Introduction to IKeyman Utility and IKeyman Troubleshooting

Jim Li
IBM WebSphere Level 2 Support

Agenda

- SSL Overview
- GSKit Overview
- IKeyman Overview
- IKeyman Troubleshooting
- Common IKeyman Problems
- Questions and Answers

SSL Overview

- SSL (Secure Sockets Layer) is an encryption system used on servers to ensure privacy when transmitting data across internet.

- Server needs a public-private key pair and a certificate. The server uses its private key to sign messages to clients.

- To send its public key to clients, the server needs a certificate issued by a certification authority (CA).

- A certification authority (CA) is a trusted third party that issues certificates.

GSKit Overview

- GSKit (Global Security Kit)
  - GSKit provides SSL (Secure Socket Layer) functions for IBM Products
  - GSKit provides IKeyman (IBM Key Management Utility)
- GSKit packages
  - WAS, IHS, Edge, MQ, Tivoli, etc.
  - Contact product support for IKeyman problems

GSKit Version

- To check GSKit full version, run following command
    - gsk5ver for GSKit 5
    - gsk7ver for GSKit 7

- On Windows – checking from Window registry

  HKEY_LOCAL_MACHINE\SOFTWARE\IBM\GSK7\CurrentVersion

- http://www.redbooks.ibm.com/redbooks/pdfs/sg246325.pdf

IKeyman Overview

- IKeyman (IBM Key Management Utility)
  - Java-based application to manage keys and key databases

- With IKeyman, you can
  - Create a new key database
  - Add root CA to your database
  - Request and receive a certificate from a CA
  - Set default keys
  - Change password

- http://www.ibm.com/support/docview.wss?uid=swg24010275

IKeyman Debugging

- Examples to run GSKit 7 IKeyman debugging
  - `gsk7ikm -Dkeyman.debug=true -Dkeyman.jnitracing=YES`
  - `gsk7cmd -Dkeyman.debug=true -Dkeyman.jnitracing=YES`
- Check log files
  - ikmcdbg.log, ikmgdbg.log, ikmjdbg.log
- http://www.ibm.com/support/docview.wss?uid=swg21202820

Common IKeyman Problems

- Cannot Start IKeyman
- Cannot Load GSKit Lib
- Cannot Create kdb File
- Missing an Intermediate Certificate
- Expired Certificates
- Corrupted Certificates
- No Request Key Error

IKeyman Issues

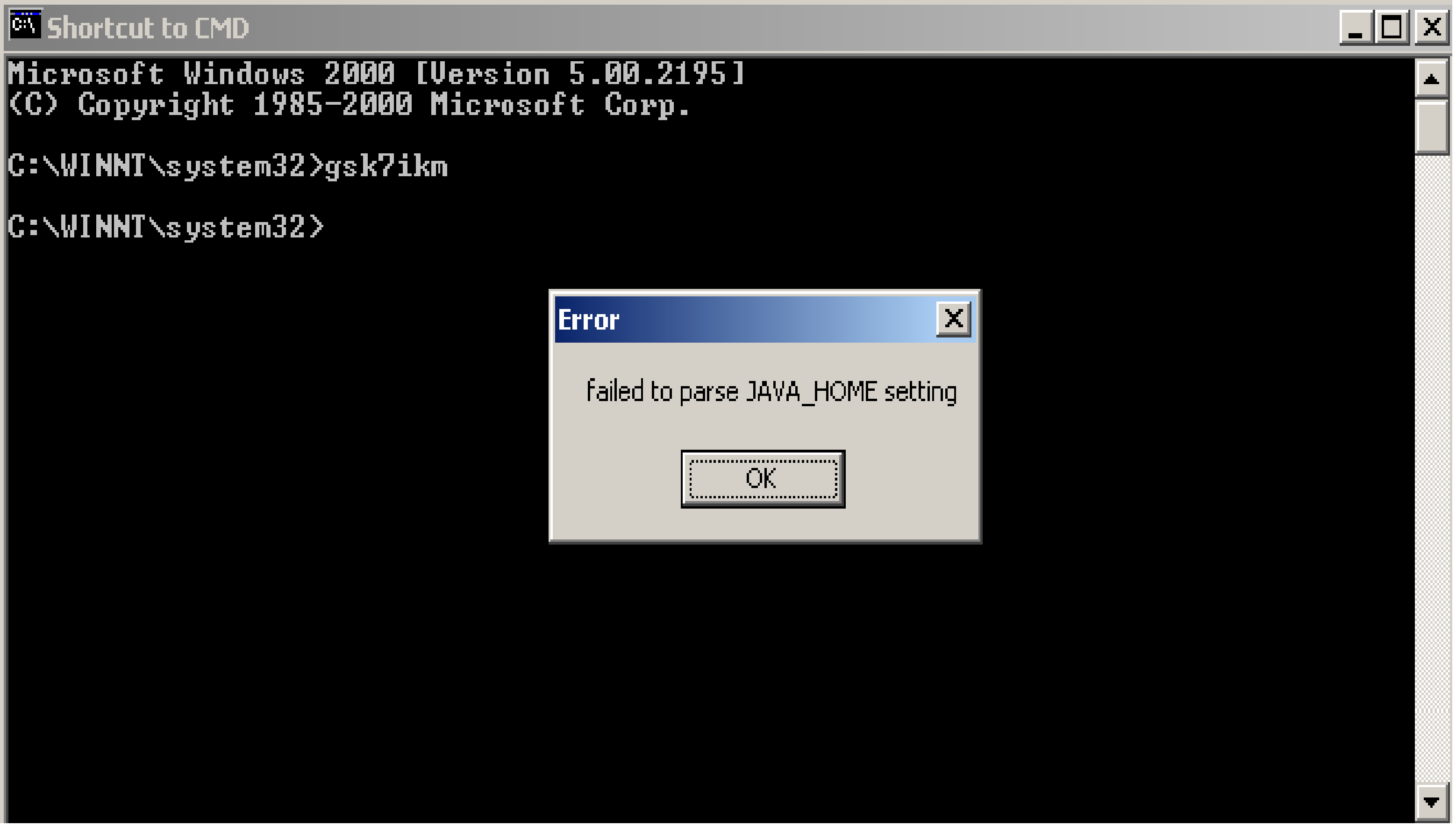
- Upgrading GSKit to the Latest Level
  - Many issues fixed
  - VeriSign root CA expiration
- APAR for the latest GSKit
  - PK09108 - GSKit 7.0.3.17
  - PK02947 - GSKit 5.0.5.97
- http://www.ibm.com/support/docview.wss?uid=swg27005198

Cannot Start IKeyman

- Error Message
    - “Failed to parse JAVA_HOME Setting”
    - Cause: JAVA_HOME is not set
    - Solution: Set JAVA_HOME=C:\java141\jre\

- SDK (JDK)
    - Solaris requires Sun JDK
    - All other platforms require IBM SDK
    - GSKit 5 requires Java 1.3.1
    - GSKit 7 requires Java 1.4.1 or above

Cannot Start IKeyman



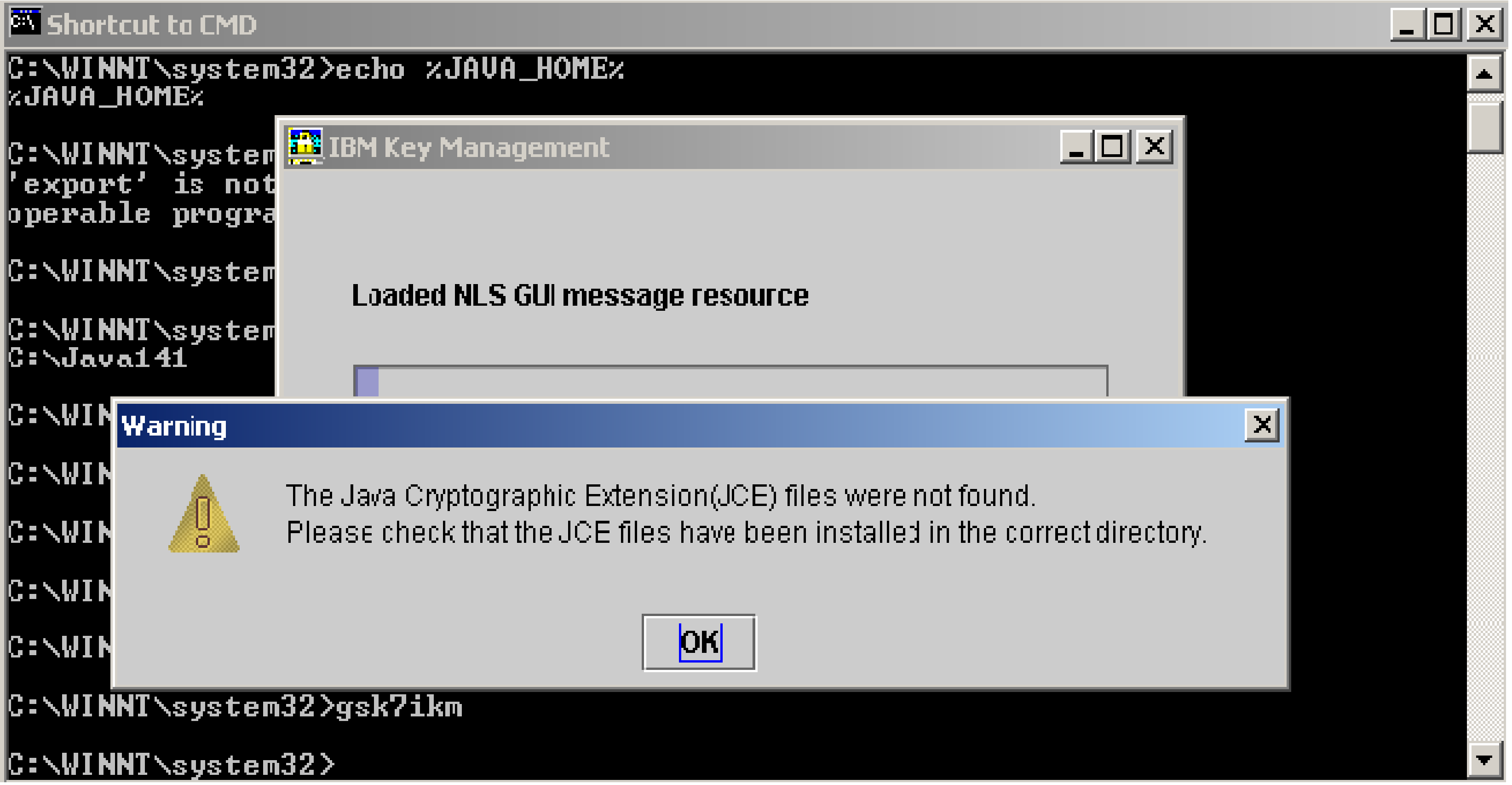
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>gsk7ikm

C:\WINNT\system32>
```

failed to parse JAVA_HOME setting

Cannot Start IKeyman



```
C:\WINNT\system32>echo %JAVA_HOME%
%JAVA_HOME%

C:\WINNT\system
'export' is not
operable progra

C:\WINNT\system

C:\WINNT\system
C:\Java141

C:\WIN

C:\WIN

C:\WIN

C:\WIN

C:\WIN

C:\WINNT\system32>gsk7ikm

C:\WINNT\system32>
```

Loaded NLS GUI message resource

The Java Cryptographic Extension(JCE) files were not found.
Please check that the JCE files have been installed in the correct directory.

Cannot Start IKeyman

- Under JAVA_HOME/jre/lib/ext directory
  - Rename ibmjsse.jar, gskikm.jar and ibmjcaprovider.jar

- Update JAVA_HOME/jre/lib/security/java.security
  - security.provider.1=sun.security.provider.Sun
  - security.provider.2=com.ibm.spi.IBMCMSProvider
  - security.provider.3=com.ibm.crypto.fips.provider.IBMJCEFIPS
  - security.provider.4=com.ibm.crypto.provider.IBMJCE

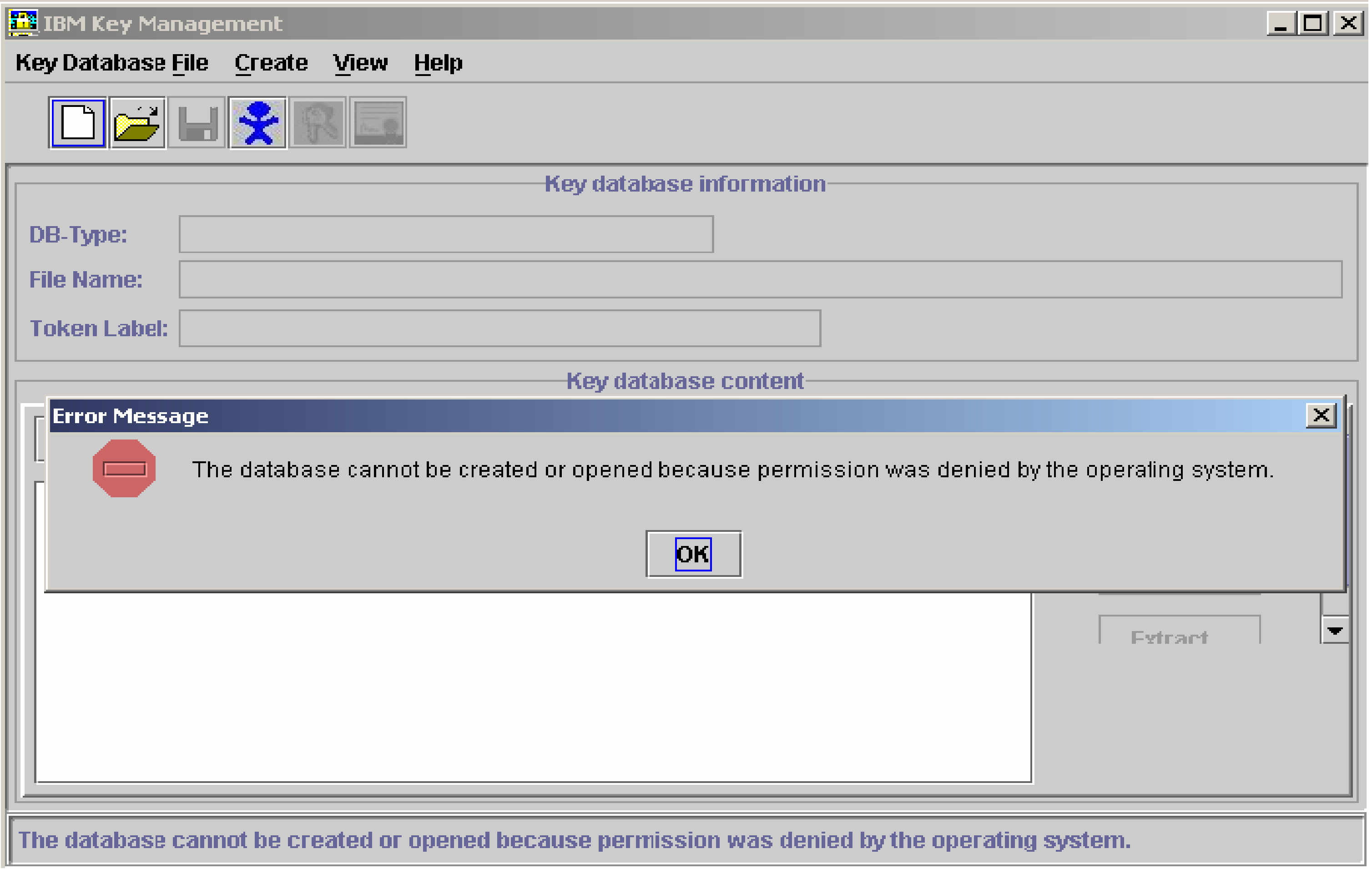
- http://www.ibm.com/support/docview.wss?uid=swg21172447

Cannot Create kdb File

- Problems
    - Cannot create a kdb file
    - No cms option to create a kdb file
- Causes
    - No write-permission
    - Expired Root CA

- http://www.ibm.com/support/docview.wss?uid=swg21166332

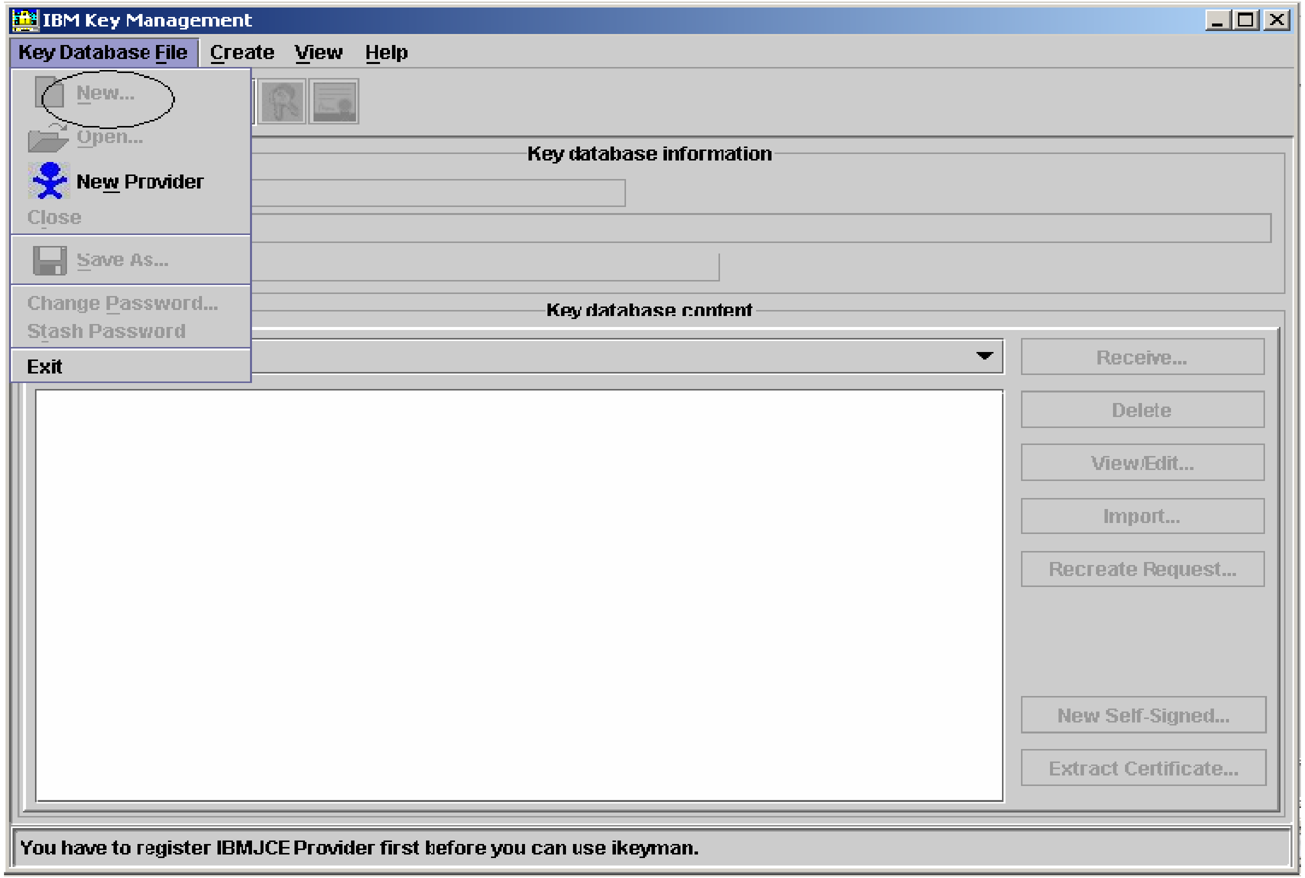
Cannot Create kdb File



The database cannot be created or opened because permission was denied by the operating system.

The database cannot be created or opened because permission was denied by the operating system.

Cannot Create a kdb File



You have to register IBMJCE Provider first before you can use ikeyman.

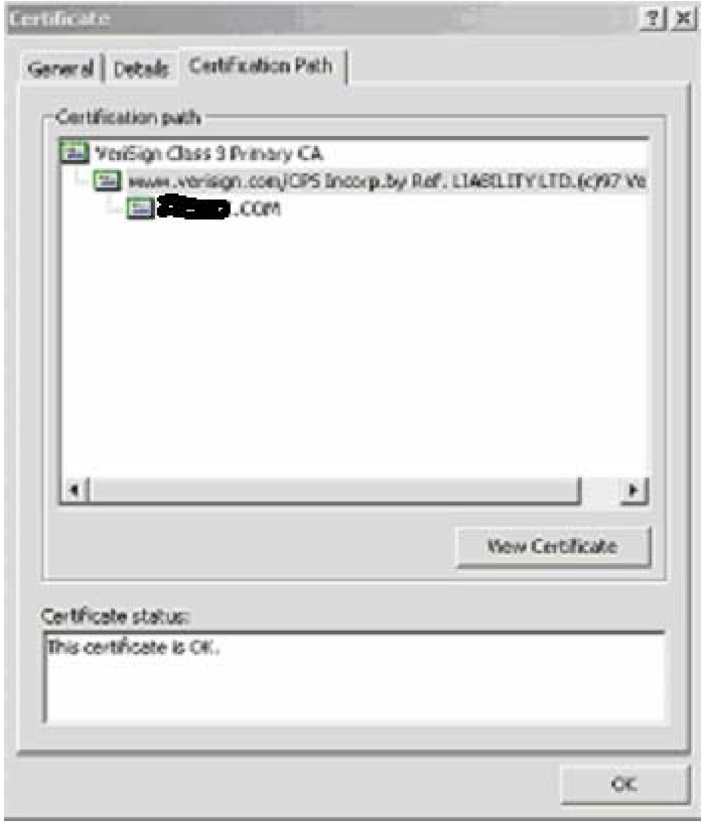
Missing an Intermediate Certificate

- IKeyman error

"An error occurred while storing the certificate from the given file"

- Cause
    - Missing an intermediate CA?
- Verifying
    - Rename certificate as cert.cer file open it in Window Explorer
    - Click the 'Certification Path'
- http://www.ibm.com/support/docview.wss?uid=swg21006397

Certificate with an Intermediate CA



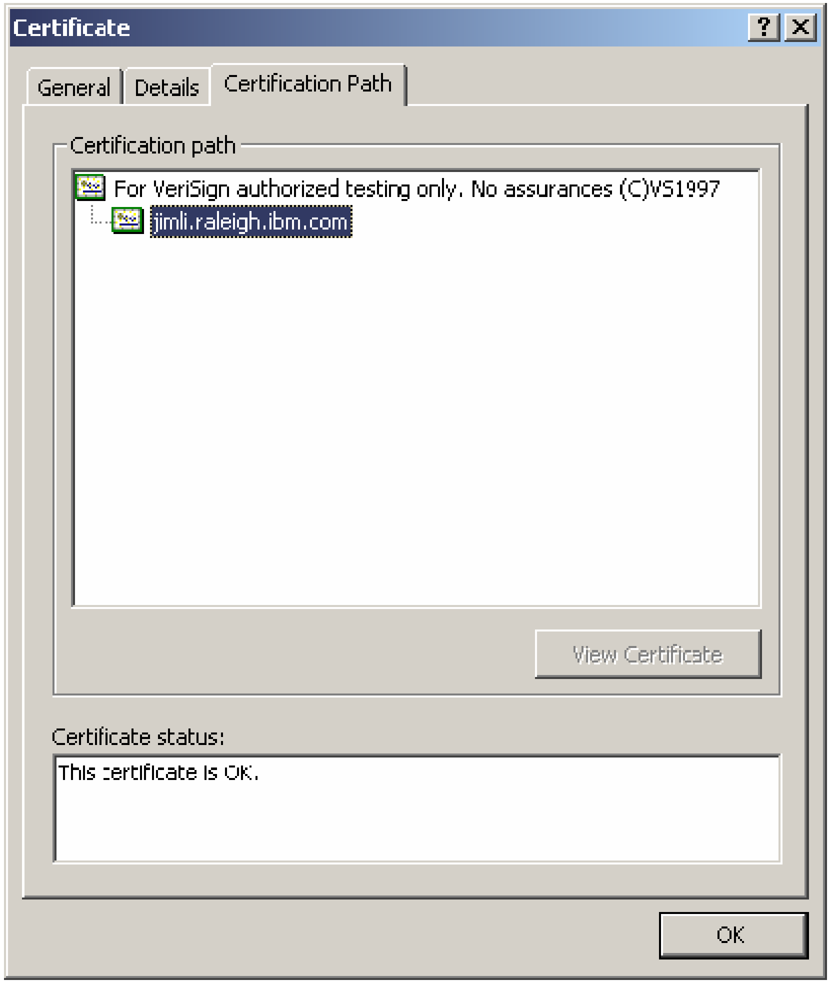
Certification path

VeriSign Class 3 Primary CA
www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 Ve
[redacted].com

Certificate status:

This certificate is OK.

Certificate without an Intermediate CA



For VeriSign authorized testing only. No assurances (C)VS1997
jimli.raleigh.ibm.com

Certificate status:

This certificate is OK.

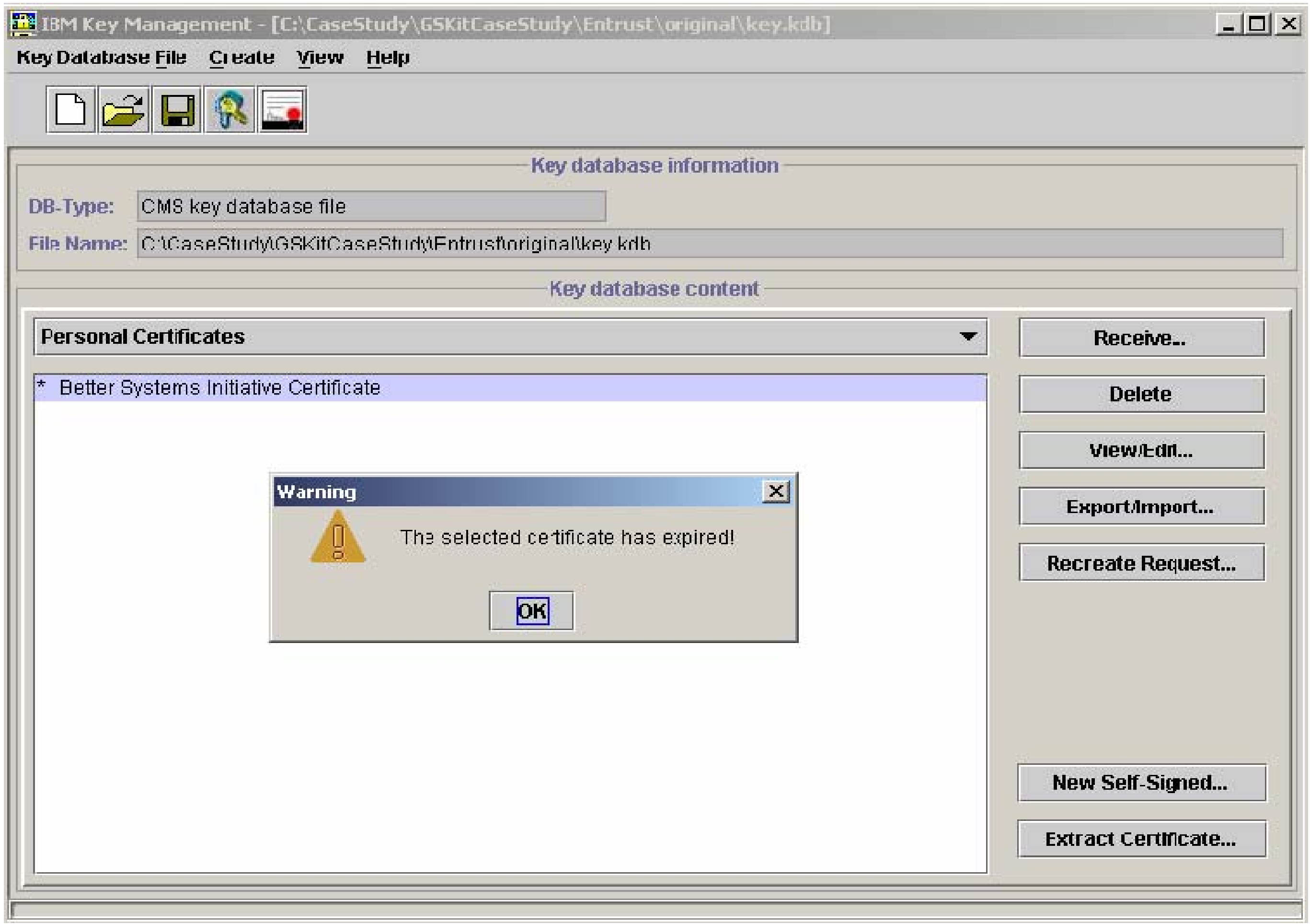
Expired Certificates

- Error message from IHS error log

“[error] mod_ibm_ssl: SSL Handshake Failed, Invalid date.”

- Verifying from IKeyman
  - Open kdb file and highlight the certificate
  - Click View/Edit button
- Verifying from Internet Explorer: double click locker icon
- Renewing an expired certificate
  - http://www.ibm.com/support/docview.wss?uid=swg21045925

Verifying Expiration from IKeyman



IBM Key Management - [C:\CaseStudy\GSKitCaseStudy\Entrust\original\key.kdb]

Key database information

DB-Type: CMS key database file

File Name: C:\CaseStudy\GSKitCaseStudy\Entrust\original\key.kdb

Key database content

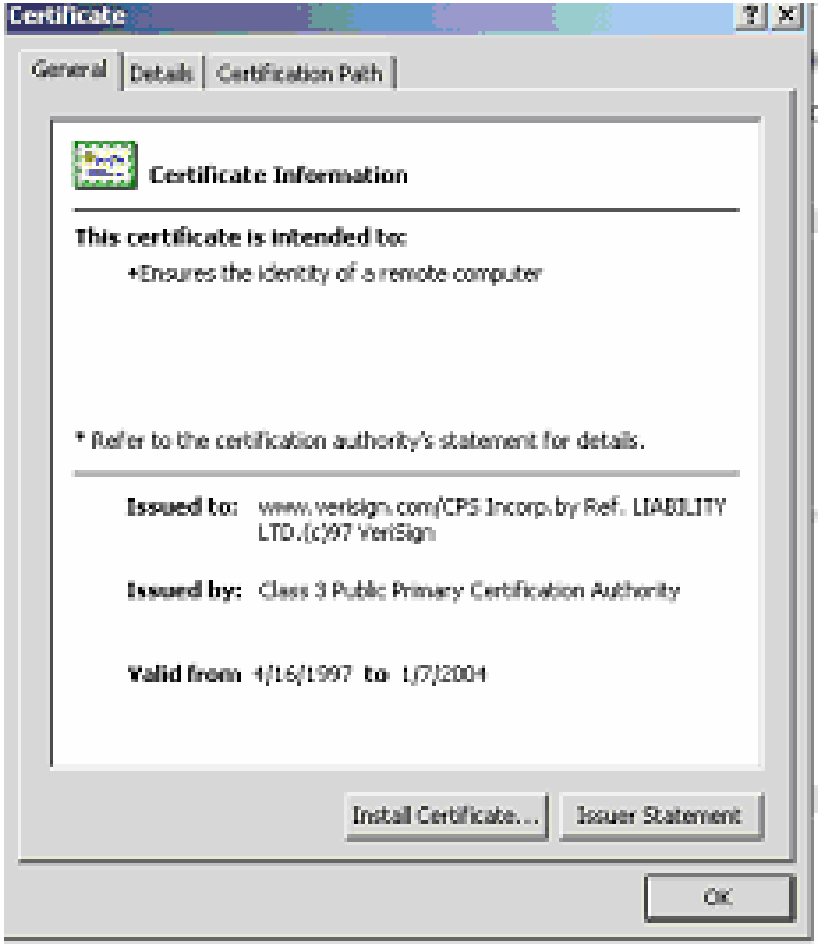
Personal Certificates

* Better Systems Initiative Certificate

Warning

The selected certificate has expired!

Verifying Expiration from IE



Certificate Information

This certificate is intended to:

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign

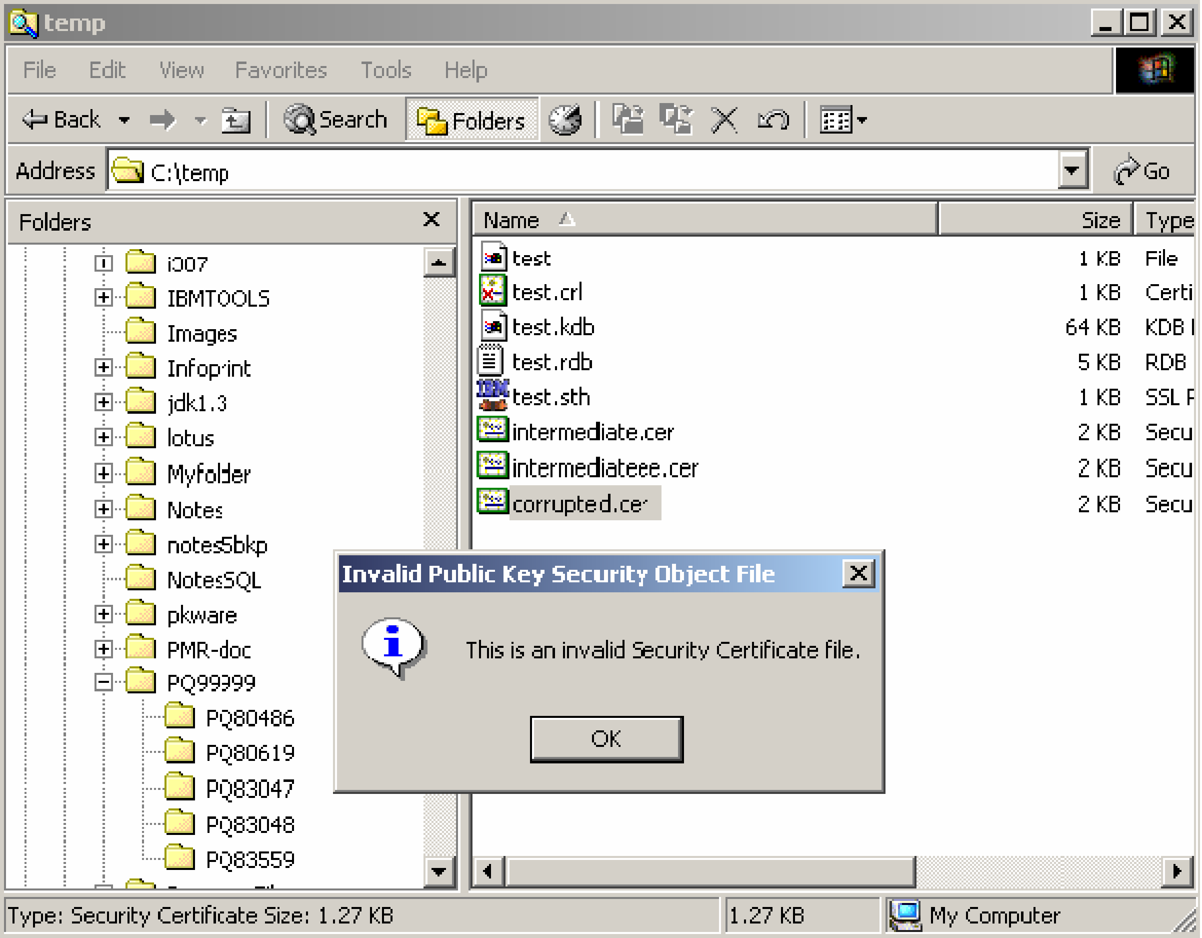
Issued by: Class 3 Public Primary Certification Authority

Valid from 4/16/1997 **to** 1/7/2004

Corrupted Certificate

- Error message from IKeyman
  “The internal database handle table is corrupted”
- Verifying the certificate
  - Rename the certificate as a .cer file
  - Double click cert.cer
- Solution
  - Request a new one

Corrupted Certificate



Address: C:\temp

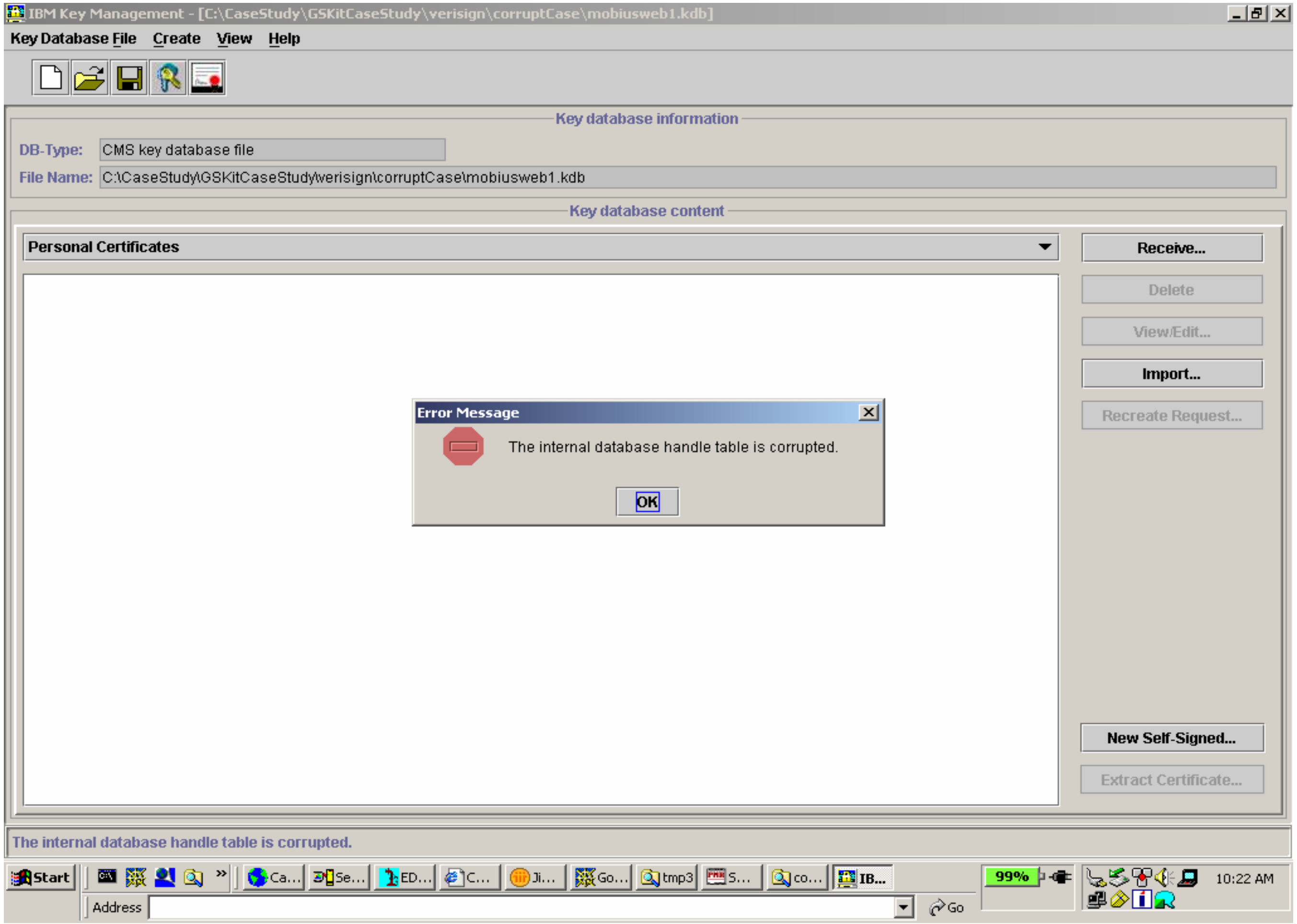
Name	Size	Type
test	1 KB	File
test.crl	1 KB	Certi
test.kdb	64 KB	KDB I
test.rdb	5 KB	RDB
test.sth	1 KB	SSL F
intermediate.cer	2 KB	Secu
intermediateee.cer	2 KB	Secu
corrupted.cer	2 KB	Secu

Invalid Public Key Security Object File

This is an invalid Security Certificate file.

Type: Security Certificate Size: 1.27 KB | 1.27 KB

Corrupted Certificate



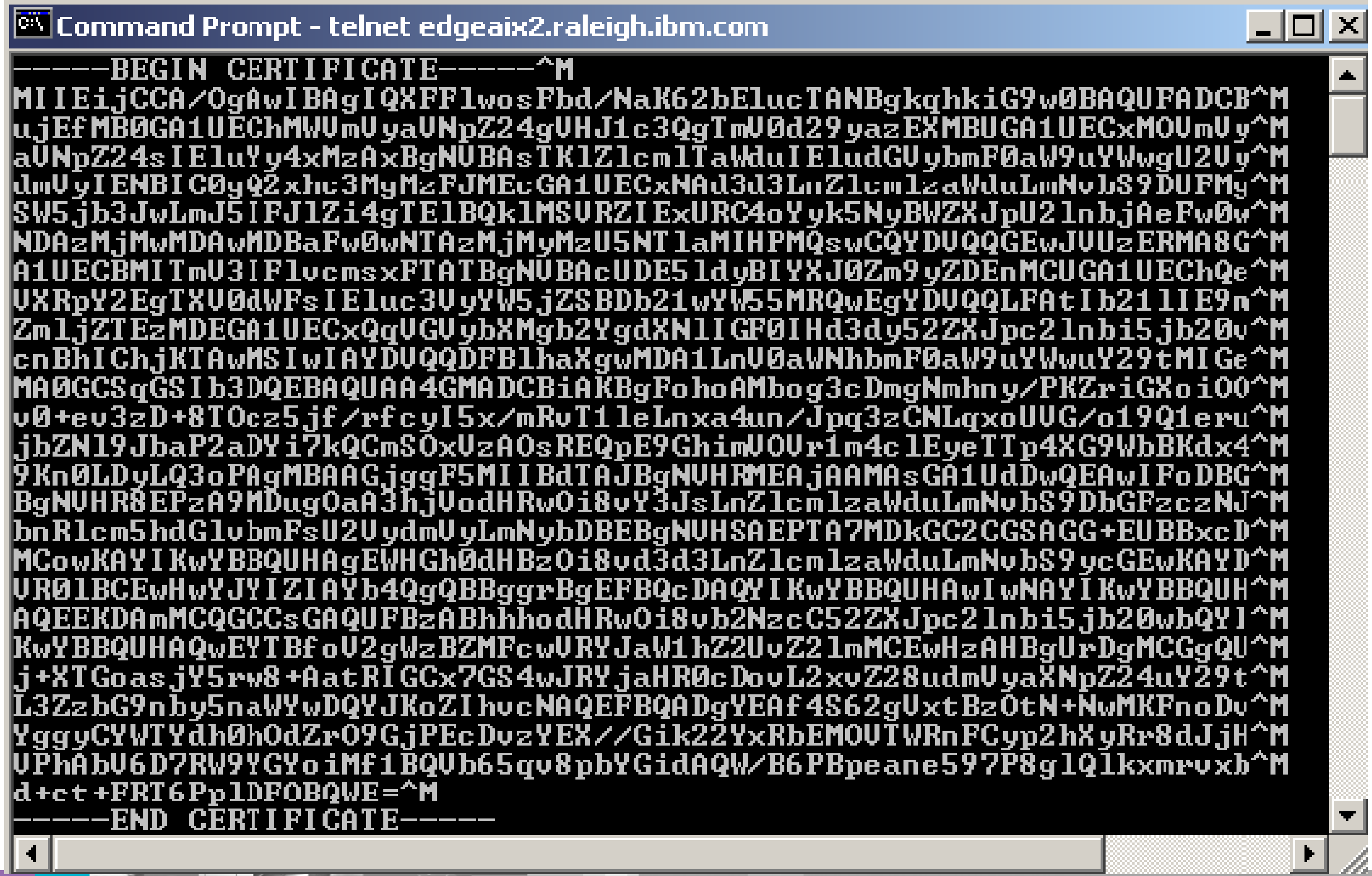
DB-Type: CMS key database file

File Name: C:\CaseStudy\GSKitCaseStudy\verisign\corruptCase\mobiusweb1.kdb

The internal database handle table is corrupted.

The internal database handle table is corrupted.

Corrupted Certificate



```
-----BEGIN CERTIFICATE-----^M
MIIEijCCA/OgAwIBAgIQXFFlwosFbd/NaK62bElucTANBgkqhkiG9w0BAQUFADCB^M
ujEfMB0GA1UEChMWVmVyaVNpZ24gVHJ1c3QgTmV0d29yazEXMBUGA1UECxMOVmVy^M
aVNpZ24sIEluYy4xMzAxBgNVBAsTKlZlcmlTaWduIEludGVybmF0aW9uYWwgU2Vy^M
dmVyIENBIC0yQ2xhc3MyMzFJMEcGA1UECxNAd3d3LnZlcmlzaWduLmNvbS9DUFMy^M
SW5jb3JwLmJ5IFJlZi4gTElBQklMSVRZIExURC4oYyk5NyBWZXJpU2lnbjAeFw0w^M
NDAzMjMwMDAwMDBaFw0wNTAzMjMyMzU5NTlaMIHPMQswCQYDVQQGEwJVUzERMA8G^M
A1UECBMITmV3IFlvcmsxFTATBgNVBAcUDE5ldyBIYXJ0Zm9yZDEnMCUGA1UEChQe^M
UXRpY2EgTXV0dWFsIEluc3VyYW5jZSBDb21wYW55MRQwEgYDVQQLFAtIb21lIE9n^M
ZmljZTEzMDEGA1UECxQqVGVybXMgb2YgdXNlIGF0IHd3dy52ZXJpc2lnbi5jb20v^M
cnBhIChjKTAwMSIwIAYDVQQDFBlhaXgwMDA1LnV0aWNhbmF0aW9uYWwuY29tMIGe^M
MA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgFohoAMbog3cDmgNmhny/PKZriGXoiO0^M
v0+ev3zD+8TOcz5jf/rfcyI5x/mRvT1leLnxa4un/Jpq3zCNLqxoUVG/o19Q1eru^M
jbZNl9JbaP2aDYi7kQCmSOxVzAOsREQpE9GhimVOVr1m4clEyeTTp4XG9WbBKdx4^M
9Kn0LDyLQ3oPAgMBAAGjggF5MIIBdTAJBgNVHRMEAjAAMAsGA1UdDwQEAwIFoDBG^M
BgNVHR8EPzA9MDugOaA3hjVodHRwOi8vY3JsLnZlcmlzaWduLmNvbS9DbGFzczNJ^M
bnRlcm5hdGlvbmFsU2VydmVyLmNybDBEBgNVHSAEPTA7MDkGC2CGSAGG+EUBBxcD^M
MCowKAYIKwYBBQUHAgEWHGh0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9ycGEwKAYD^M
VR01BCEwHwYJYIZIAYb4QgQBBggrBgEFBQcDAQYIKwYBBQUHAwIwNAYIKwYBBQUH^M
AQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC52ZXJpc2lnbi5jb20wbQY]^M
KwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQU^M
j+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29t^M
L3ZzbG9nby5naWYwDQYJKoZIhvcNAQEFBQADgYEAf4S62gVxtBzOtN+NwMKFnoDv^M
YggyCYWTYdh0hOdZrO9GjPEcDvzYEX//Gik22YxRbEMOVTWRnFCyp2hXyRr8dJjH^M
VPhAbV6D7RW9YGYoiMf1BQVb65qv8pbYGidAQW/B6PBpeane597P8glQlkxmrvxb^M
d+ct+FRT6PplDFOBQWE=^M
-----END CERTIFICATE-----
```

No Request Key

- Error message
  "No Request Key was found for Certificate”
- Causes
  - The kdb file is not the original one
  - The request file is deleted
  - The cert is received into the kdb
- http://www.ibm.com/support/docview.wss?uid=swg21138209

Other IKeyman Error Messages

- “GSKKM_ERR_CRYPTOGRAPHIC_TOKEN_NOT_INITIALIZED”
  - http://www-1.ibm.com/support/docview.wss?uid=swg21053361
- Cannot load libikeyman.a
  - export LIBPATH=.:$LIBPATH
  - export PATH=/usr/java131/bin:$PATH
- "The Java Cryptographic Extension(JCE) files were not found. Please check that the JCE files have been installed in the correct directory.”
  - http://www-1.ibm.com/support/docview.wss?uid=swg21166332
- IBM HTTP Server: ikeyman crashes when receiving a personal certificate
  - http://www-1.ibm.com/support/docview.wss?uid=swg21115052
- Configuring SSL and Mustgather for SSL problems:
  - http://www-1.ibm.com/support/docview.wss?uid=swg21179559

Additional WebSphere Product Resources

- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at: www.ibm.com/developerworks/websphere/community/
- Learn about other upcoming webcasts, conferences and events: www.ibm.com/software/websphere/events_1.html
- Join the Global WebSphere User Group Community: www.websphere.org
- Access key product show-me demos and tutorials by visiting IBM Education Assistant: www.ibm.com/software/info/education/assistant
- Learn about the Electronic Service Request (ESR) tool for submitting problems electronically: www.ibm.com/software/support/viewlet/probsub/ESR_Overview_viewlet_swf.html
- Sign up to receive weekly technical My support emails: www.ibm.com/software/support/einfo.html

Questions and Answers