Remote Secure Access of RDC, TMS and OC: The Secrets of SSL and HTTPS configuration in the OPA 4.0 Environment

Sunil G. Singh

Introduction

- Sunil G. Singh of DBMS Consulting, Inc.
- Specialize in Oracle Pharmaceutical and E-Business implementations and long-term support.
- Available for follow-up discussions and questions at Booth 7-8.

Acknowledgements

- Thanks to OCUG for this opportunity to speak.
- Special thanks to my many friends and colleagues at Oracle, Industry and other Vendors for their comments and insights into this topic.

Goals

- Explanation of the needs and issues surrounding security and remote access of RDC, TMS and OC.
- Walk through a HTTPS and SSL configuration of the current OC 4.0.2.16 architecture with secure public access to the 9iAS Apache and Developer 6i Forms Server NT Middle Tier.
- Establish procedure for an https URL that is accessible anywhere that can access a particular RDC, OC and TMS environment.

Scope

- Technical discussion.
- Client access techniques to the Oracle Pharmaceutical Applications only.
- Internal security issues concerning responsibilities or Application Tier to Database Tier security are not covered.

Assumptions

- OC 4.0.2.16 configuration using the latest NT Middle Tier technology stack of 9iAS with Apache and Developer 6i Patchset 8.
- No implementation of servlets.

Overview of https

- Secure version of the standard http protocol because it **uniquely** encrypts traffic between a web client and web server.
- Uses Secure Socket Layers (SSL)
  - Encrypts TCP/IP traffic along a specific port, usually 443
- Requires Public Key and Private Key encryption via certificates with a trusted third party, called a Certifying Authority (CA), e.g., VeriSign.
- Secure standard for all Web transactions involving secure data, credit cards, passwords.

Advantages of https configuration

- Use of a De Facto standard.
- Can be made readily available to low bandwidth dial-up users via any Internet Service Provider (ISP).
- SSL is a well-known protocol
  - Extremely well-supported

The need for Secure Remote access with SSL for OPA

- ”Instant Anywhere Access”, the ability to access a specific Oracle Pharmaceutical environment from any web client.
- EDC/RDC may allow companies to have public internet access to internal servers running OC (eventually)
  - Small Pharmaceuticals and Biotechs could distribute trials and research very effectively in "virtual offices.”

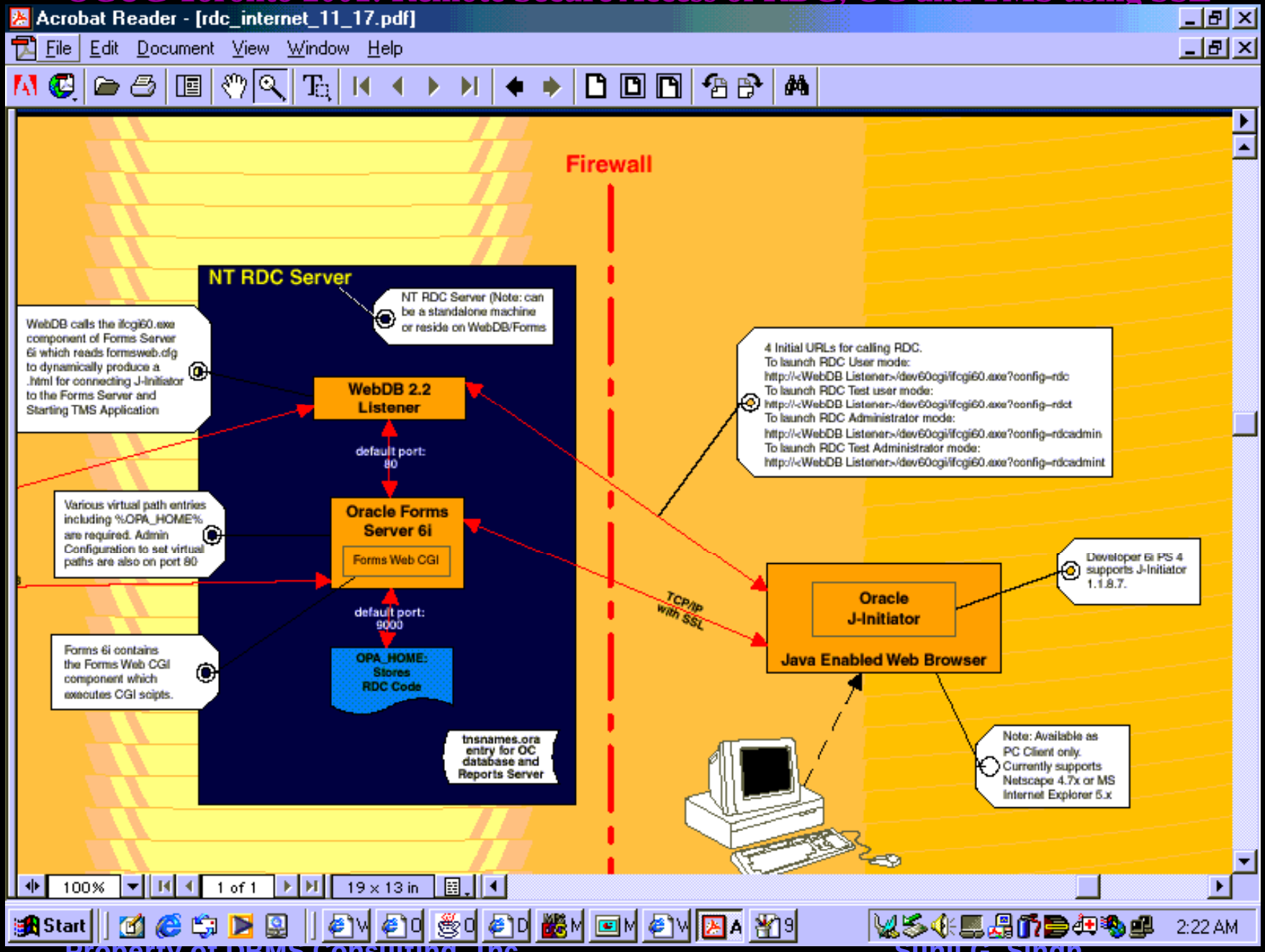
Needs for Secure Remote access with SSL (2)

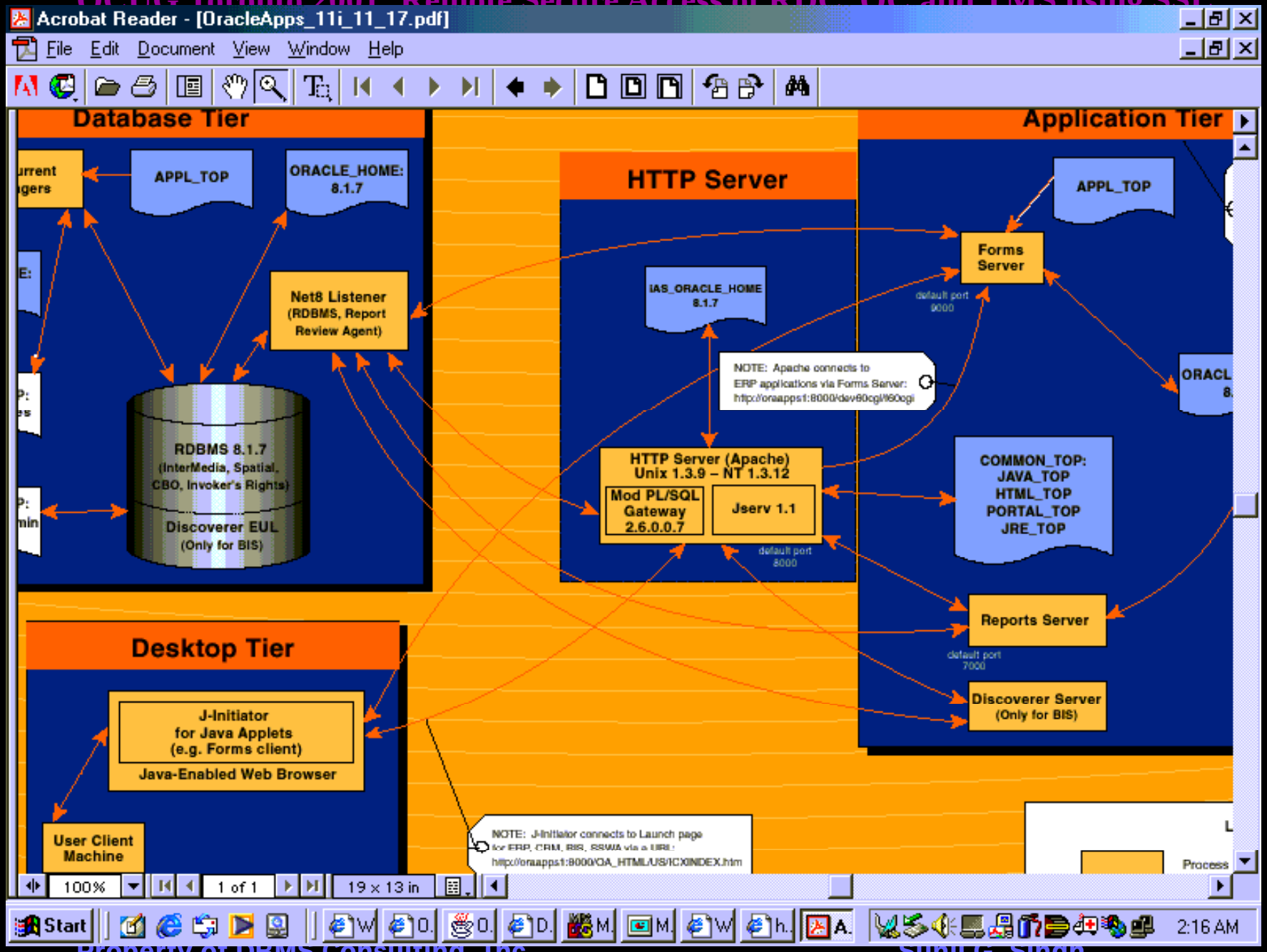
- Requires a level of security where any remote machine can securely access a database server
  - Similar to eBAY and amazon.com
- In the future, perhaps CROs could access OC and TMS in the same way.

Current Architecture of NT Middle Tier

- Recently changed with patchset 4.0.2.16, which requires an NT server rebuild and introduces:
  - 9iAS
  - Developer 6i Patchset 8

OCUG Toronto 2001: Remote Secure Access of RDC, OC and TMS using SSL




Acrobat Reader - [OracleApps_11i_11_17.pdf]
File Edit Document View Window Help
Database Tier
APPL_TOP
ORACLE_HOME: 8.1.7
Net8 Listener (RDBMS, Report Review Agent)
RDBMS 8.1.7 (InterMedia, Spatial, CBO, Invoker's Rights)
Discoverer EUL (Only for BIS)
HTTP Server
IAS_ORACLE_HOME 8.1.7
NOTE: Apache connects to ERP applications via Forms Server: http://onaapps1:8000/dev60cgi/f60cgi
HTTP Server (Apache) Unix 1.3.9 – NT 1.3.12
Mod PL/SQL Gateway 2.6.0.0.7
Jserv 1.1
default port 8000
Application Tier
APPL_TOP
Forms Server
default port 9000
COMMON_TOP: JAVA_TOP HTML_TOP PORTAL_TOP JRE_TOP
Reports Server
default port 7000
Discoverer Server (Only for BIS)
Desktop Tier
J-Initiator for Java Applets (e.g. Forms client)
Java-Enabled Web Browser
User Client Machine
NOTE: J-Initiator connects to Launch page for ERP, CRM, BIS, SSWA via a URL: http://onaapps1:8000/OA_HTML/US/ICXINDEX.htm
100%
1 of 1
19 x 13 in
Start
2:16 AM

How do SSL and https work ?

- Browser approaches a website requesting a secure connection via an https URL
- The webserver sends a Digital Certificate to the client.

How do SSL and https work ? (2)

- Digital Certificate contains
  - The websites company's name and address, and the intended server for the URL to use. This is what makes each certificate UNIQUE and provides the verifiable data to test the encryption keys.
  - Public key from the Web Server

How do SSL and https work ? (3)

- Digital signature of the Certifying Authority (such as Verisign). This would be like a person's signature used to verify whether or not the Digital Certificate is authentic or possibly a fake.
- Test messages and an encrypted form of the algorithms used by the Public and Private Keys to encrypt messages.

How do SSL and https work ? (4)

- The client the performs some tests with the information in the Digital Certficate to:
  - Verify that the Web Server has the correct Private Key
  - Verify that the Digital Certificate was generated by the Certifying Authority and is not a forgery.

How do SSL and https work ? (5)

- Once client verifies the Digital Certificate
  - Encrypted connection between the Web Server and the client is established using a mathematical algorithm based on the Public and Private Keys.
- This encrypted connection is the Secure Socket Layer

Digital Certificates are Important !

- Setting up the remote secure access for OC/TMS/RDC depends on the these magical digital certificates.
- But these Certificates have to be applied for from the Certifying Authority.
  - These certificates must be unique.
  - The Certifying Authority charges for these Digital Certificates. Verisign charges a mininum of $349 for a small site, and thousands of dollars for larger sites.

How do I apply for my Digital Certificate ?

- Every piece of Web software has some type of utility that allows the creation of a Certificate Signing Request (CSR)
- This CSR must be sent to the Certifying Authority, such as Verisign.
- After paying for the certificate and verifying some things about the requesting company, the Certifying Authority sends a genuine certificate back.
- A trial certificate is usually issued in the interim time period for testing.

Two paths to access OC, TMS and RDC on a network.

- Usually, Forms are accessed via a Forms Server.
- In a few cases, there access via Java and PL/SQL Cartridge object not requiring a Forms Server, e.g.
  - TMS Light Dictionary Browser
  - TMS Web Search Engine

Two Paths Require Two Sets of Security

- Implies a need for two separate sets of authentication certificates
  - Secure access to 9iAS Apache
  - Secure access to the Forms Server

Setting up an SSL environment for RDC, OC and TMS

- Dedicate an NT server for external communication, could be a machine dedicated for RDC.
- Create firewall mappings for NT server through the corporate/enterprise firewall
- Generate a private key on NT for Apache
- Apply for a certificate for Apache using openSSL utility

Setting up an SSL environment for RDC, OC and TMS (2)

- Install genuine certificate from the Certifying Authority into Apache configuration
- Generate a private key and apply for a certificate for the Forms Server using Oracle Wallet Manager

Setting up an SSL environment for RDC, OC and TMS (3)

- Install the genuine certificate from the Certifying Authority into Wallet Manager
- Distribute appropriate certification file for J-Initiator (trial keys only) to client machines.

Firewall mapping to the NT

- Ports 80, 443 and 9000 (by default) opened on the NT Server through firewall
- Pass through mapping with external IP address can be used

Firewall mapping to the NT (2)

- Some network administrators might want to change the external port mapping
  - External URL may not use the same ports as the NT Server uses internally.
- An external DNS alias is required for the external IP address that will be publicly accessible. This is a requirement for the Digital Certificate.

Create a key on NT for Apache

- Create a random file:
  - d:\oracle\isuites\apache\open_ssl\bin\openssl rand -out random_file_for_apache_key.txt 1000 -base64
  - Successful output:
    - Loading 'screen' into random state - done

Create a key on NT for Apache (2)

- Use the random file in the key creation
  - set RANDFILE=random_file_for_apache_key.txt
  - d:\oracle\isuites\apache\open_ssl\bin\openssl genrsa -des3 -out apache_1024.key 1024
    - Successful output:
    - Loading 'screen' into random state - done
    - Generating RSA private key, 1024 bit long modulus

Create a key on NT for Apache (3)

- OpenSSL will then prompt:
  - Enter PEM pass phrase
- Enter some temporary password.
- This is a password that should be entered every time the Apache Webserver is started in HTTPS mode. On UNIX, this is additional security measure since a privileged user starts the Apache daemon. However, NT can not support this feature, since it can not respond to a password prompt when starting a service, and it has to be disabled.

Create a key on NT for Apache (4)

- Stop Apache from prompting for PEM Pass phrase every time it starts by storing the PEM Pass Phrase in the key file:
  - Rename the existing apache_1024.key file.
  - d:\oracle\isuites\apache\open_ssl\bin\openssl rsa -in apache_1024.key.tmp -out apache_1024.key
    - Re-enter the PEM Pass Phrase

Apply for a certificate for Apache on NT using openSSL

- Set the environment variables
  - set OPENSSL_CONF=D:\oracle\isuites\apache\open_ssl\bin\openssl.cnf
- Run the openSSL utility with req option
  - d:\oracle\isuites\apache\open_ssl\bin\openssl req -new -key apache_1024.key -out apache_1024.csr

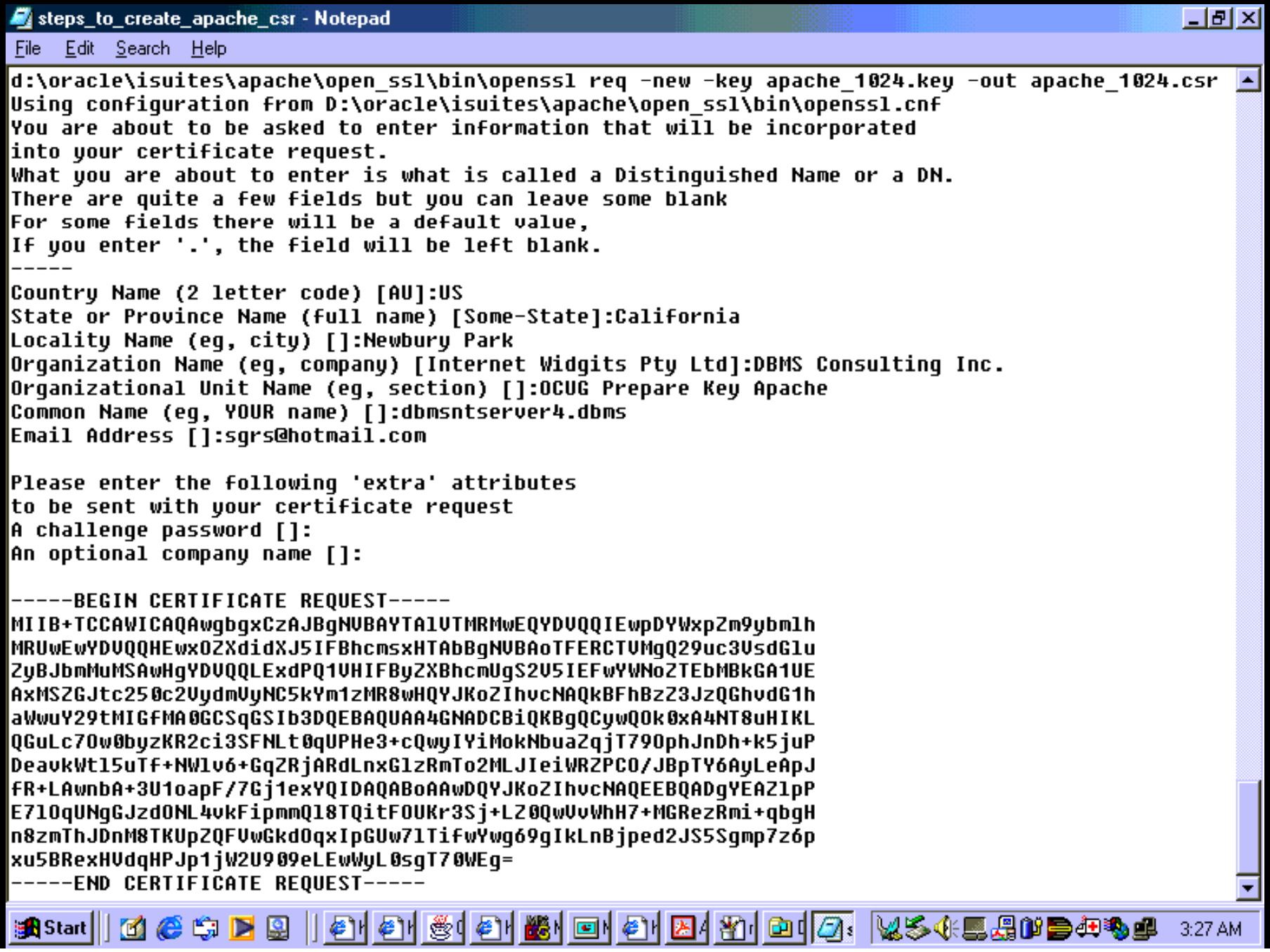
Apply for a certificate for Apache on NT using openSSL (2)

- Answer prompts for Company name and Address, and common name
- Common name MUST BE name of the server that will be used in the URL to connect to this site externally.

Apply for a certificate for Apache on NT using openSSL (3)

- During CSR request phase, do NOT:
  - Use commas
  - Use Short State names, such as CA for California
  - Use a different name for the common name other than the external name of the NT Server.

OCUG Toronto 2001: Remote Secure Access of RDC, OC and TMS using SSL



Apply for a Trial Certificate on Certifying Authority Website

- Verisign's website has a 5 step process for applying for a certificate.
- A trial certificate can be obtained within 1 hour, but a paid certificate requires much more information and can take almost 1 week.
- The trial certificate usually lasts for 14 days.

Apply for a Trial Certificate on Certifying Authority Website (2)

- Step 3 of the Verisign process will require the contents of the CSR.
- Cut and paste the section from
  - `-----BEGIN CERTIFICATE REQUEST-----`
  - `-----END CERTIFICATE REQUEST-----`
- Verisign then sends an e-mail back with the trial (or genuine) certificate information, also surrounded by:
  - `-----BEGIN CERTIFICATE REQUEST-----`
  - `-----END CERTIFICATE REQUEST-----`

Configure Apache to use SSL and the Digital Certificate

- Save the BEGIN-END certificate request file into the same directory where the apache_1024.key file was stored. Name this file apache_1024.crt
  - One convention is to create a D:\ORACLE\iSuites\admin\certs\apache directory.
- On NT, everything is configured from the http.conf file, which is by default in
  - d:\oracle\iSuites\Apache\Apache\conf

Configure Apache to use SSL and the Digital Certificate (2)

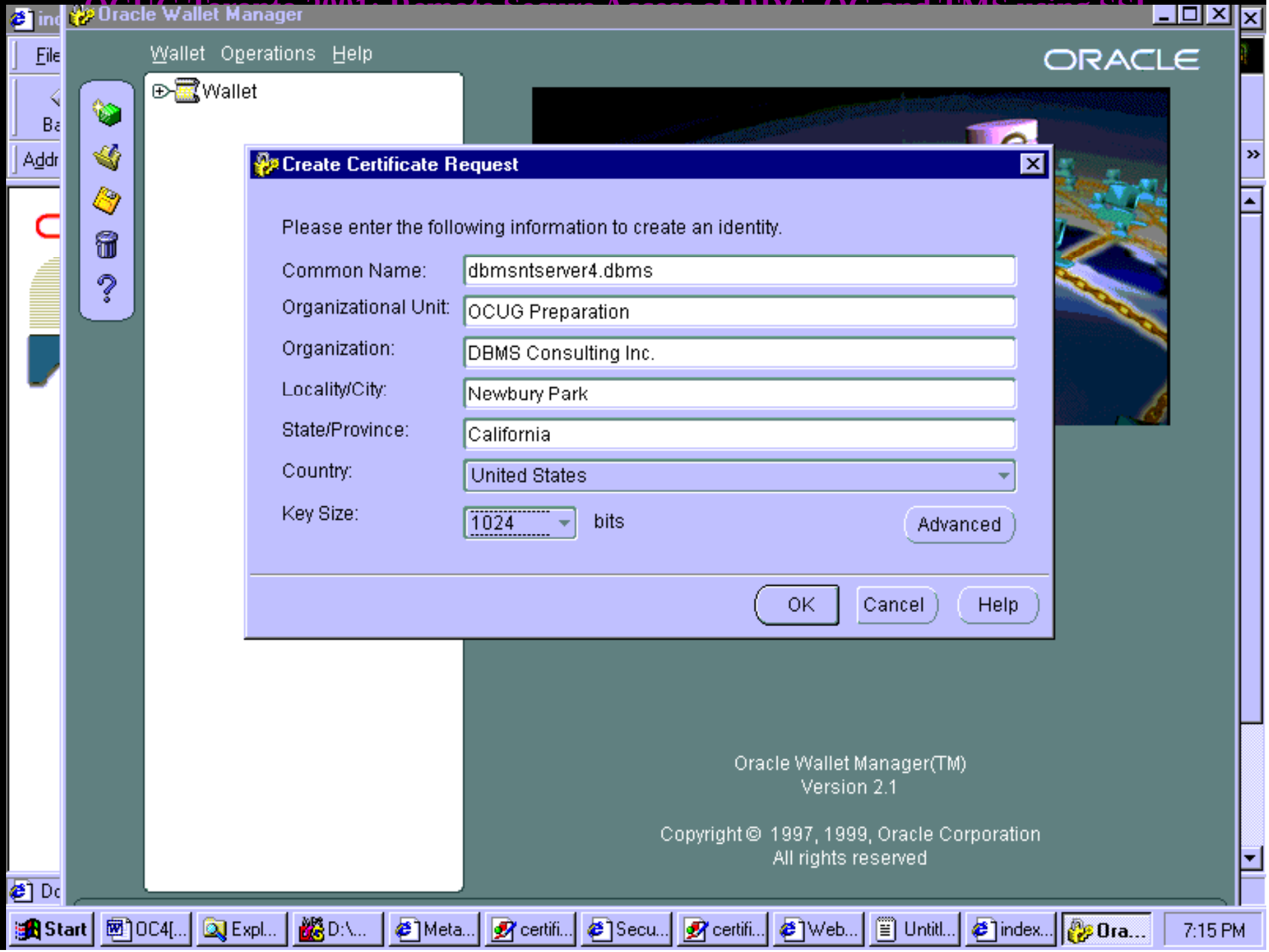
- In the httpd.conf file, edit the following lines.
  - SSLCertificateFile D:\ORACLE\iSuites\admin\certs\apache\apache_1024.crt
  - SSLCertificateKeyFile D:\ORACLE\iSuites\admin\certs\apache\apache_1024.key
  - Check the <IfDefine SSL> section, ensure that port 443 is present
  - Check that the line <VirtualHost _default_:443> is enabled.
- Restart the Apache NT Service

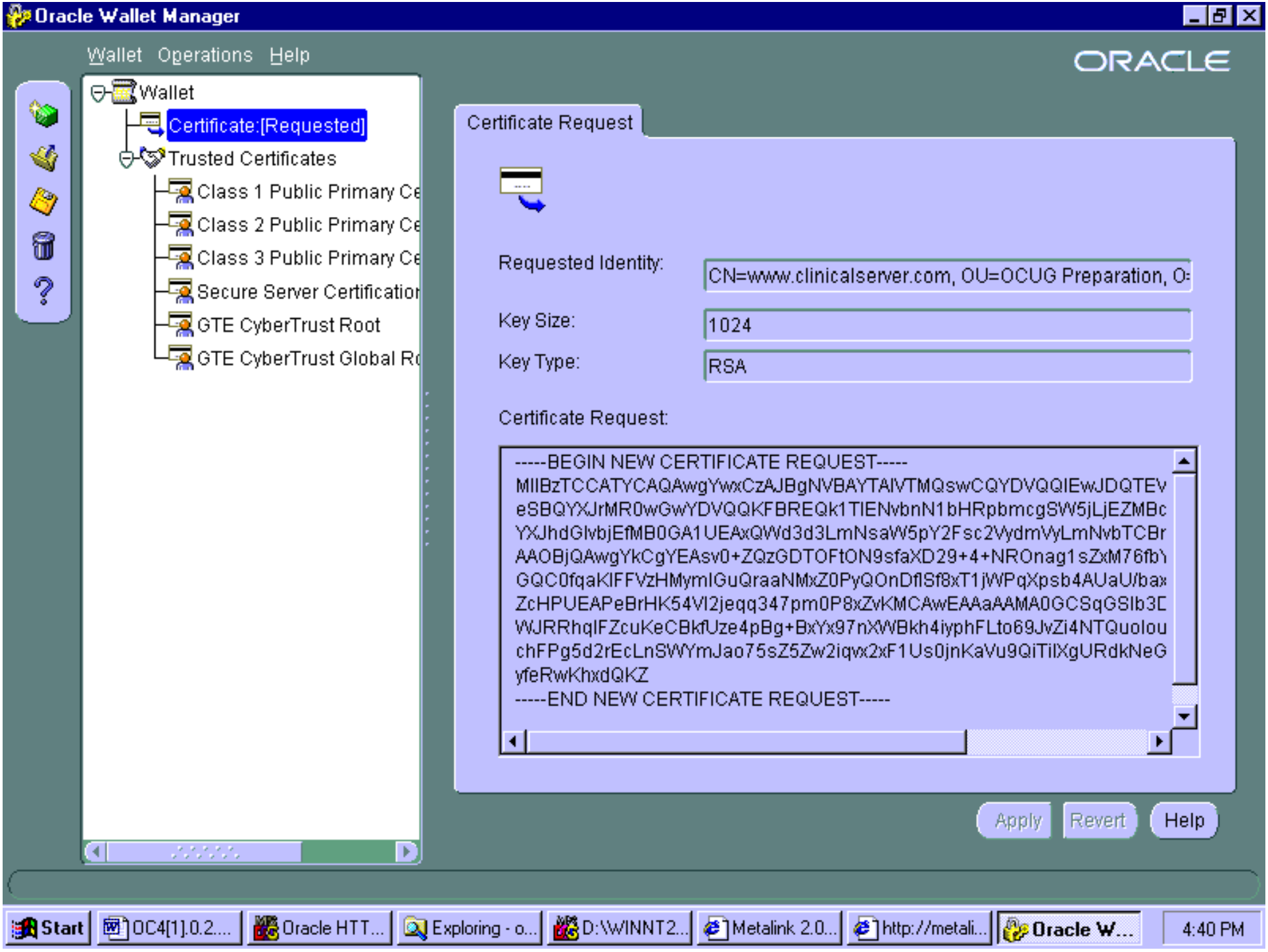
Generate CSR and Keys using the Oracle Wallet Manager

- Wallet Manager is a utility to generate Certificate Signing Requests (CSR) for Oracle Forms and Developer 6i Tools.
- It creates keys and receives certificates from CAs, such as Verisign.
- Wallet Manager creates Keys and CSRs at the same time.

Generate CSR and Keys using the Oracle Wallet Manager (2)

- During CSR request phase, do NOT:
  - Use commas
  - Use Short State names, such as CA for California
  - Use a different name for the common name other than the external name of the NT Server.


Oracle Wallet Manager
Wallet Operations Help
ORACLE
Wallet
Create Certificate Request
Please enter the following information to create an identity.
Common Name: dbmsntserver4.dbms
Organizational Unit: OCUG Preparation
Organization: DBMS Consulting Inc.
Locality/City: Newbury Park
State/Province: California
Country: United States
Key Size: 1024 bits
Advanced
OK
Cancel
Help
Oracle Wallet Manager(TM)
Version 2.1
Copyright © 1997, 1999, Oracle Corporation
All rights reserved
Start
7:15 PM


Oracle Wallet Manager
Wallet Operations Help
ORACLE
Wallet
Certificate:[Requested]
Trusted Certificates
Class 1 Public Primary Ce
Class 2 Public Primary Ce
Class 3 Public Primary Ce
Secure Server Certificatior
GTE CyberTrust Root
GTE CyberTrust Global Rc
Certificate Request
Requested Identity:
CN=www.clinicalserver.com, OU=OCUG Preparation, O=
Key Size:
1024
Key Type:
RSA
Certificate Request:
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBzTCCATYCAQAwgYwxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEV
eSBQYXJrMR0wGwYDVQQKFBREQk1TIENvbnN1bHRpbmcgSW5jLjEZMBc
YXJhdGlvbjEfMB0GA1UEAxQWd3d3LmNsaW5pY2Fsc2VydmVyLmNvbTCBr
AAOBjQAwgYkCgYEAsv0+ZQzGDTOFtON9sfaXD29+4+NROnag1sZxM76fb\
GQC0fqaKIFFVzHMymIGuQraaNMxZ0PyQOnDflSf8xT1jWPqXpsb4AUaU/ba
ZcHPUEAPeBrHK54Vl2jeqq347pm0P8xZvKMCAwEAAaAAMA0GCSqGSIb3D
WJRRhqIFZcuKeCBkfUze4pBg+BxYx97nXWBkh4iyphFLto69JvZi4NTQuolou
chFPg5d2rEcLnSWYmJao75sZ5Zw2iqvx2xF1Us0jnKaVu9QiTilXgURdkNeG
yfeRwKhxdQKZ
-----END NEW CERTIFICATE REQUEST-----
Apply
Revert
Help
Start
OC4[1].0.2....
Oracle HTT...
Exploring - o...
D:\WINNT2...
Metalink 2.0...
http://metali...
Oracle W...
4:40 PM

Apply for a certificate for Oracle Forms

- Recall that the two separate certificates are required, one for Apache, and one for Oracle Forms
  - Repeat the same process as for Apache to request a Trial Certificate, including Step 3 on Verisign's site where the BEGIN-END Certificate Request block from Wallet Manager needs to be pasted into Verisign's website.
  - The information on the CSR must be unique, this is usually done by Organizational Unit.
- Verisign will send an e-mail back with the Trial certificate.

Import the Digital Certificate into Wallet Manager

- Wallet Manager has a menu option to import the certificate, under Options -> Import User Certificate.
- However, it will not recognize that Verisign is a Trusted Certifying Authority by default for Trial Certificates.

Import the Digital Certificate into Wallet Manager (2)

- Verisign has a Certificate that must be imported into Wallet Manager to solve this problem.
- However, the format of this certificate can not be read by Wallet Manager, therefore the certificate has to be imported into Internet Explorer, then exported to the format that Wallet Manager can import.

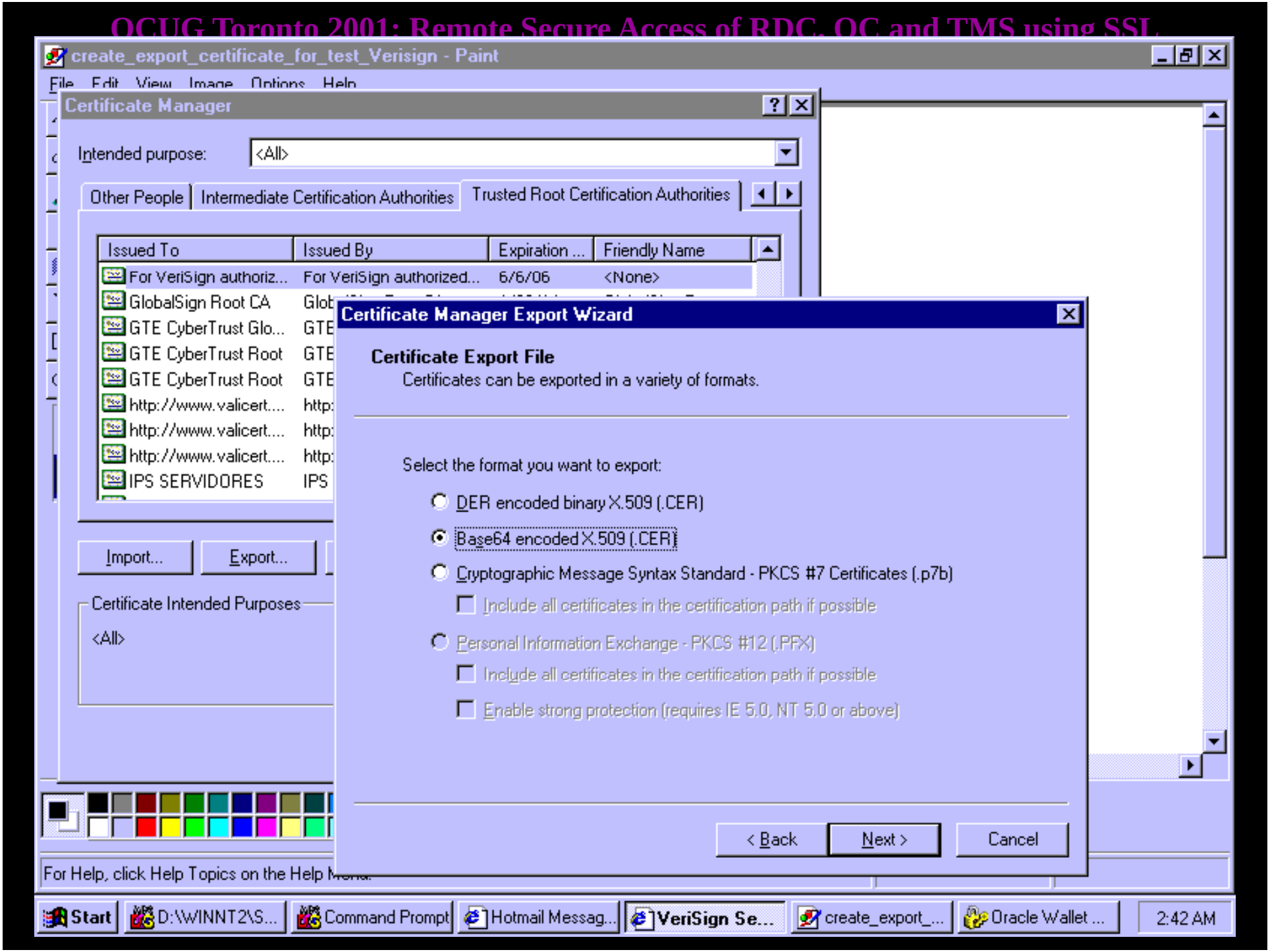
Import the Digital Certificate into Wallet Manager (3)

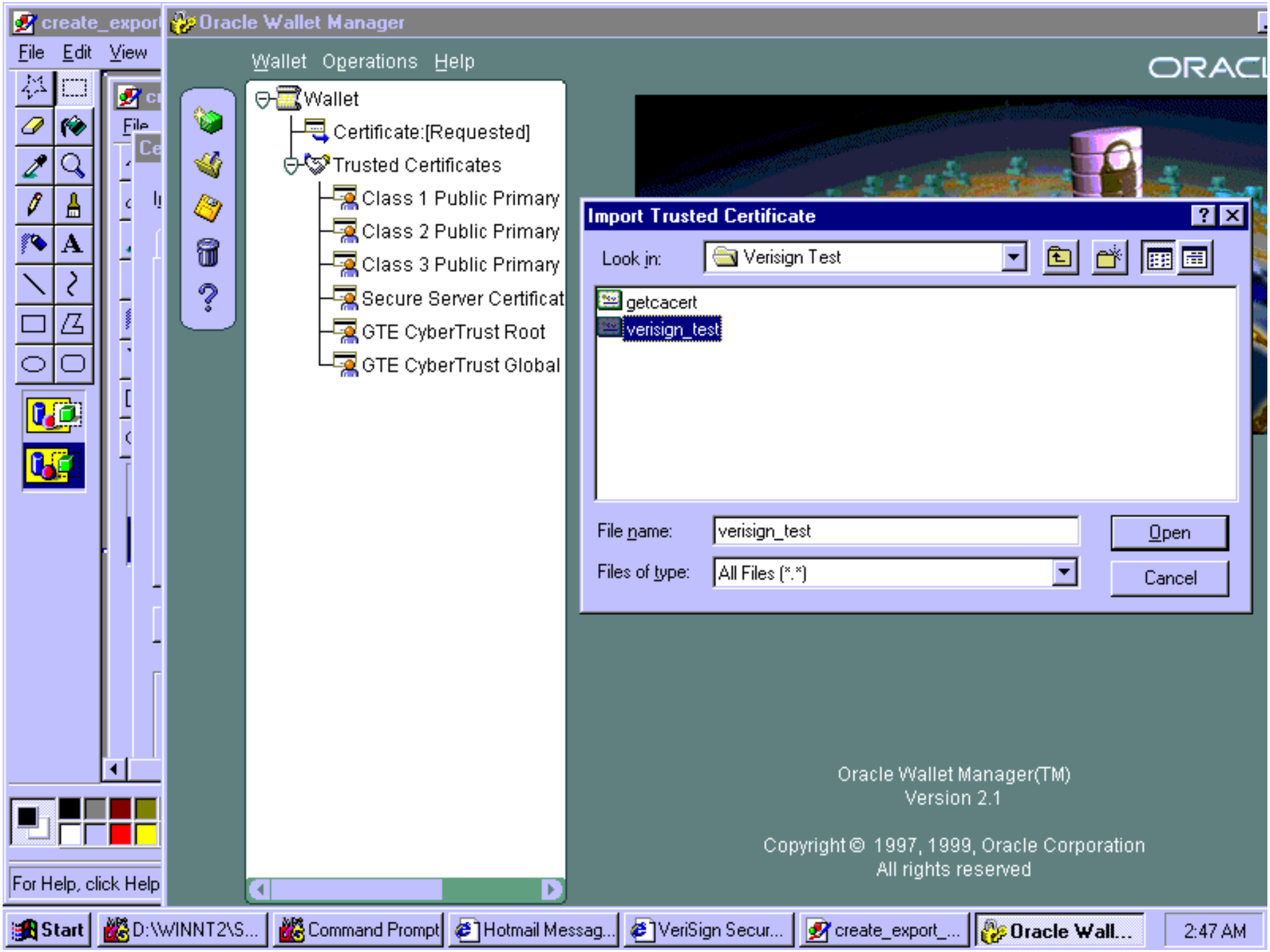
- On Verisign's website, there is a link that can store the Trial Certificate for Verisign as a Certifying Authority into Internet Explorer.
- Once this is stored in IE, it can be exported to a file that can be read by Wallet Manager

Import the Digital Certificate into Wallet Manager (4)

- Wallet Manager has a menu option to import Trusted Certificates from Certifying Authorities, under Options -> Import Trusted Certificate
- Complete this step before attempting Options -> Import User Certificate for the Trial Certificate returned from Verisign.

OCUG Toronto 2001: Remote Secure Access of RDC, OC and TMS using SSL




create_expor
File Edit View
Oracle Wallet Manager
Wallet Operations Help
Wallet
Certificate:[Requested]
Trusted Certificates
Class 1 Public Primary
Class 2 Public Primary
Class 3 Public Primary
Secure Server Certificat
GTE CyberTrust Root
GTE CyberTrust Global
Import Trusted Certificate
Look in:
Verisign Test
getcacert
verisign_test
File name:
verisign_test
Open
Files of type:
All Files (*.*)
Cancel
Oracle Wallet Manager(TM)
Version 2.1
Copyright © 1997, 1999, Oracle Corporation
All rights reserved
For Help, click Help
Start
D:\WINNT2\S...
Command Prompt
Hotmail Messag...
VeriSign Secur...
create_export_...
Oracle Wall...
2:47 AM

Configure Forms to use HTTPS

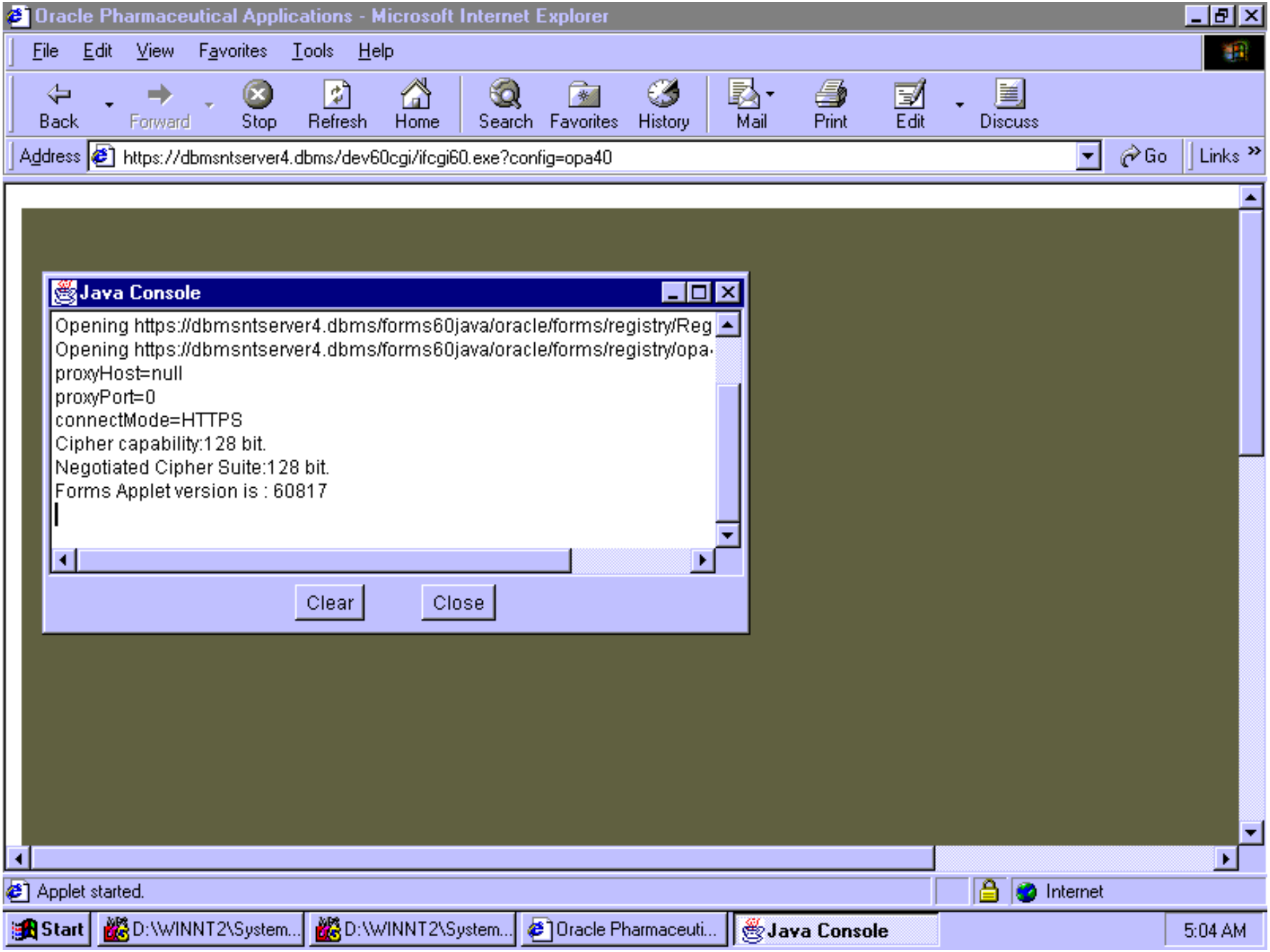
- Set the following Registry Keys:
  - FORMS60_WALLET=<Directory where wallet was created on NT Server>
  - FORMS60_HTTPS_NEGOTIATE_DOWN=TRUE
- Edit the formsweb.cfg file:
  - Set the connect mode to HTTPS instead of HTTP.
- Restart the Forms Server Service

Update the J-Initiator client to use Trial Digital Certificates.

- On Each client machine, edit the file:
  - `C:\Program Files\Oracle\JInitiator 1.1.8.16\lib\security\certdb.txt`
- Add the BEGIN-END Certificate block from the Certifying Authority e-mail to each J-Initiator client connecting to this NT Forms Server.

SSL connection can be established

- Should be able to navigate to the calling URL for OC/TMS/RDC using HTTPS instead of HTTP.
- Turning on the Java Console will show the Forms Connection is indeed HTTP.


Oracle Pharmaceutical Applications - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address https://dbmsntserver4.dbms/dev60cgi/ifcgi60.exe?config=opa40
Go Links
Java Console
Opening https://dbmsntserver4.dbms/forms60java/oracle/forms/registry/Reg
Opening https://dbmsntserver4.dbms/forms60java/oracle/forms/registry/opa
proxyHost=null
proxyPort=0
connectMode=HTTPS
Cipher capability:128 bit.
Negotiated Cipher Suite:128 bit.
Forms Applet version is : 60817
Clear
Close
Applet started.
Internet
Start
D:\WINNT2\System...
D:\WINNT2\System...
Oracle Pharmaceuti...
Java Console
5:04 AM

Conclusions

- HTTPS and SSL can be established for the 9iAS Apache and Developer 6i Forms Server architecture.
- Intricate setup process and requires maintenance of two sets of Digital Certificates

Other Useful Sources

- Oracle Applications Performance Tuning Handbook by Andy Tremayne
- Metalink (Article 123718.1)

Q&A ?

- Please visit us at Booth 7 & 8 for
  - more detailed description of SSL Configuration
  - Wireless Demo OC and RDC with a Compaq IPAC
  - Demo Auto-generated WinRunner-based execution of an OC 4.0 test suite
- Free Laser Pointer and OC 4.0.2 and TMS 4.0.3 Architecture poster