringent about giving permissions to the power users group for files and registry keys. This will be discussed briefly in the next few of sections.

2.10 System Services

Neither the template nor the NSA explicitly recommends setting permissions for a particular service. This area would need to be reviewed if new services were installed but as we are dealing with a relatively clean system (apart from the third party smart card software) from a service point of view we can reasonably safely leave these setting empty.

2.11 Registry Permissions

There are a whole host of registry permissions that could be discussed (probably enough for a whole paper to be written on them) but we will take some major examples and discuss those.

Given the fact the power users group has been added to the restricted groups the differences between the NSA settings and those that come default on the operating system are fairly minimal.

The biggest difference noted so far is the setting of inheritable permissions. For instance the \MACHINES\SOFTWARE key in the registry is set by the NSA to replace the current inheritance (or lack thereof) of all sub-keys to inherit from this keys permissions. This is not the case by default but does make some sense to make use of. Based on this and the fact that the actual permissions as a whole are not changed significantly it has been decided that we will add the registry permissions portion of the NSA template to our template, but we will have to keep an eye on various bits of functionality to see if they are affected by this decision.

2.12 File Permissions
There are quite a lot of permissions that could be discu ssed here but we only have the space to discuss them briefly.

This section partially mirrors the previous session. The NSA make a number of recommendation which do not vary much from the original setting part from the inheritance settings which they set.

For our template we will try to use the NSA's recommendations, purely for the reason that some of the file permission inheritance settings seem to make some common sense. You also get the feeling that the Microsoft default, while being good if your syst em was not changed considerably, may fall over in the future (or require a large amount of work to rectify) if permission were required to be added in the future (like if another security group was added that needed access to particular files or registry s ettings).

2.13 Extra Settings, Permissions and Manual Operations
Some extra permission and settings were needed to round out the security template. These include some to secure IIS so that it can only be used on the domain controller and not across the n etwork to prevent denial of service attacks. Also required were some settings to restrict the use of certificate templates so that certificates cannot be issued for purposes other than those prescribed (i.e. smart card logon certificates and enrollment ag ent certificates).

The certificate template policies can be set manually under the public key policies section on our certificate authority. We need to determine the changes to the system when we add new certificate templates (and delete some default ones) and add permissions to the required certificate templates.

For these templates we need to make sure that the accounts administrator group has appropriate permission to make use of these templates so that they can enroll for an enrollment agent certific ate and the issue users smart card logon certificates. These settings may be able to by automated (especially if the settings are included in active directory or the registry) but for the moment we will have to apply them manually.

To add permissions to existing templates we need to access the Active Directory Site and Services administrative snap -in. Here we need to assign the permissions on the Enrollment Agent and Smart Card Logon certificate templates to include the enrollment permission for account operators.

Overall the certificate templates settings are perhaps the easiest settings to get wrong because they exist in quite a few different areas in the administration of our domain controller. When in doubt view the MMC help files that come by defau lt with the Windows 2000 Advanced Server operating system, which give detailed instructions on how to access all the settings that you should require.

3. Apply and Test

The application and testing of the template is where we hope that all our hard work will bear some fruit. Obviously in the development we have made a fair amount of assumptions and possibly even taken a few settings on plain blind faith (either in Microsoft or the NSA) and now this will be tested out reasonably thoroughly (particularly fro m the security perspective).

3.1 Applying the template

The template can be applied easily using secedit.exe or the Security Configuration and Analysis snap -in on the local machine. The biggest benefit from using a command line executable to install the t emplate is that it makes it easy to roll out to any number of domain controllers on your system either now or in the future when they come online (though with the manual steps that are involved with installing the CA this may not be necessary or feasible). The command line can be rolled out via group policy and the ability it has to run scripts on machines at scheduled intervals. In this case the Security Configuration and Analysis snap -in was used.

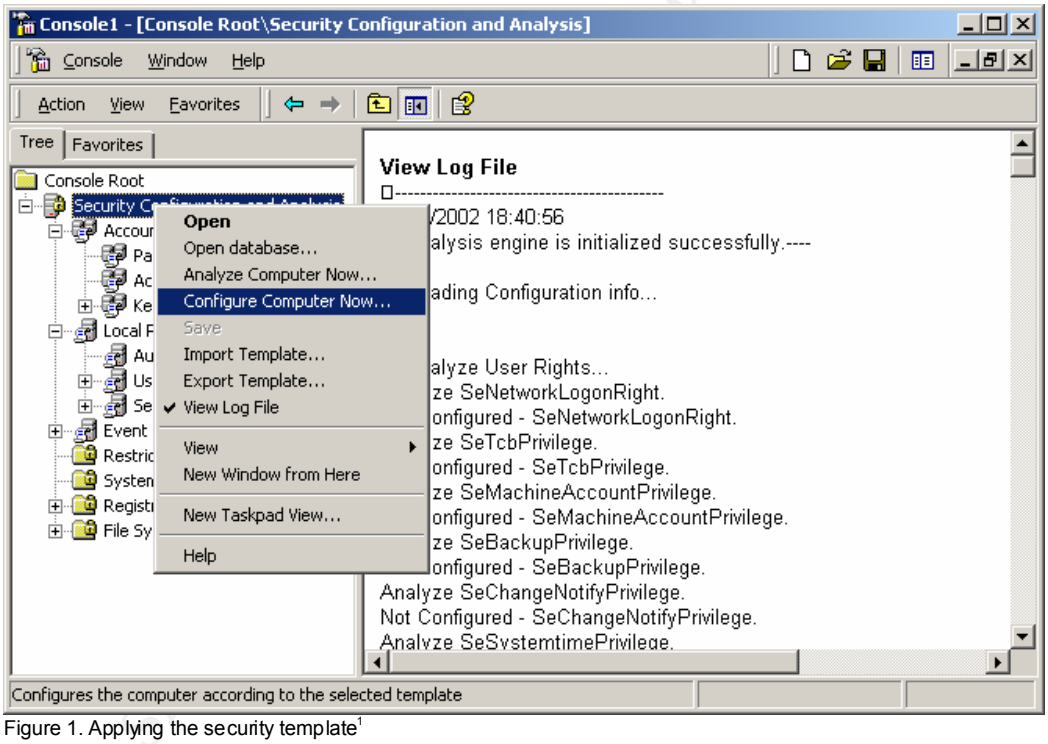

Figure 1. Applying the security template[1]

For administrators unfamiliar with security templates it is best advised to use the Security Configuration and Analysis snap -in (at least once) as it can provide you with some easily traversable analysis.

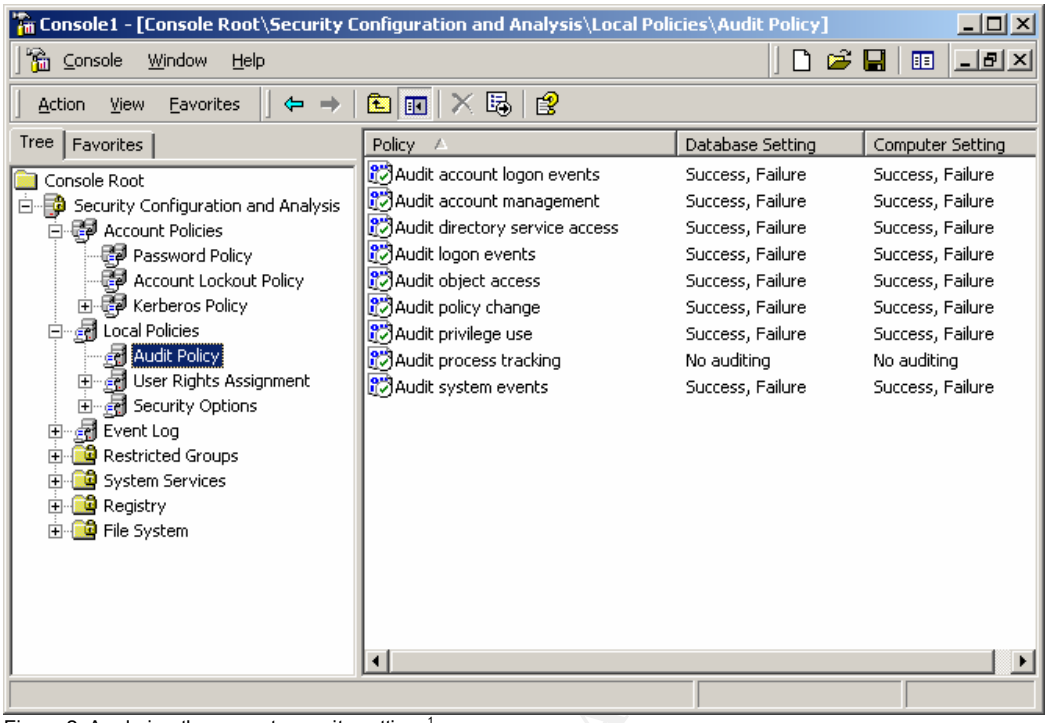

Figure 2. Analyzing the current security settings[1]

There is a fairly large manual process for getting each CA up and running (after which the template can be applied), and this is unavoidable as the details and security aspects of any CA require a lot of human interaction (especially when keys and certificates a re being generated). The template helps secure the usage of the CA by protecting some of the resources that interact with the CA's private key functions, such as the certificate services web pages hosted by IIS. The template helps restrict access to thes e web pages, and some manual steps restrict the use of certificate templates to a minimum (and thus not over exposing the private keys of the CA in the process).

Below we can see some of the resultant security policy settings by applying the template, which we just developed.

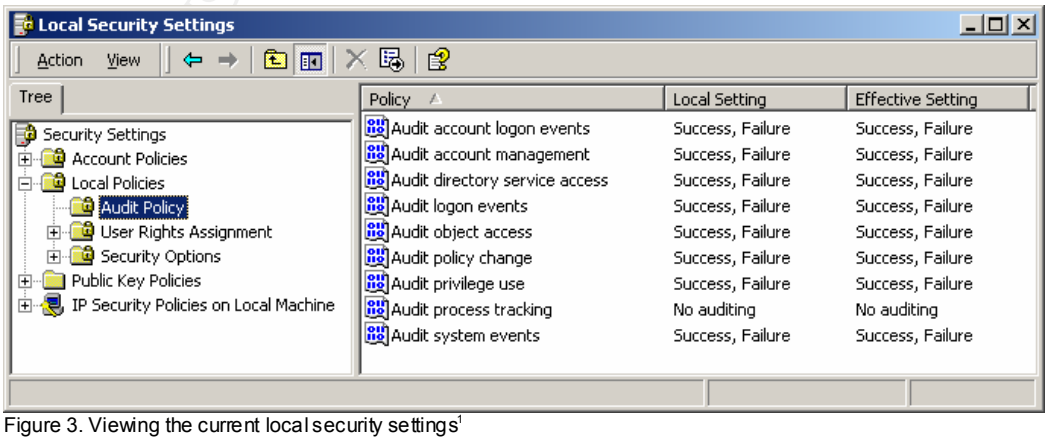

Figure 3. Viewing the current local security settings[1]

3.2 Testing the security

You will notice that the account operator will perform a lot of the proceeding security tests. This illustrates how important the password policy is to the security of our domain, as while the account operator's tasks might not be performed as frequently as smart card logon, the tasks are integral to the security of the system.

An approach that was taken to testing was making use of a few of the hidd en security features within the operating system.

3.2.1 Enrollment Agent Enrollment

We begin this test with the account agent logging in to the domain controller. The account operator user has been given the privilege to request an Enrollment Agent certi ficate using the Enrollment Agent certificate template. Once we are logged in we start Internet Explorer and access the Certificate Services web pages on the local machine (this could be delegated to a remote machine if configured to do so).

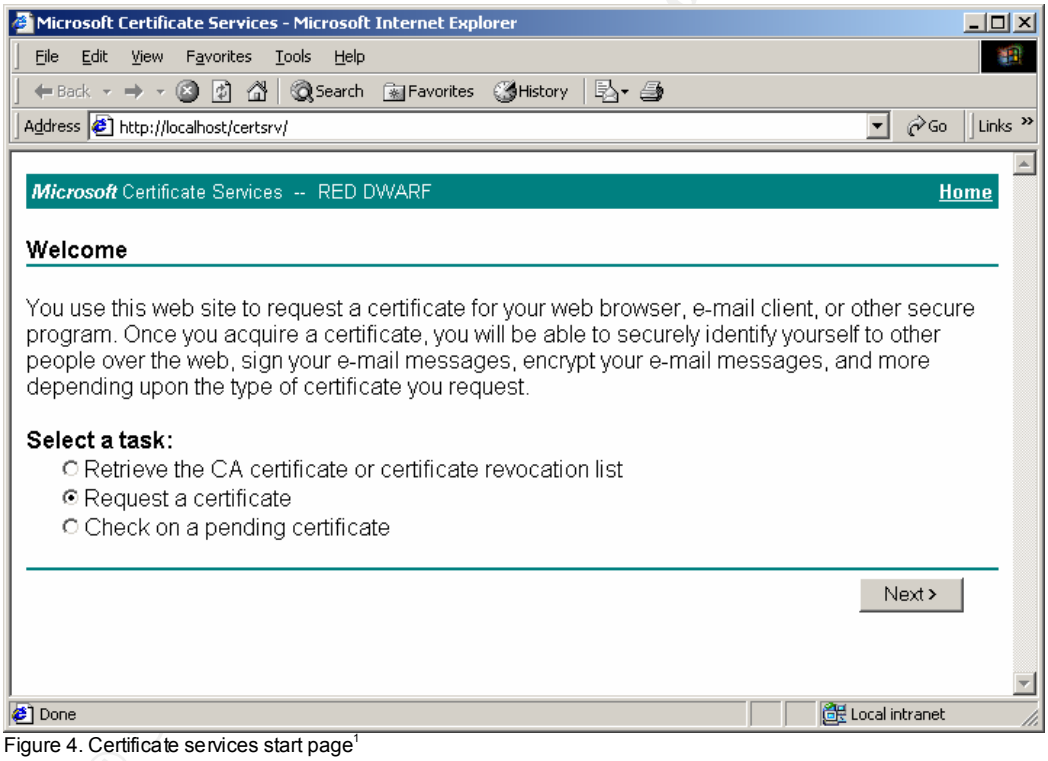

Figure 4. Certificate services start page[1]

We then select the advanced enrollment option.

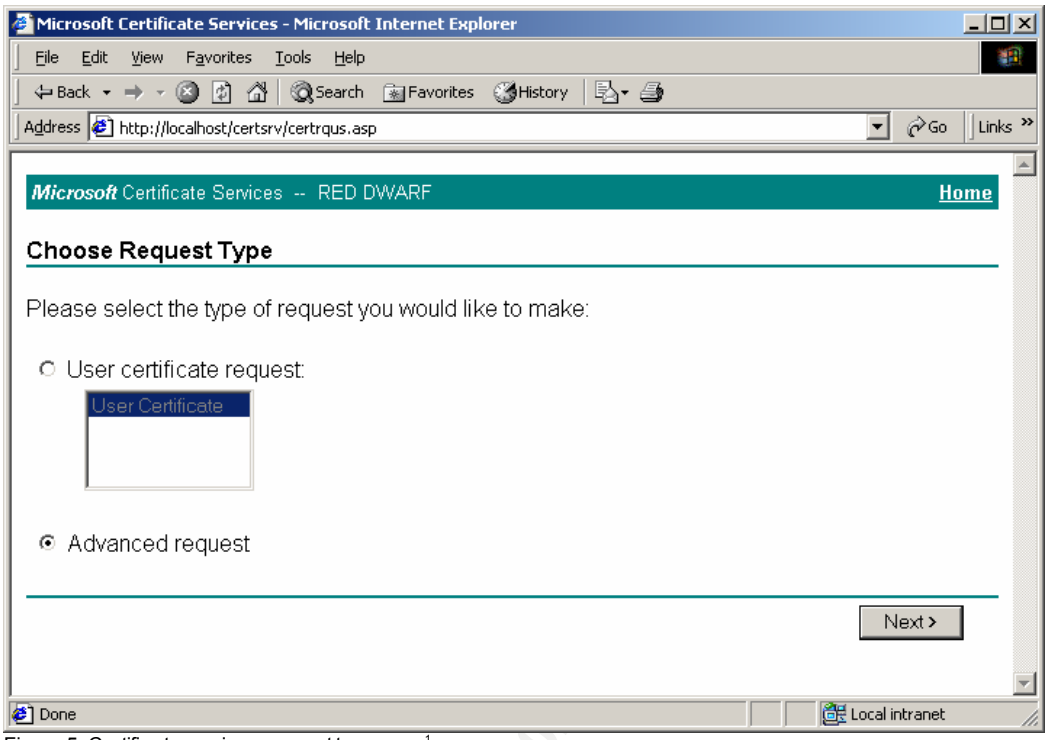

Figure 5. Certificate services request type page[1]

From there we select the certificate request option.

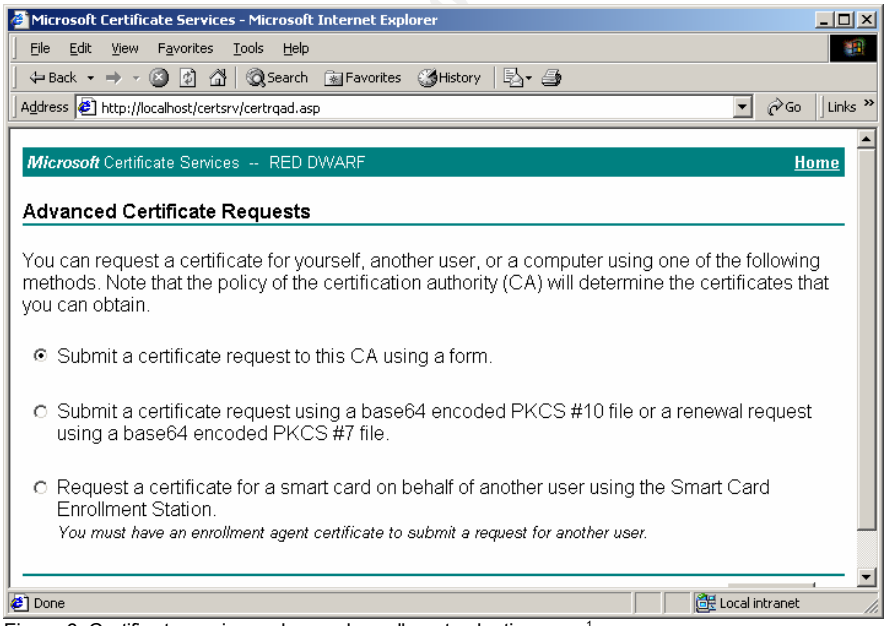

Figure 6. Certificate services advanced enrollment selection page[1]

Now we select the appropriate CSP (in this case the Microsoft Enhanced CSP), enrollment agent template, and strong private key protection and click the request button.

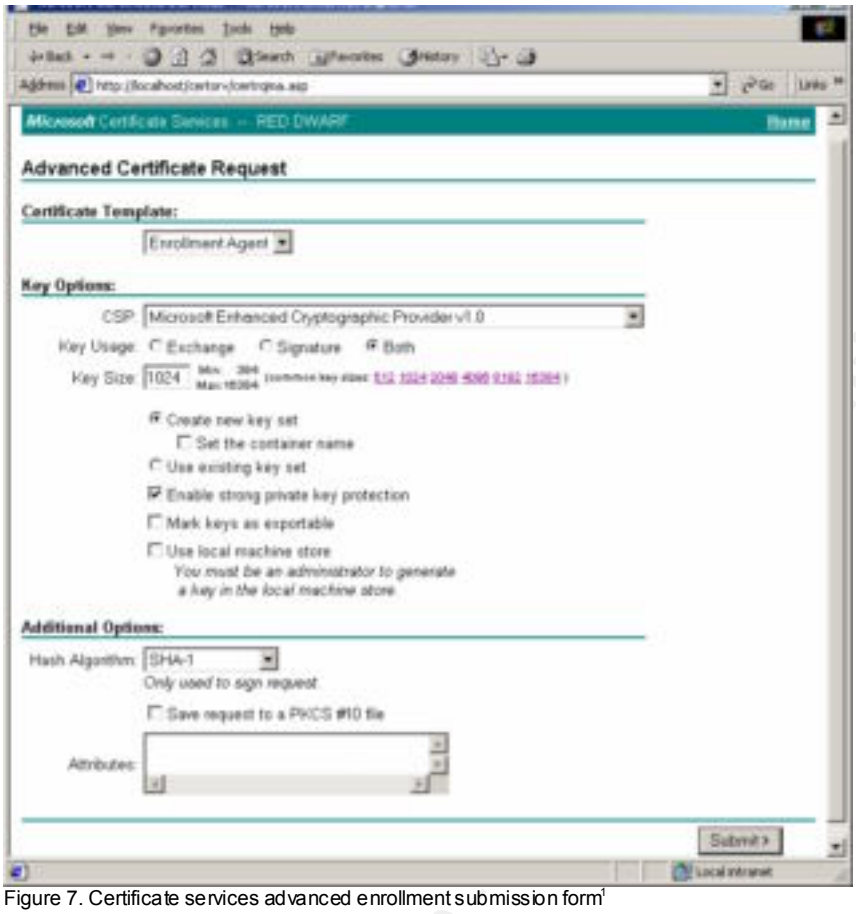

Figure 7. Certificate services advanced enrollment submission form[1]

Appropriate details (including the user account user name) will be extracted from the account operator's settings in active directory for insertion into the certificate; a new key pair is generated (in software) and an appropriate level of security can be attached to this as can been seen in the following screen captures.

Figure 8. Software based key generation[1]

Figure 9. Software based key generation security level[1]

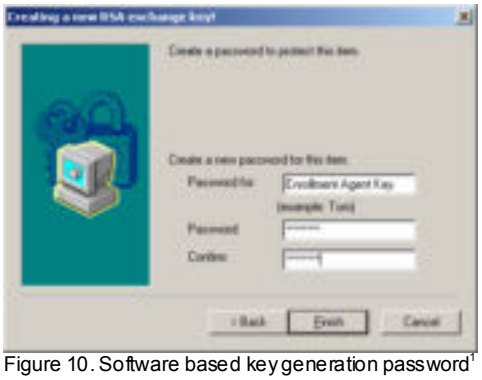

Figure 10. Software based key generation password[1]

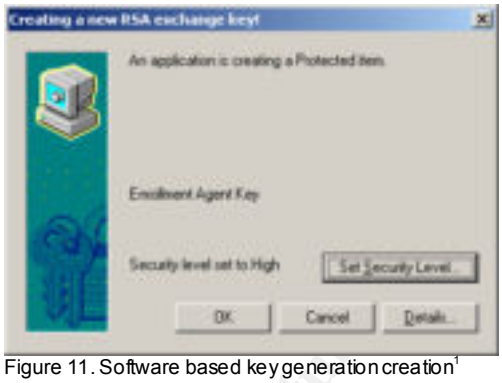

Figure 11. Software based key generation creation[1]

The CA key pair on the domain controller signs the certificate and the certificate will be loaded into the browser (actually the Microsoft certificate store). The important details in the certificate are the certificate template type (in this case Enrollment Agent), the issuer (which establishes trust to our CA, and the subject which indicates that this certificate can be used by the current user.

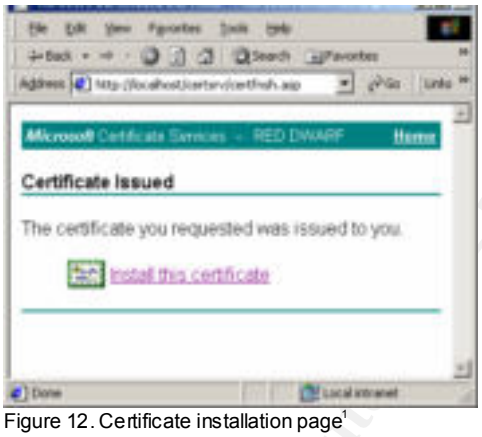

Figure 12. Certificate installation page[1]

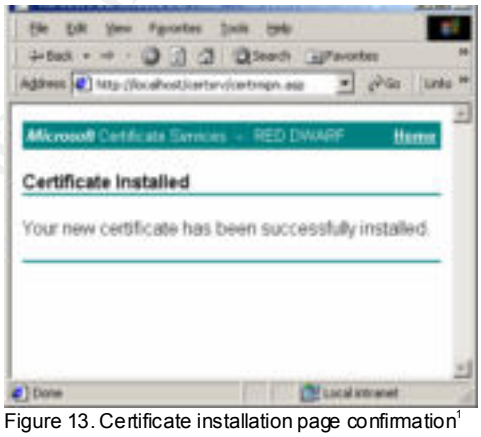

Figure 13. Certificate installation page confirmation[1]

The test was completed successfully when the enrollment agent certificate was issued to the account operator and was visible in the browsers personal certificate list.

Figure 14. Certificate details[1]

3.2.2 Add a new user to the domain

This is also the responsibility of the account operator so we logon on to the domain controller and start up active directory users and computers.

Under the user section we select the "New User…" dialog and enter the appropriate details. While a password will also need to be entered at this time, the next step will effectively rule out the need to know what it is to practically any password that meets our security settings can be entered (i.e. a complex 14 character password). We could have written a scr ipt at this point to generate some random passwords that could have been pasted into the password entry text boxes but it was felt this was unnecessary.

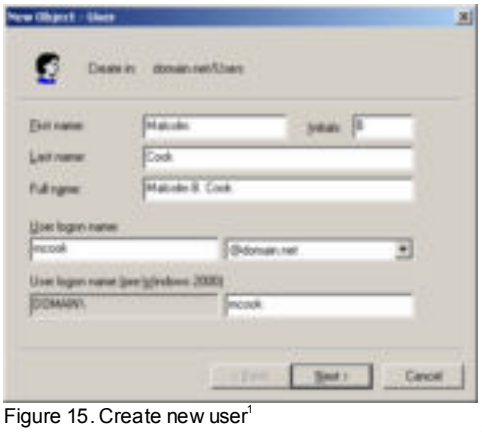

Figure 15. Create new user[1]

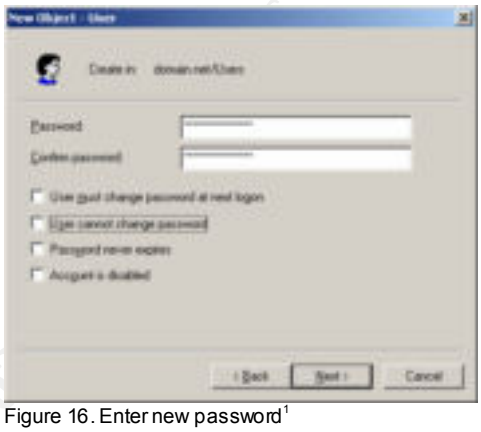

Figure 16. Enter new password[1]

An important follow step is to requ ire that the user must logon with a smart card. Modifying the user account and ticking off the appropriate tick box sets this setting.

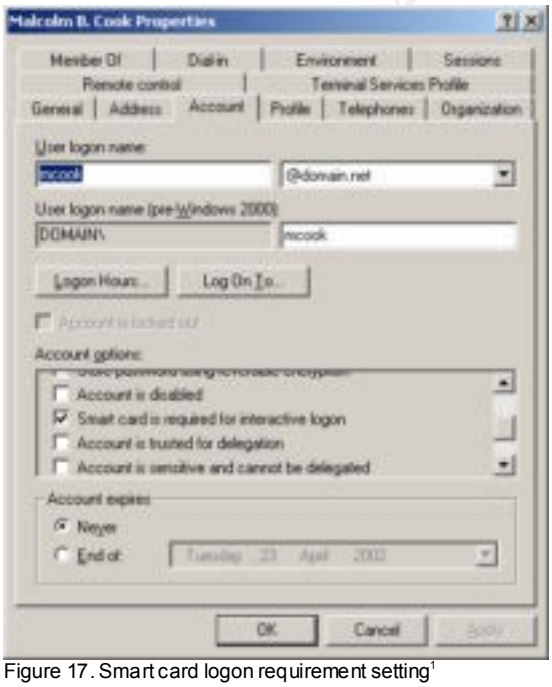

Figure 17. Smart card logon requirement setting[1]

Now with smart cards in the mix, user enrollment is effectively a tw o-stage process with the user being created (which was just completed successfully) and then the smart being created on behalf of the user by the enrollment agent (in our case the account operator), which is covered under the next heading.

3.2.3 Smart Card Enrollment

We begin this test by logging in as a user from the account operators group (these users are the only active users that will use passwords) who already has already enrolled for an enrollment agent certificate. Once we are logged in we start Internet Explorer and access the Certificate Services web pages on the local machine (this could be delegated to a remote machine if configured to do so).

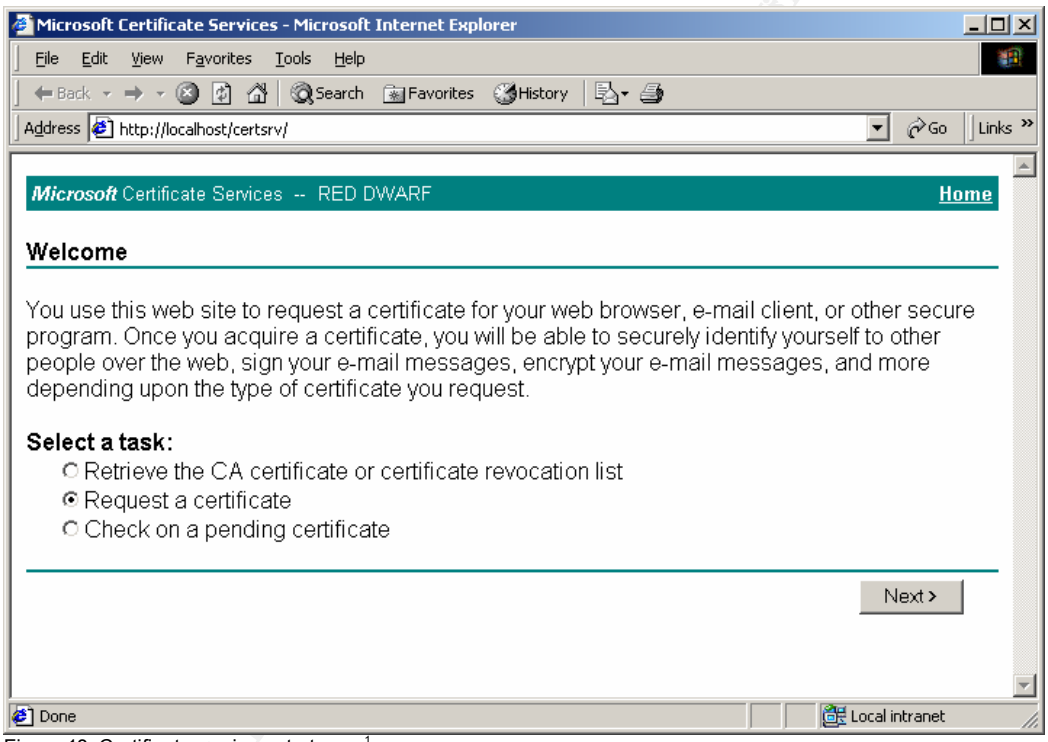

Figure 18. Certificate services start page[1]

We then select the advanced enrollment option.

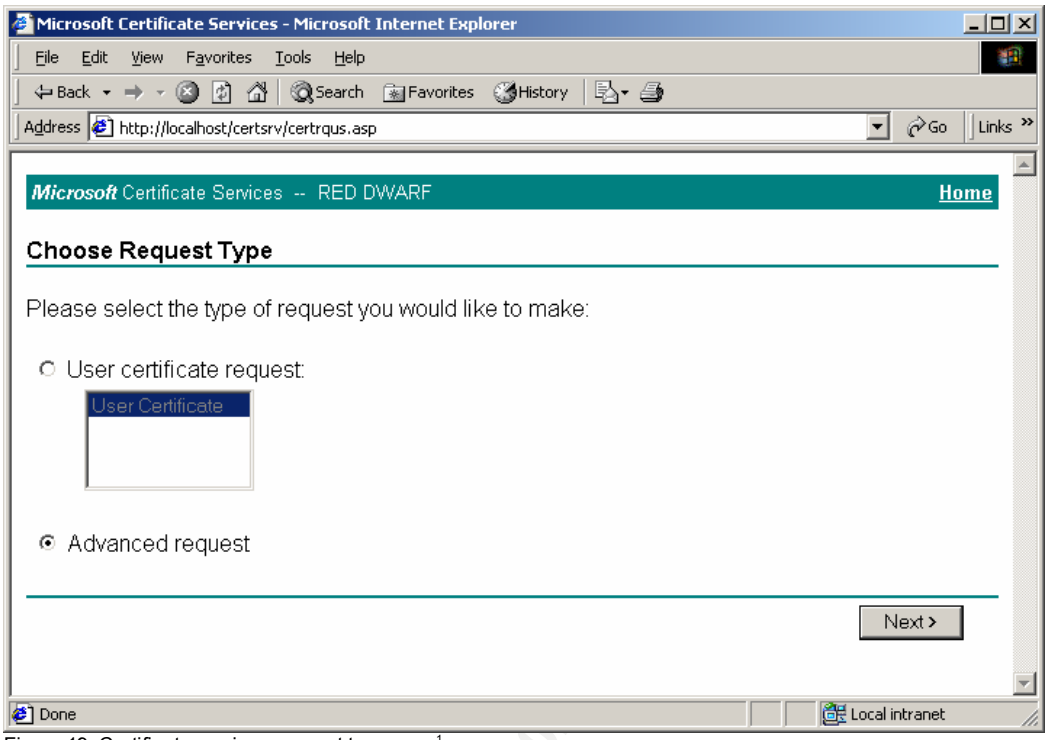

Figure 19. Certificate services request type page[1]

From there we select the smart card enrollment option.

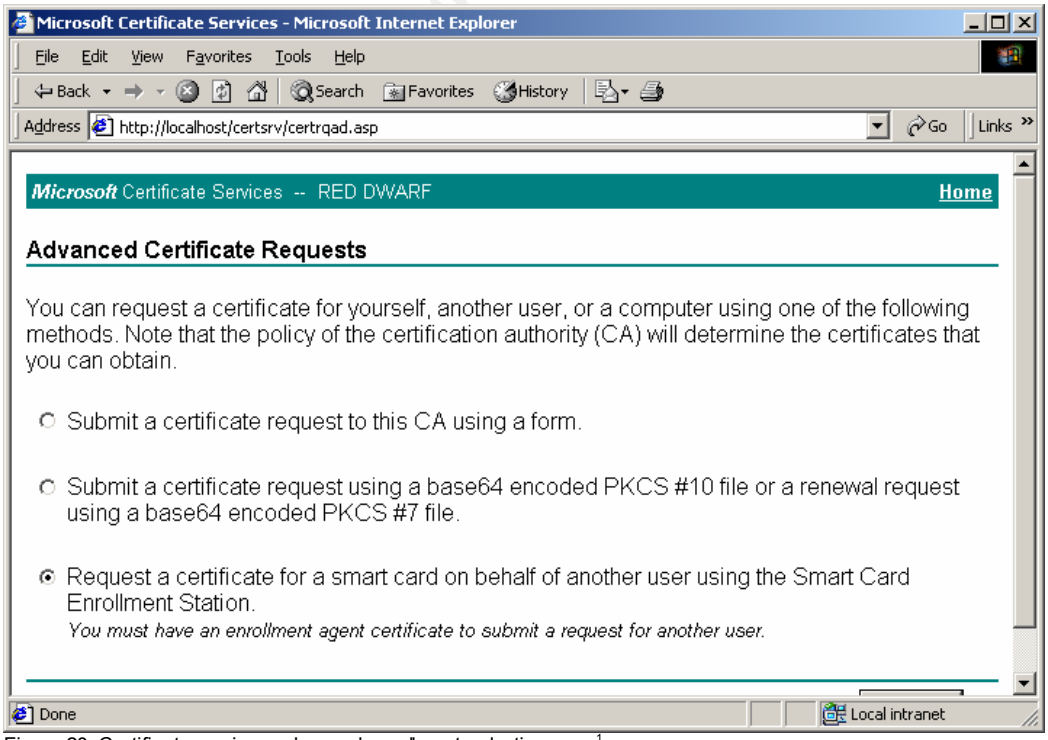

Figure 20. Certificate services advanced enrollment selection page[1]

Now we select the appropriate CSP, enrollment agent, certificate template (in this case smart card logon) and user and then click the enroll button.

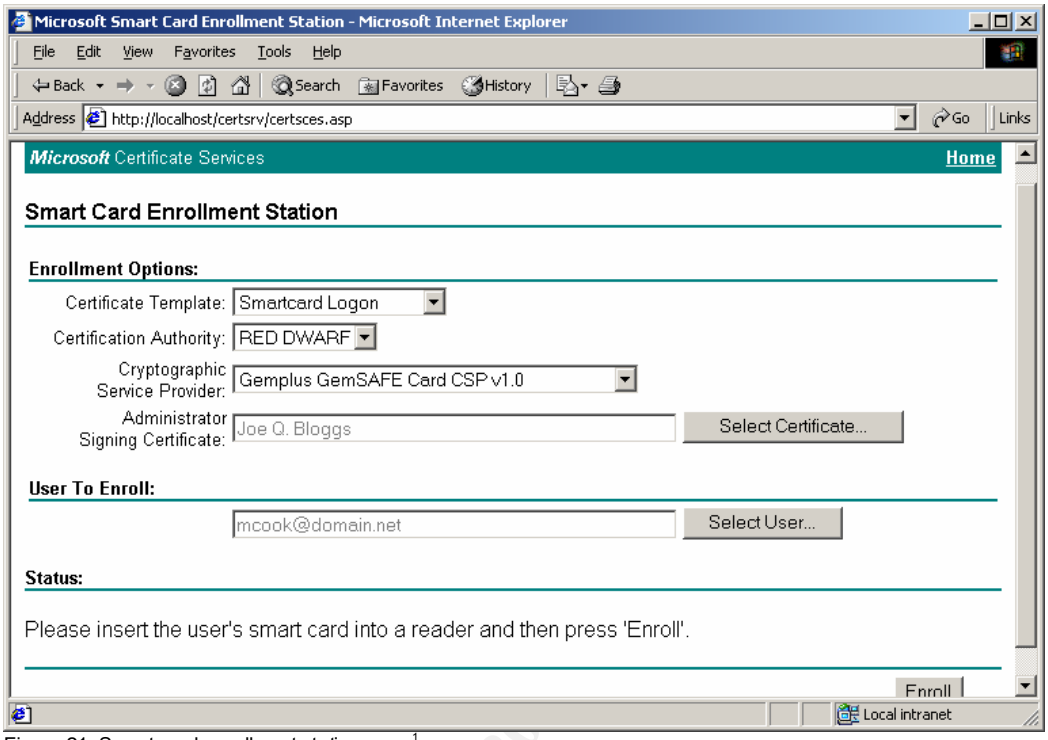

Figure 21. Smart card enrollment station page[1]

Appropriate details (including the user account user name) will be extracted from the selected users settings in active directory for in sertion into the certificate, a new key pair will be generated (on the smart card), the certificate will be signed by the CA key pair on the domain controller and the certificate will be loaded on the smart card. The enrollment agent (or user if he or she is present) will be asked for a pass phrase along the way and this along with the smart card will allow the recipient of the smart card to logon and access domain resources. The next few screen shots show the third party smart card software aiding the key generation process, and while a lot of it will be unfamiliar to you, it illustrates the potential details that can be involved in any particular key generation.


Figure 22. Smart card selection[2]


Figure 23. Smart card key name creation[2]

Figure 24. Smart card key usage selection[2]

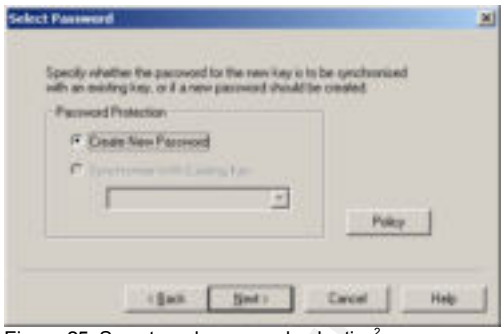

Figure 25. Smart card password selection[2]

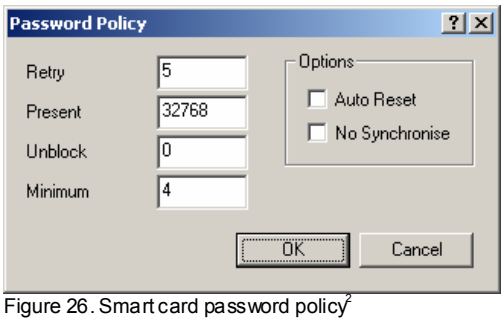

Figure 26. Smart card password policy[2]

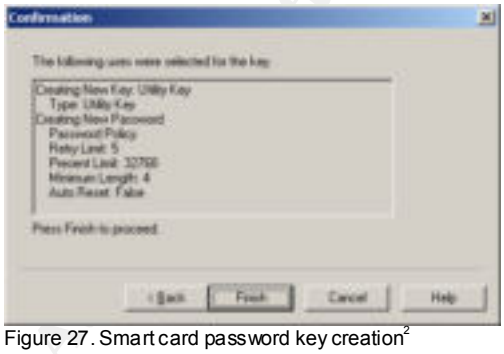

Figure 27. Smart card password key creation[2]

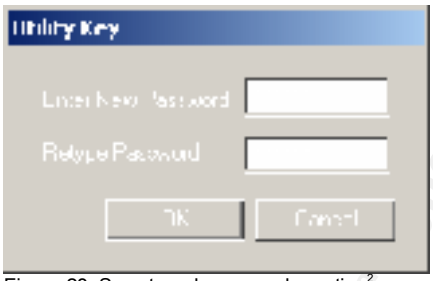

Figure 28. Smart card password creation[2]

Figure 29. Smart card unlock for request signing[2]

The test was completed successfully and a smart card was produced and a pass phrase remembered. A smart card logon certificate has been loaded onto the smart card with the appropriate details and permissions.

Figure 30. Smart card logon certificate information[1]

3.2.4 Smart Card Logon

While we can describe the details of this test, most of the actual screen shots are unavailable for viewing as they happen in the winlogon desktop. Of course we can show the audit logs surrounding the smart card logon tests, and show the settings that the user account possessed. If we had a program like VMWare we would have been able to capture all the screens shots (as that program runs the operating system entirely within a single window) but unfortunately this was not available at the time of testing (nor was there time to install a test Windows 2000 operating system using VMWare).

This test begins with a machine that has been added to the domain (and allowed enough time for group policy to pro pagate to the computer for the purposes of trusting the CA), has a PC/SC compliant smart card reader attached (in this case a GemPC 410) and the appropriate third party software installed. The user is prompted to either logon using a password (CTRL + ALT + DEL) or to insert a smart card. We now insert the smart card we obtained from the previous test.

Provided the smart card has a recognizable reset string (meaning there is an appropriate smart card CSP installed on the system) the user will be prompted for a PIN (in our case it will be alphanumeric). We enter the pass phrase that was chosen from the last test and the logon process takes place.

Provided the keys on the card match the certificate and the certificate was a smart card logon certificate iss ued from the correct CA the logon should smoothly. In this case it does and the user can access the domain resources (and local resources) just as if they had logged on using a password. Effectively the user has been granted a kerberos ticket as can be s een in the following screen shot.

We can also see the certificate that was used to successfully log on and the user account settings which forces the user to use a smart card to logon (without this last setting the smart card could still have been used bu t so to could have the password which could undermine the security of our system). We can see some of the successful audit logs below (keep in mind that smart card logon utilizes standard Windows 2000 kerberos ticket based authentication)

Figure 31. Smart card logon account logon audit log #1[1]

Figure 32. Smart card logon account logon audit log #2[1]

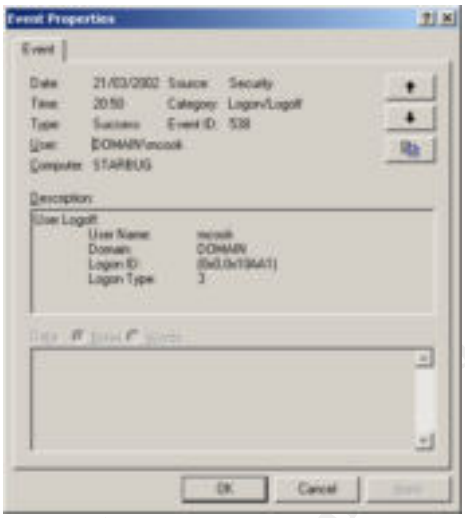

Figure 33. Smart card logon account logon audit log #3[1]

3.2.5 Smart Card Removal Behavior

Again this test is hard to illustrate using screen shots as the entire user interface occurs in the winlogon desktop. This test begins with the user logged on using their smart card. The template has set that on smart card removal the workstation will lock and from their can either be logged out be an administrator or unlocked by the same user.

The user removes the card and workstation is locked.

The user reinserts the card, enters the pass phrase, and the smart card re - authenticates to the domain controller and the workstation is subsequently unlocked.

The test is completed successfully as the user can once more access the domains resources (and local resources) and continue on where they left off.

3.2.6 Password length, password repetition and password complexity

Again, another test that occurs in the winlog on desktop. This test occurred when the account operator was about to change their password (the same would also apply if they were forced to change there password also).

The account operator types in their old password and then selects a new password.

A password of 13 characters is typed in and the password is rejected as was expected.

A password that matches a recently used password was typed in and this was also rejected.

A new password of 14 characters was typed in but containing only numbers and this was also rejected.

The test is completed successfully when finally a new password of 14 characters containing a mix of upper case, lower case, punctuation and numerical values was type in and this was accepted.

3.2.7 Revoking Certificates

This security test is important to show that we can control the effectiveness of the certificates we issue from the domain controller. We start this test logged in as the account operator. We start the CA snap -in and display the list of issued certificates.

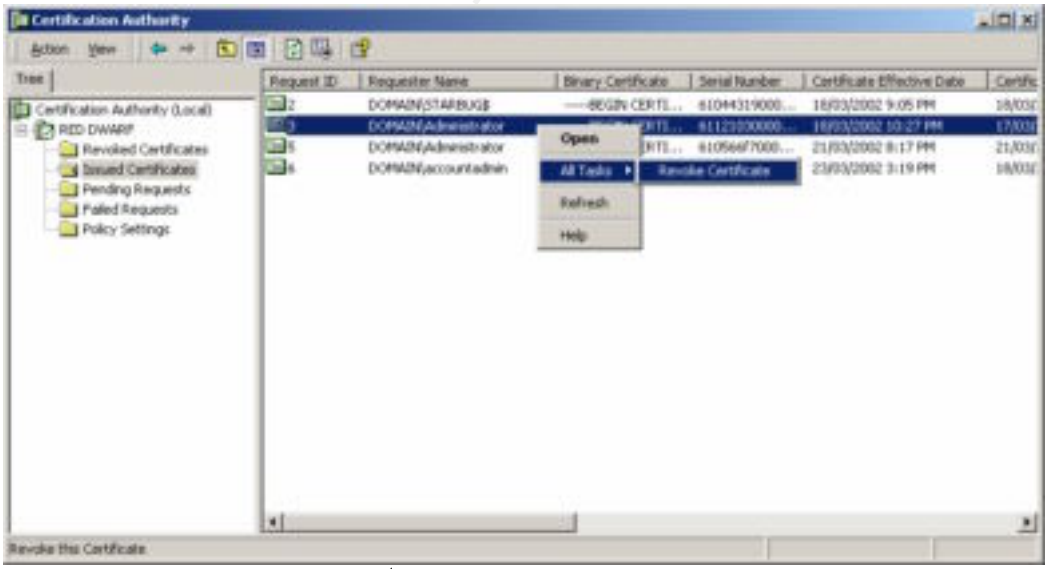

Figure 34. Smart card certificate revocation[1]

Then we select to revoke the certificate with appropriate reason.

Figure 35. Smart card certificate revocation reason[1]

The certificate ends up under the revoked folder.

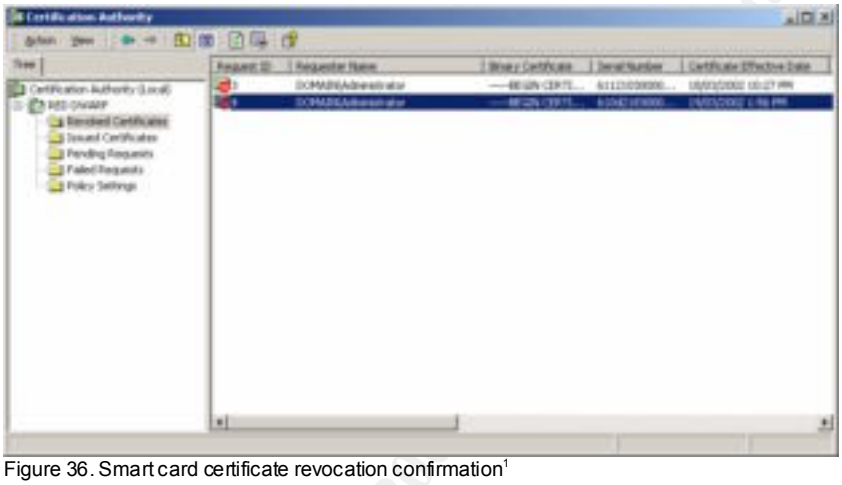
Figure 36. Smart card certificate revocation confirmation[1]

It is important to publish the certificate revocation list (CRL) immediately, otherwise you any certificates you revoke will still be operation within your domain until the next scheduled CRL update.

Figure 37. Revocation list forced publish[1]

To complete the test we attempt to logon using the revoked certificate and fail. We can see the failed audit log for the logon attempt below (the descriptive is a little vague, but that's Windows 2000 for you).

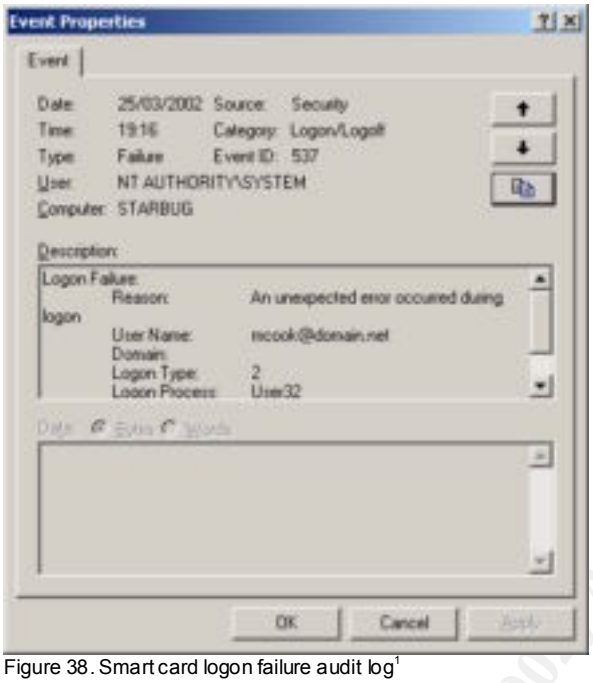

Figure 38. Smart card logon failure audit log[1]

This was a simple but important test as we have verified one of the important control elements that we have access to in the administration of our CA. This security feature could be used when we issue certificates by mistake, or an employee no longer has the right to logon to your domain, or even when a smart card may have been stolen, lost or compromised in some way.

3.3 Testing the functionality

To be honest this was perhaps the hardest area to cover, as the author does not strictly speaking come from a systems administrator background (and thus does not have the awareness of all the operations expected of a domain controller). Thus we have chosen some rather simple (but vital) tasks that the domain controller would expect to b e able to perform.

3.3.1 Accessing networked resources (drives and printers)

One of the most vital aspects of any network (and a feature that users take for granted) is the access users have to networked resources such as printers and application (e.g. internet, email, and more specialist applications like source safe to name but a few).

Here we will test out a user attempting to access source safe across our domain's network.

Unfortunately with the use of smart cards we need to enter our source safe password each the first time we start source safe. Previously, provided the source safe password matched your domain password, you could log on

automatically, but now this is not the case. Apart from this however source safe could be accessed across the ne twork and this test was successful.

3.3.2 Install new hardware
To test out this procedure we will attempt to add a different smart card reader onto our domain controller. We will do this logged in as the account operator as it could be possible that the existing smart card reader could be broken and a new one has to be added (and as the administrator uses a smart card to logon he or she can't add it, unless we retrieved our disaster recovery administrator account from a vault, which we would prefer not to have to do for such a minor problem).

We start by plugging a new smart card reader into the machine and log on as an account operator. This prompts a new hardware installation dialog where we select the appropriate drivers (in this case they are signed) .

The new hardware wizard finishes and we log off our account operator and test out the installation by logging on using our administrator smart card. While this isn't a definitive test as various readers may have greater installation requirements than t he one that we tested with, at least it tests out the feasibility of recovering from a smart card reader malfunction (where updated drivers may be the only thing that is needed).

3.3.3 Add new computer to the domain
This is the responsibility of the accou nt operator and we need a newly created Windows 2000 operating system that needs to be added to the domain. The test begins with the local user logging on as the local administrator.

We select the "Add computer…" option from the Active Directory User and Computers snap-in and enter the name of the computer.

The computer is successfully added to the domain. To test this fully we would need to wait for group policy to propagate to the newly added machine and the logon using a user smart card. The reason we must wait for group policy to take affect is that the CA certificate must propagate to the machine (and then be trusted) before smart card logon will be successful.

4. Evaluation
Now that we have applied and tested the template we can do some further analysis based on what we have seen. On the surface we have achieved what set out to do. This is not to say there were not any hiccups along the way, though most of these were to do with non -security related items like installing Windows 2000 and promotin g it to a domain controller (which took a fair time for reasons that won't be entered into here). In fact the most trouble was had getting the smart card reader to work as the default drivers would not talk to the device (though once the latest drivers we re downloaded it worked like a charm). It is also interesting to note that Windows XP decided to ever so nicely disable the installation of Windows 2000 (because it detected that your were trying to install a previous version of the operating system and i t didn't want you to do this).

Once a proper procedure is followed, creation of user accounts and the issuing of smart cards is an easy and fairly timely task and really will not add as much overhead as might have been thought. In fact when you look at i t closely smart cards in small to medium sized companies would not be to taxing on resources, however larger organization will be another story altogether.

Large organizations would raise a number of complexities, particularly when users started to block their smart cards (which will happen frequently) and effectively go off line. This is where smart card unblocking would have to be looked at and while it is okay for smart cards to be issued from a central location, unblocking would have to be more widesp read so your users would not be twiddling their thumbs for too long. This would also raise issues whether having a fast and effective smart card unblocking system would weaken the overall security.

4.1 Too strong, too weak and potential changes

Probably the settings for the audit log for the template that was used will be hard to maintain for quite a few systems (especially when budgetary constraints are taken into consideration). To make the template more general so it could be applied to more systems i t would be a good thing to analyze what is actually required from a security perspective, and find out what setting would actually be useful in analyzing attacks on the system and which ones merely add overhead to the processor, memory, disk space and back up requirements.

4.2 Affected Functionality

As noted in one of our tests previously the functionality of source safe was affected by the introduction of smart card logon into our system. This could affect any number of third party applications that tied (either tightly or loosely) their usernames and passwords to the domain user accounts.

When you think about it carefully there are quite a few things that you would be unable to do now that users can only use smart cards to logon, like accessing network resources from non-domain computers (we used to be able to enter the username and password in a popup box but now we do not have that option).

This is not say that the introduction of smart cards is a bad idea, but it illustrates how it can affect things that we have previously taken for granted.

Although it was not noticeable while completing the testing, having such stringent auditing requirements may affect the performance of the system, which may impact on the functionality of time sensitive programs . This would need to be closely monitored to see if this was the case under load conditions and if so either better hardware would be required or the audit settings would need to be scaled back.

4.3 Further Research

There are many areas where research co uld branch out. One area in particular that could be looked at would be trying to totally eliminate passwords from every account (apart from one domain administrator account whose password would be locked in a bank vault). To achieve this we would need to determine the capabilities of the smart card enrollment station when two smart card readers are installed (one for the logged on smart card issuer and one for the smart cards that are being enrolled).

The automation of the certificate template settings and permissions would be an area where some research could also be performed. The current way that they need to be configured is mildly complex and extremely prone to error as any little error along the way can make your system non -operational or leave your system with some potential unnecessary security holes.

It would also be nice to be able to create users with their smart card logon requirement automatically enabled, rather than having to manually edit the users properties each time a user is created . This would further harden the system by taking out the chance for human error to leave user accounts open for logging in via a password. Also it is important to note that the omission of this setting will not prevent your users logging in with their sm art cards so you may not even be aware that this security hole may exist for any particular user. Also be aware that the audit log does not explicitly log that a user has logged on using a smart card, it merely provides kerberos log information. In fact this area of the log seemed a little lacking, as it would be nice to be able to log whether a user was using a smart card or a password (hopefully something was missed and this is not the case, but it on the surface it there appeared to be no smart card lo gon event logs available).

Another potential research area would be looking at how to roll out smart cards with certificates for other purposes such as secure email (maybe with separate signing and encryption keys), client authenticated SSL, code signing and user authenticated VPN access among others. If we were to do this we would most likely require an intermediate CA issued from a well -trusted third party (like Verisign for instance) so that our certificates would be trusted outside our organization, w hich really is a necessity when we are considering secure email (S/MIME).

Smart card use over terminal services session could be an interesting area of research. The third party smart card software that was used for this report worked successfully over C itrix Metaframe, and thus that area could be researched to se what benefit this could provide an appropriate organization.

The encrypted file system and smart cards has thus far been an intrigue (especially as the two do not interoperate). There is a fee ling that they could be massaged to work together given a bit of creative CSP development (like wrapping the base or enhanced provider and palming of the calls that would use the EFS private key to the smart card instead of the relatively insecure software based keys).

The templates themselves could be improved considerably by getting them out in the field on live sites in real life situation where feedback can be accumulated. Analysis could be done on the performance of the template when applied to systems running on different hardware (with different memory and processor speeds) with different sized hard disks. You could even develop a wizard or utility that could customize the template based on the hardware requirements and backup capabilities of the system.

As you can see by the length of this section that there are many areas of research that could be done, and any one of them could be the topic of a paper similar to this. Computer security is a growing and evolving area and until now it was always expensive to roll out system incorporating such things as PKI and smart cards, but now with Windows 2000 (and Window XP, Windows .NET and beyond) a lot of this infrastructure is available for a pittance (compared with how much custom systems used to cost). Security templates provides only a small piece of the puzzle, and if used correctly (as has been illustrated) it may be one of the last puzzle pieces that is required to make your systems secure.

5. References

Haney, Julie M. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Toolset. Ft. Meade: National Security Agency, 2001

Christman, Sheila. Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services. Ft Meade: National Security Agency, 2001

Microsoft. How It Works.
URL: http://www.microsoft.com/windows2000/techinfo/howitworks/ (10 March, 2002)

Microsoft. Windows XP: Help and Support Centre. Redmond: Microsoft, 2001, Assorted Help Files

1. Microsoft. Windows 2000 Advanced Server. Redmond: Microsoft, 2000, Assorted Screen Shots

2. SecureNet. TrustedNet Connect. Melbourne: SecureNet, 2002, Assorted Screen Shots

Last Updated: May 23rd, 2017

Upcoming Training

SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 06, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**