



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 permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at <http://www.giac.org/registration/gcwn>

Sans Windows 2000 Security GCNT Practical Exercise:

**Microsoft Windows 2000 Security:
Windows 2000 Stand-alone Offline Root Certificate Authority Protection Guide**

© SANS Institute 2000 - 2005 Author retains full rights.

William S. Pachucki

March 2000

***Microsoft Microsoft Windows 2000 Security:
Windows 2000 Stand-alone Offline Root Certificate Authority Protection Guide***

A Windows 2000 (W2K) Stand-alone Offline Root Certificate Authority (SaORCA) is an extremely important element in an organization's W2K Public Key Infrastructure (PKI). A W2K SaORCA is the cornerstone of an organization's W2K Certificate Authority (CA) Hierarchy and an organization's W2K CA Hierarchy is the frame to support an effective organizational W2K PKI.

Because of its importance, the W2K SaORCA requires an elevated level of protection to ensure the confidentiality and integrity of its own self-signed Root CA Certificate(s), of its own private key(s), and the issued and/or revoked Certificates that belong to its subordinate W2K CAs.

This protection guide is designed to offer a starting point for seasoned W2K Server Administrators assigned the organizational W2K PKI role and responsibility of W2K SaORCA Administrator. This guide is the combination of:

- a number of pre-existing Windows NT and Windows 2000 Security Checklists
 - Windows NT C2 Configuration Checklist
<http://www.microsoft.com/technet/security/C2config.asp>
 - Windows 2000 Installation Security Checklist.
<http://www.labmice.net/articles/securingwin2000.htm>
- a number of PKI references (both offline and online)
 - *Windows NT Security: Step by Step & Windows 2000: PKI* (J. Fossen)
 - The IETF Security Working Group: Public-Key Infrastructure (X.509) (pkix) <http://www.ietf.org/html.charters/pkix-charter.html>
 - The RSA Public Key Cryptography Standards
<http://www.rsasecurity.com/rsalabs/pkcs/>
- a number of years of experience the author has had with
 - Public Key Infrastructure (business, policy & technology)
 - Information Security
 - Windows NT 4.0 Security
 - Windows 2000 Security

This guide covers both technical and non-technical best practices to assist administrators protect the SaORCA and attain a degree of confidentiality and integrity that is required and in accordance with the organization's W2K PKI Certificate Policy, Certificate

Practice Statement, and/or all other applicable security policies.

Note: Although this guide was specifically designed to protect a W2K SaORCA server that DOES NOT have a network connection, it may be used as a baseline document to create a protection guide for a W2K SaORCA server that does have network connectivity.
Part 1: Obtain the Knowledge to Protect the W2K SaORCA

❑ Research/Review Public Key Infrastructure Concepts

Administrators new to PKI should familiarize themselves with PKI concepts, technology, and operations, such as: Public-Private Key Pair, Digital Signature, Certificate Policy (CP), Certificate Practice Statement (CPS), Certificate Authority (CA), Registration Authority (RA), Directory Service (DS), Certificate Revocation List (CRL), X.509 Certificates, Public Key Cryptography Standards (PKCS), and the list goes on and on.

A great way to start is by attending a PKI Training Course offered by a reputable PKI vendor or Technical Training Organization. Many vendors offer both online and traditional face-to-face classroom instruction. Here are just a few:

- Verisign PKI Training
<http://www.verisign.com/training/courses/pki/index.html>
- Xcert Resources
<http://www.xcert.com/resources/index.html>
- Entrust PKI Training
<http://www.entrust.com/training/courses.htm>

Another way to acquire PKI knowledge, specifically W2K PKI knowledge, is through the Certificate Services. Once installed additional Windows 2000 PKI information is available via the Certificate Services built-in help files. If the help files are not available at this time, much of the same PKI information can be found online. Here are some the online links to start with:

- Planning Your Public Key Infrastructure -
<http://www.microsoft.com/technet/win2000/dguide/chapt-12.asp>
- Windows 2000 Certificate Services Best practices -
http://windows.microsoft.com/windows2000/en/server/help/sag_cs_bestpract.htm
- Creating a certification hierarchy with an offline root certification authority -
http://windows.microsoft.com/windows2000/en/server/help/sag_CS_Checklist_Offline.htm

- To install a stand-alone root certification authority -
http://windows.microsoft.com/windows2000/en/server/help/sag_CSprocsInstallRoot_SA.htm
- Certificate Overview -
<http://windows.microsoft.com/windows2000/en/server/help/default.asp>

For additional information concerning PKI, here are just a few excellent online resources to begin with:

- The IETF Security Working Group: Public-Key Infrastructure (X.509) (pkix) -
<http://www.ietf.org/html.charters/pkix-charter.html>
- The RSA Home Page -
<http://www.rsasecurity.com/>
- Site dedicated to listing PKI References -
<http://www.pkiforum.org/resources/>

Reminder: It is a good idea to start a PKI Favorites Folder in I.E. before you start browsing. Once you get out and onto the PKI information highway you'll be able to quickly "Add" your preferred PKI websites with a quick click of the mouse.

❑ **Review Organizational Security Policies**

To effectively administer the SaORCA an administrator must be familiar with all organizational information security (InfoSec) policies. SaORCA Administrators will definitely become extremely familiar with the W2K PKI CP and CPS. (Keeping a copy close by is a recommended... "best practice".)

When reviewing the CP/CPS administrators should pay particular attention to the areas that will affect W2K SaORCA administrative tasks as well as protective measures. Here are the normal CP areas to look out for:

- Compliance audit frequency and topics
- Security audit procedures used to describe event logging and audit systems
- Key changeover
- Compromise and disaster recovery
- CA termination
- Physical security controls
- Technical security controls like PINs, passwords, or manually-held key shares
- Network security controls like disabling unnecessary services
- Cryptographic module engineering controls that addresses identification of the
- Cryptographic module roles and services, physical security, operating system security, algorithm compliance, etc.

❑ ***Review Organizational PKI Design and/or Implementation Plan***

An organization's PKI Design and/or Implementation Plan covers a number of issues relevant to SaORCA administration. For instance, the CA hierarchy plan addresses the naming convention that, in turn, directly affects the SaORCA Computer Name.

Part 2: Physically Protect the W2K SaORCA

❑ **Physical Protection**

Ensure the physical protection of the W2K SaORCA, (and the W2K SaORCA backup), is in accordance with the CP/CPS, Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), etc. For example:

- When not in use, the SaORCA is stored in a locked room with video monitoring and logged access
- When not in use the SaORCA is stored in a locked cabinet in the server room
- Surveillance cameras are required inside and outside the data center
- Physical access to the machine requires the “two man rule”
- When not in use, the hard drive must be removed and placed in the vault
- Backup media is stored at an alternate site (at least 25 miles away)



❑ **Machine Requirements**

Ensure the selected computer meets the minimum system requirements outlined by Microsoft for a Windows 2000 Server (plus Certificate Services).

Computer's hardware configuration is in compliance with the organization's CP/CPS:

- The CP may specifically state that the SaORCA will not have networking capability – no NIC, no Modem, no infrared capability, etc.
- The Computer has Power on Password Protection (If required and/or available)
- Third party products are authorized for use:
 - Smart card readers used in two-factor authentication
 - Zip disk drive used to transport certificates and certificate requests

Part 3: Protect W2K SaORCA Operations

□ Network Connectivity

As a rule of thumb, a root ca should not be connected to a network and should only issue Subordinate CA Certificates. The certificates are transported via a peripheral media device such as a floppy or zip disk.

Organizational business objectives and money play important roles in whether or not the SaORCA is connected to the network or not.

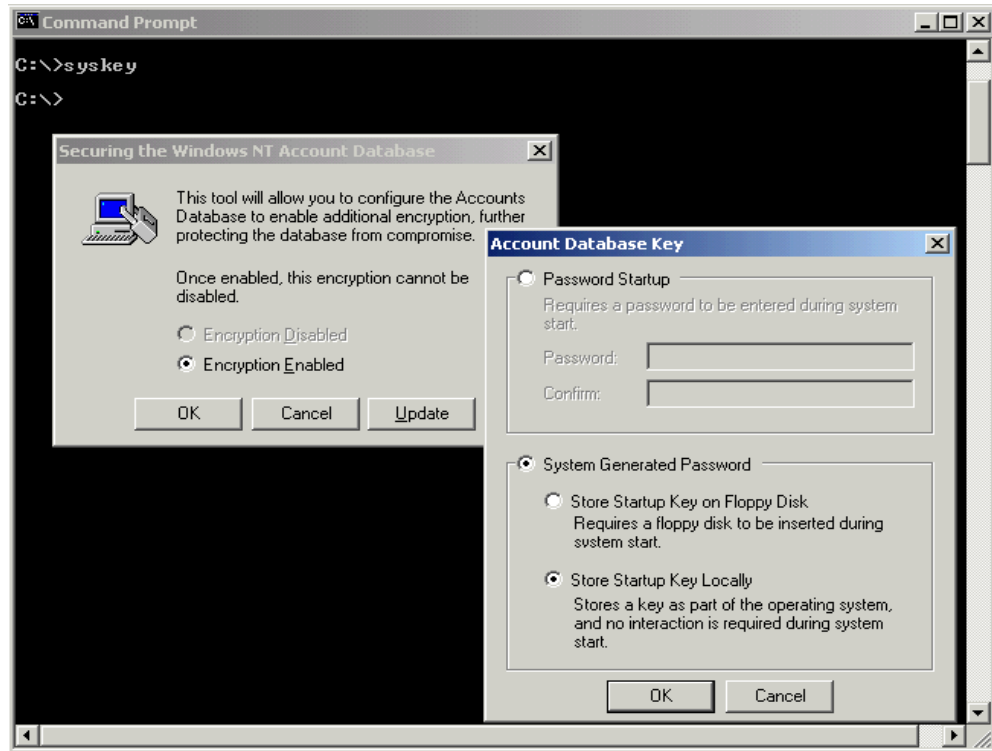
Remember,... this guide is designed for a “**connectionless**” computer.

□ Operating System

The W2K SaORCA contains only one Operating System: Windows 2000 Server or Windows 2000 Advance Server.

□ Boot Protection

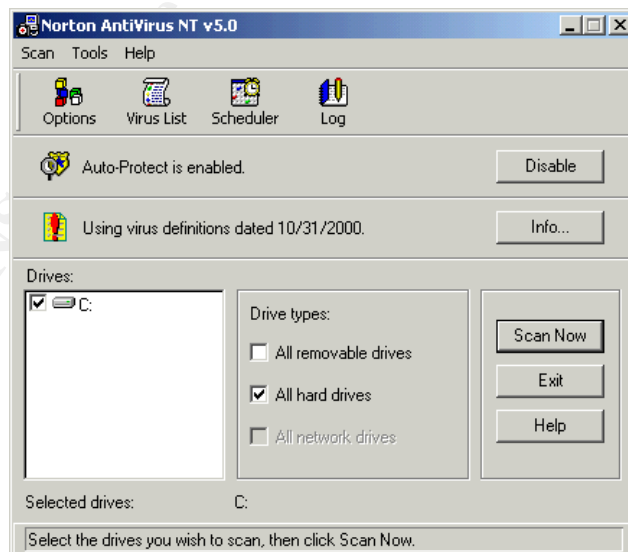
Windows 2000 Server offers “syskey” as another layer of protection to limit access to the Operating System. The use of “syskey” is optional for a W2K SaORCA since it will be physically protected from access and not connected to a network.



From the command line > "syskey" then, update for available options.

❑ Anti-Virus Protection

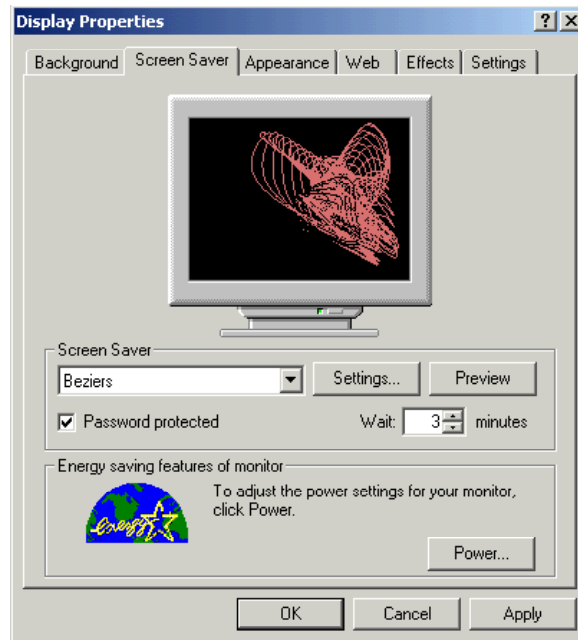
Anti-Virus Protection must be installed, operational, and current. Procedures must be in place to update the virus protection software package.



Anti-Virus Software provides an extra layer of protection when importing/accepting possibly infected certificate requests.

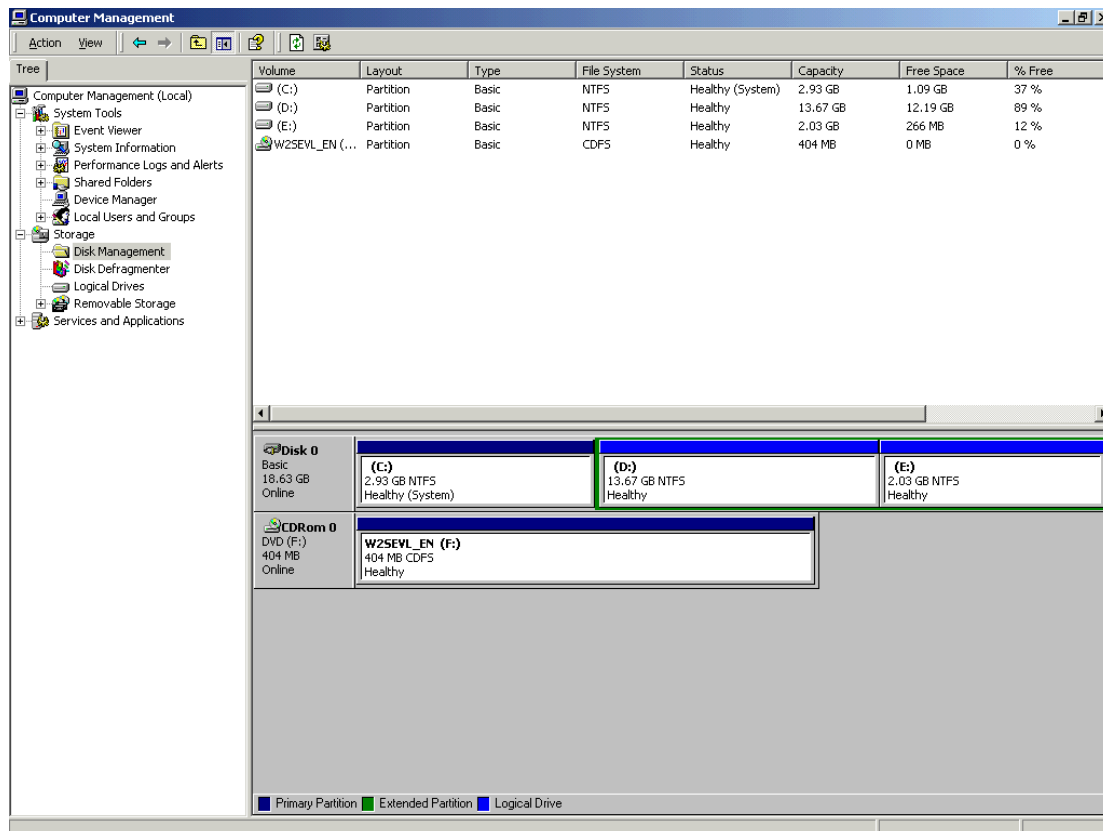
❑ Screen Saver

The password protected screen saver is yet another optional layer of protection that may be applied to a W2K SaORCA. (Policy will drive its use and configuration)

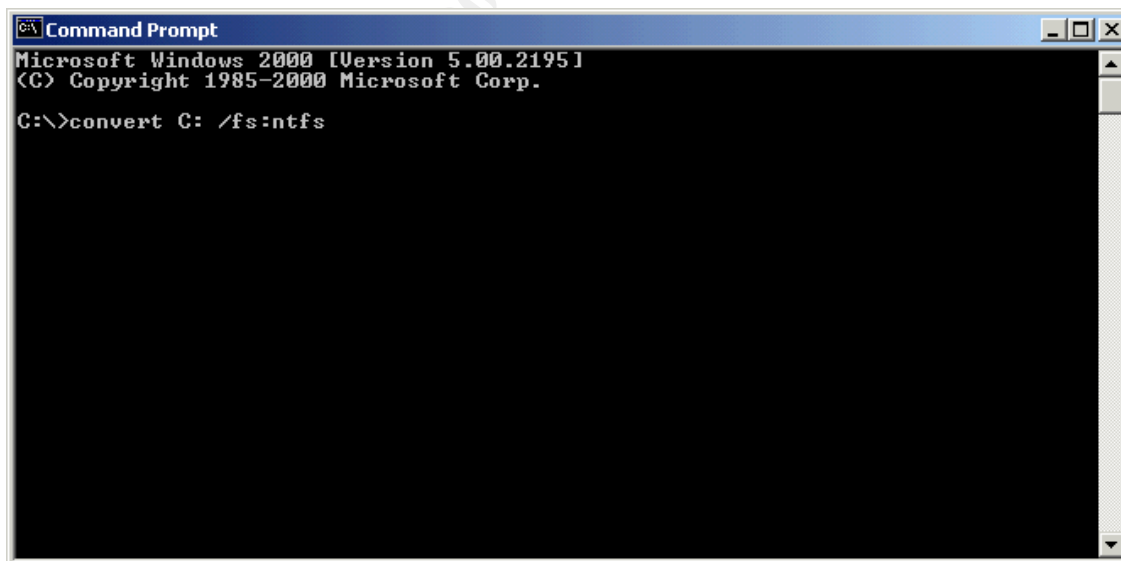


❑ Partitions

All partitions must be NTFS. Right Click on a partition for formatting options.



Right Click: My Computer > Manage > Storage > Disk Management

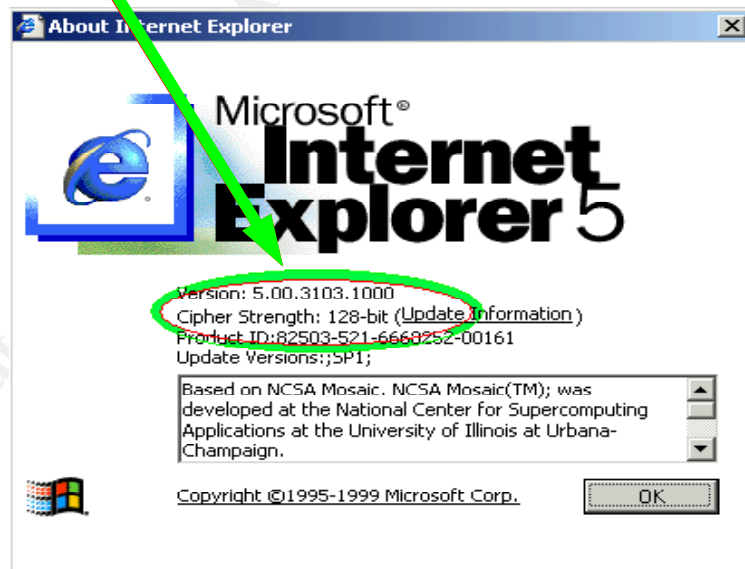
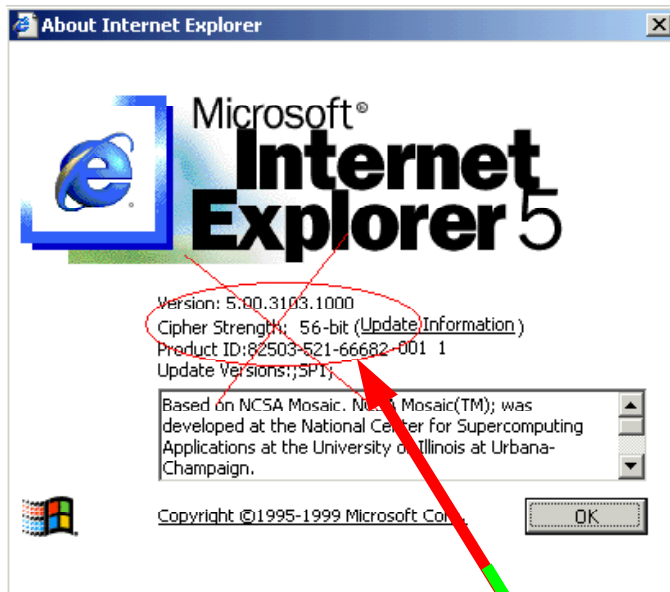


To format from the command line.

❑ High Encryption Pack

The High Encryption Pack (HEP) must be installed on the computer. The Cipher

Strength should read 128-bit.



From Desktop Select: Internet Explorer > Help > About Internet Explorer

The EHP upgrade only takes a few seconds and is available via internet download or CD.
<http://www.microsoft.com/windows2000/downloads/recommended/sp1/default.asp>

The upgrade will not affect previously created keys. If these previously created keys exist an upgrade is possible with the use of the Key Migration Tool. See next section, "Service Packs", for more information.

❑ **Service Packs**

The latest service pack must be installed on the computer. The Service Pack is available via internet download or CD.

<http://www.microsoft.com/windows2000/downloads/recommended/sp1/default.asp>



Select: Start > Run > Open: “winver”

❑ Microsoft Security Notification Service

All Windows 2000 Administrators, including W2K CA Administrators, should subscribe to the Microsoft Security Notification Service to keep abreast of the latest security vulnerabilities.

To subscribe visit the following website:

<http://www.microsoft.com/technet/security/notify.asp>

Most bulletins and their related patches are for network related issues and will not directly affect W2K SaORCA operations. But, for audit purposes, the CA Administrator must be aware of all known server vulnerabilities and their fixes. Administrators must also be on the look out for performance related issues.

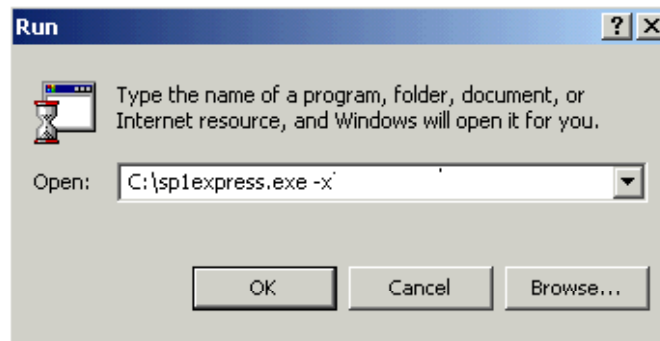
To view current bulletins or search for earlier bulletins visit the following website:

<http://www.microsoft.com/technet/security/current.asp>

Note: Ultimately, the CA Administrator is responsible for being aware of all known vulnerabilities and performance issues and then deciding which fixes to apply.

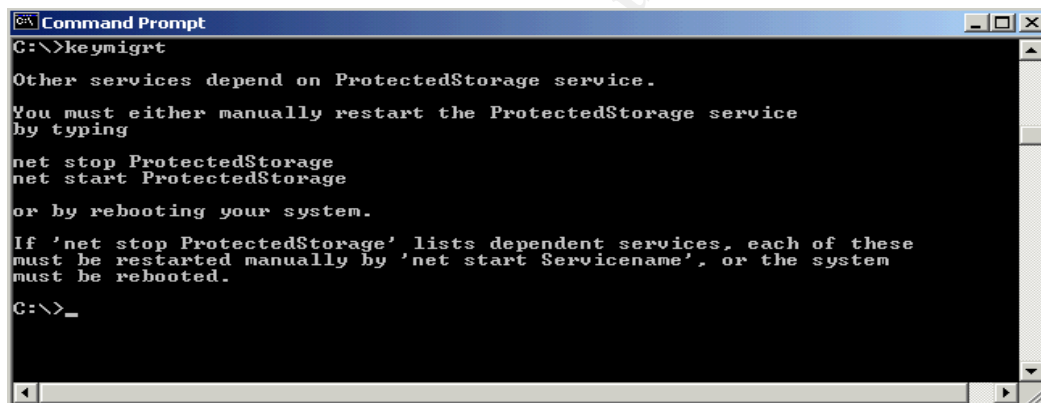
□ Key Migration Utility

Once the **Service Pack** is installed the Key Migration Tool may be extracted for use.

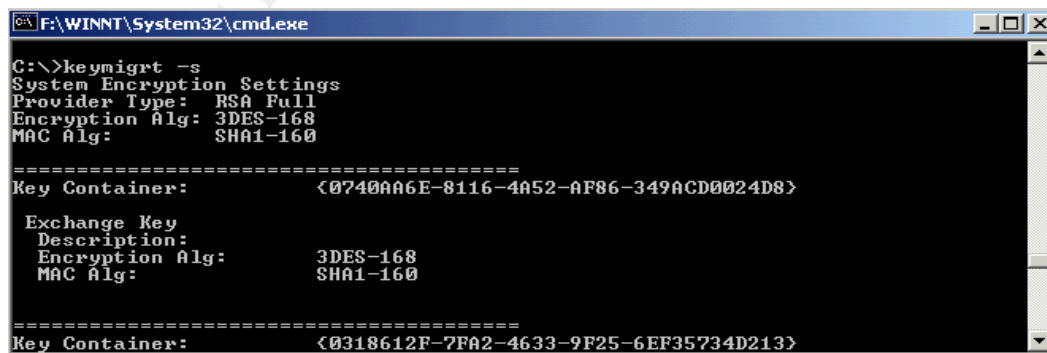


The “keymigt” executable can be extracted for use with the “-x” switch.

Use the “keymigt” tool to verify key(s) upgrade status.



Execute: >“keymigt” and then, Stop Storage



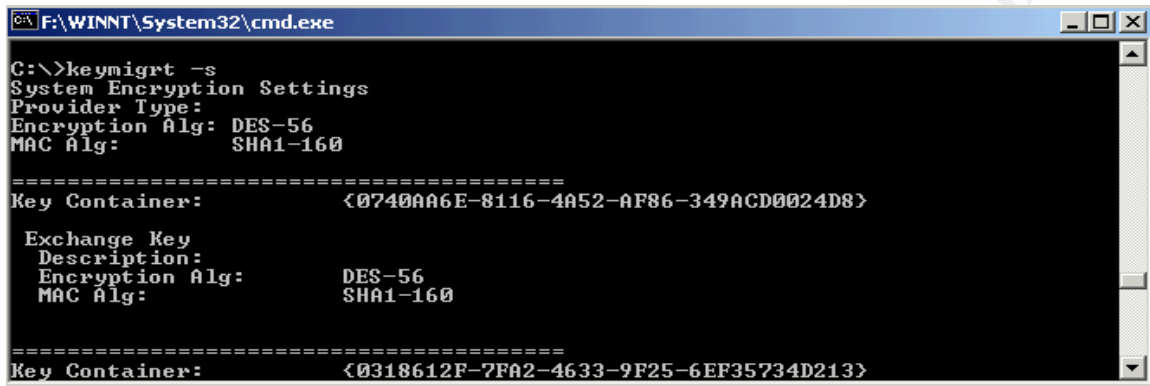
Execute: >“keymigt -s”

As seen above, the System Encryption Settings indicate encryption upgrade status. If

private keys and containers exist they also appear.

“Keymigrt” was designed to upgrade keys that were created prior to an EHP upgrade.

As seen below, if weak keys exist, simply migrate the encryption keys using the tool. (Migrate keys that are less than 3DES-168)



```
C:\>keymigrt -s
System Encryption Settings
Provider Type:
Encryption Alg: DES-56
MAC Alg: SHA1-160

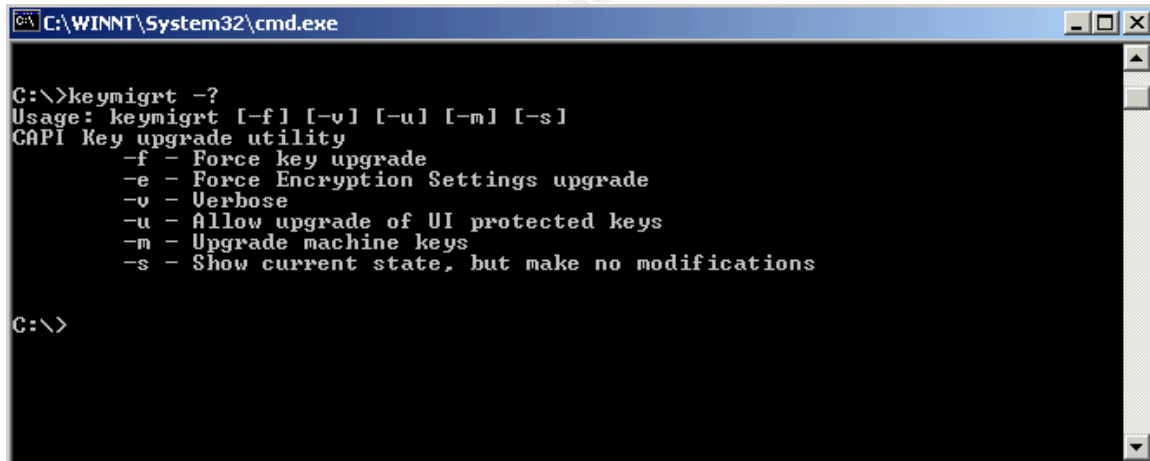
=====
Key Container: <0740AA6E-8116-4A52-AF86-349ACD0024D8>

Exchange Key
Description:
Encryption Alg: DES-56
MAC Alg: SHA1-160

=====
Key Container: <0318612F-7FA2-4633-9F25-6EF35734D213>
```

Execute: “keymigrt -s”

Using the command “Keymigrt -s >> output.txt” will create a text file that can be used for audit and analytical purposes.



```
C:\>keymigrt -?
Usage: keymigrt [-f] [-v] [-u] [-m] [-s]
CAPI Key upgrade utility
-f - Force key upgrade
-e - Force Encryption Settings upgrade
-v - Verbose
-u - Allow upgrade of UI protected keys
-m - Upgrade machine keys
-s - Show current state, but make no modifications

C:\>
```

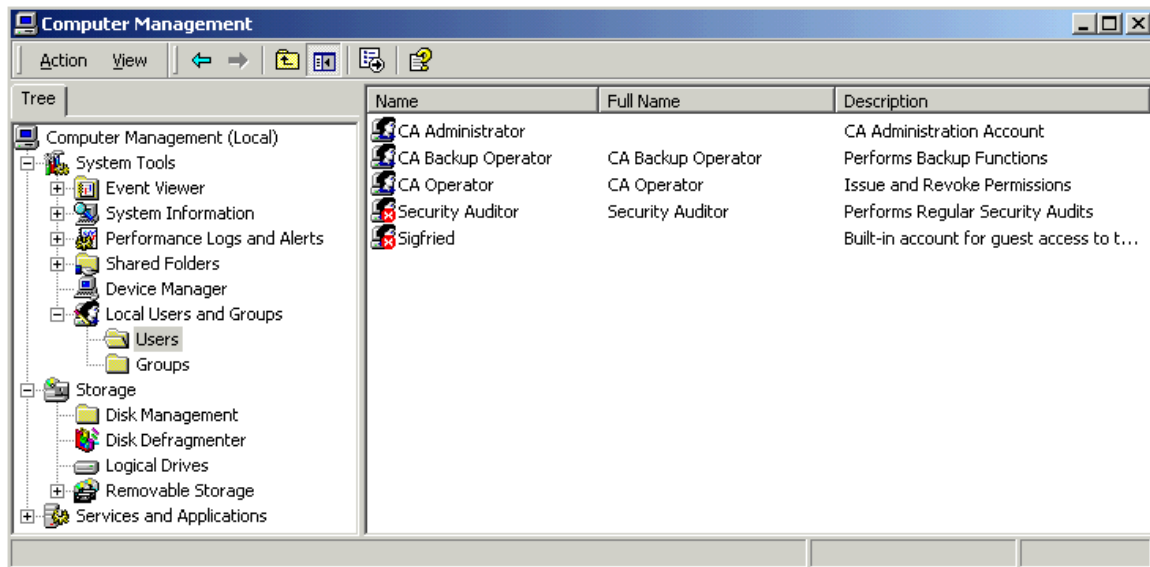
To view all “keymigrt” options ... *Execute: > “keymigrt -?”*

To perform a complete upgrade *Execute: > “keymigrt -v -m -u -f -e”*

Note: To avoid Key Migration issues of any kind, ensure the EHP is installed

prior to Certificate Service Installation.

❑ Manage Accounts



- Limit accounts to only those PKI Roles specified in the CP/CPS. Normal PKI Administration Roles are: CA Administrator (Renamed Administrator Account), CA Operator, Security Auditor, and CA Backup Operator.
- Disable all newly created accounts, i.e., Security Auditor, until they are needed.
- Delete built in accounts that are not required.
- Disable the Guest Account (renamed) and create an extremely complex password.
- Keep account management simple. W2K SaORCA access auditing/record keeping is extremely important to the integrity of SaORCA Operations. Look to CP/CPS for further guidance.

❑ Shut down unnecessary Devices

The SaORCA hardware configuration should consist of the minimum required devices to get the job done. The SaORCA normally requires peripheral storage devices such as Floppy Drives and/or Zip Drives for Certificate Management.

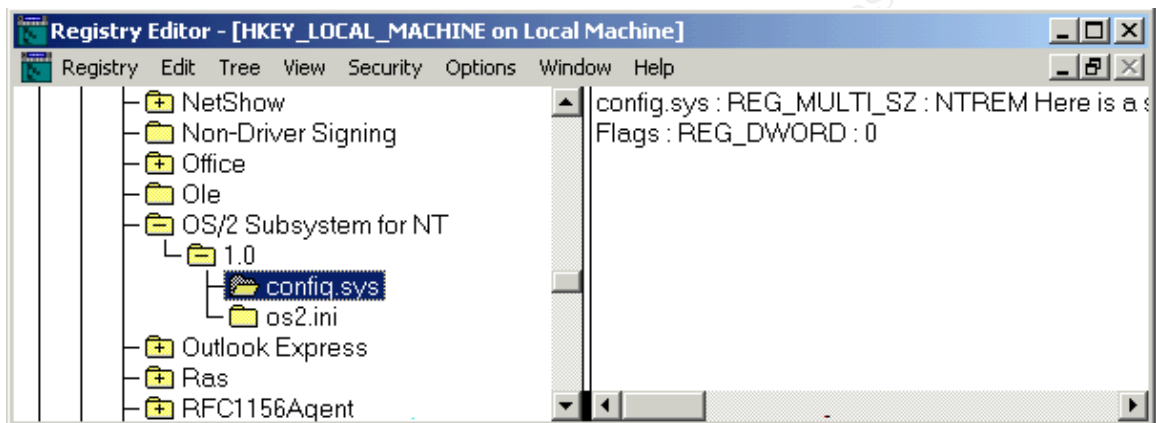
When dealing with a connectionless SaORCA, services like TCP/IP and accompanying tcpip.sys driver are not a concern.

The primary concern over devices in a connectionless SaORCA is for audit purposes and system performance.

❑ Remove the OS/2 and POSIX Subsystems

Removing these subsystems only help to improve the system's performance. If performance is an issue, disable these subsystems by simply making the following changes to the Registry:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT



Delete all sub keys

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment

Delete the value for Os2LibPath

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems

Delete the value for Optional

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems

Delete entries for Posix and OS/2

Part 4: Protect W2K SaORCA Operations with Local Computer Policy

Since the machine is connectionless, the Local Computer Policy settings will effectively protect a great majority of the standard Windows 2000 Operating System features. (Features normally considered to be, security “holes.”)

In the sub-sections that follow:

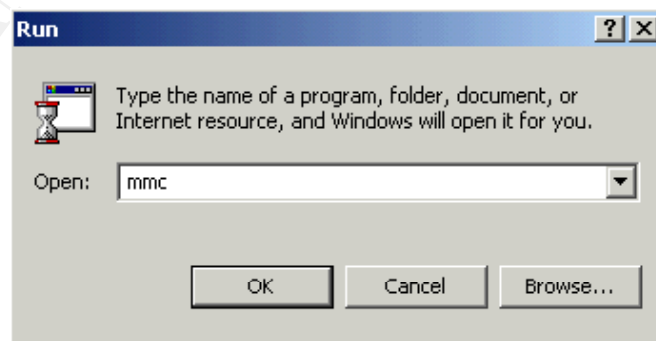
- Part 4a: Create a W2K SaORCA High Security Template (SaORCAHiSec.inf)
- Part 4b: Analyze Local Computer Policy and update SaORCAHiSec.inf
- Part 4c: Save and Implement SaORCAHiSec.inf Template

A Windows 2000 Security Template will be created, saved, and then, applied to the W2K SaORCA. Application of the template will directly affect the following containers:

- Account Policies
- Local Policies
- Event Log
- Restricted Groups
- System Services
- Registry
- File System

Part 4a: Create a W2K SaORCA High Security Template (SaORCAHiSec.inf)

❑ Create the new Template



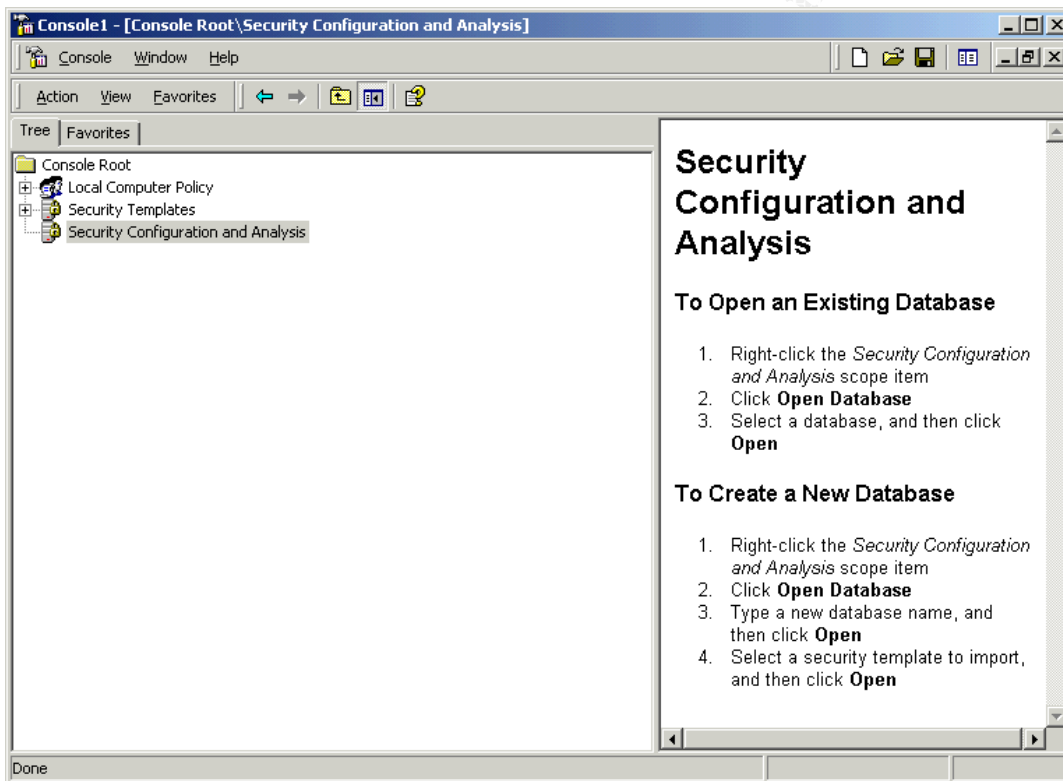
Open: “MMC” or, Execute from Command Line “gpedit.msc”

Load the “Local Computer Policy”, “Security Templates”, and “Security Configuration and Analysis” Snap-ins. Expand “Security Templates” and then, right click the “hisecdc.inf” security template and “Save as... SaORCAHiSec.inf”. The new template may now be used to analyze the local computer.

Part 4b: Analyze Local Computer Policy and update SaORCAHiSec.inf

❑ Perform the analysis

Analyze the current local policy using the new “SaORCAHiSec.inf” security template.



*Instructions to analyze the computer appear automatically in the “mmc”.
For more information view the built-in help files.*