Implementing https/SSL with the Oracle Pharmaceutical Applications 4.5

Presented by Sunil G. Singh of DBMS Consulting.

Acknowledgements

- Thanks to the OCUG and Administration and Configuration Management Focus Group for this opportunity to present this topic
- Thanks to Andy Alasso and the participants of the RDC Early Adopters’ Group which covered some of this material in the meeting of 6-APR-2004
- Many thanks to the OCUG Presentation committee, Bob Belousek, Bryan Judge, Stephan Clover and Lori Venable for their patience with the completion of these presentations.

Goals

- Follow-up from the first part version of this presentation given in January 2002.
- Discuss two methods of https/SSL access to OPA 4.5
  - https/SSL configuration of the 9iAS Middle Tier
  - Public facing SSL Accelerators and network devices using reverse proxy
- Discussion of multiple Middle Tier server configuration for external requests

Scope and Assumptions

- Technical perspective and overview.
- Client access techniques to the OPA only.
- Assume that there is current running OPA 4.5 environment with 9iAS Windows 2K Middle Tiers Assumptions
- Assume there is some type of connectivity infrastructure from this environment to the public internet

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

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 then 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

https/SSL Access in the OPA 4.5 Installed Base

- In the presentation given in Toronto at OCUG 2001 in January of 2002, there were very few companies that had tested or were implementing public-facing https/SSL access to their OPA environment.
- However, it is clear from that time to the present that many OPA customers are implementing this type of deployment for a variety of reasons.
  - Remote Data Capture deployments by large OPA customers to many sites is demanding a near-seamless but secure way to access a central environment, without requiring additional network or server hardware at the site.

https/SSL Access in the OPA 4.5 Installed Base (2)

- Multiple CROs can work with large sponsor companies with reduced costs and increased connectivity to the sponsor's central OPA environment, and can also attract new sponsors by demonstrating internal expertise in the administration and deployment of OPA
- Application Outsourcing and Support providers for OPA can co-locate or host smaller OPA customers' environments
- https/SSL has become even more accepted for critical transactions, such as on-line banking, adding credibility to the concepts of secure remote access of critical data.

Major options for Public-facing https/SSL access

- Option 1: Use an OPA Middle Tier as a public facing https/SSL server
- Option 2: Use of separate SSL Hardware Accelerators with integrated network devices
- Virtual Private Networks (VPNs) are common, but usually require a separate client or account or code to be accessible. In this respect, they are more secure, but not truly publicly accessible
- Today, the trend is clearly toward option 2. However, Option 1 is still viable and is generally less expensive than Option 1.

Option 1: OPA Middle Tier as a public facing https/SSL server

- Amazingly, the configuration of the Windows Middle Tier is very similar to the configuration options available in Jan 2002:
  - Windows 2000 Server SP 4
  - 9iAS 1.0.2.2.2a with Apache 1.3.19 pre-bundled
  - Forms 6i Patchset 14 and Reports 9i
  - Java Servlets
  - OC4J
- The crucial part of the external connectivity is exactly the same: 9iAS and Apache
- Additionally, the Forms Server is gone, and this has a major benefit in the https/SSL configuration

Option 1: Only one SSL Certificate Required for Apache

- Previously, the Forms Server SSL Certificate and the Apache SSL Certificate were incompatible. This meant configuration of two Digital Certificate to access pre-OPA 4.5 versions.
- Now, there is no more Forms Server Service, and all traffic goes through Apache.
- Additionally, the version of Apache is **exactly the same** as it was over 2 years ago. So the same steps for Apache only are necessary!

Option 1: High-Level steps Apache https/SSL configuration

- Dedicate a Windows 2000 server for external public access, this could be a machine dedicated for RDC.
- Create firewall mappings for Windows 2000 server through the corporate/enterprise firewall
  - Only port 443 (by default) is required
- Generate a private key on Windows 2000 for Apache
  - Create a 1024 character Random File
  - Create a key using openssl with the genrsa option
- Apply for a certificate for Apache using openSSL utility
  - Generate a CSR (Certificate Signing Request)
  - Use the public name of the Windows 2K Middle server (public DNS Name)

Option 1: High-Level steps Apache https/SSL configuration (2)

- Send CSR to the Certifying Authority (CA)
  - Usually uploaded to the CA’s website or sent via e-mail
- Receive genuine certificate from the CA
  - Usually received via e-mail from the CA
- Install genuine certificate from the Certifying Authority into Apache configuration
  - Modification of httpd.conf to enable SSL parameters and to refer to the location of the genuine certificate file
- I will not review the exact details as they are located in my original presentation and later appeared on Metalink (Doc ID: 274358.1)

Option 2: Using a Separate Network Device/SSL Accelerator

- Recall that the entire principle of SSL communication is based on encryption.
- In order to encrypt data, it is necessary to perform complex mathematical calculations, usually involving matrix arithmetic and matrix reductions/inversions
- These mathematical computations are CPU intensive
- The concept here is that an OPA Server should be dedicated to running OPA, not running these computations required for SSL encryption
- Many hardware vendors now exist which provide a dedicated hardware device to perform these encryption algorithms
- These hardware devices are usually integrated into some type of firewall or network hardware component

Option 2: Some vendors of SSL Accelerators

- Several vendors exist which provide SSL Hardware accelerator, such as:
  - nCipher - AEP
  - Rainbow - F5
  - Symantem - Cisco
  - IBM
- Most of these devices are bundled together with a firewall and proxy, and have their own IP address.
- All SSL Accelerators which are integrated with a firewall and proxy are considered to be reverse proxy servers. By definition a reverse proxy server is one which is a single point of contact for an external network, which sits in front of other application or web servers protected from the external network.

Option 2: Installing a Digital Certificate on SSL Accelerator

- The high-level steps for requesting and installing a Digital Certificate on any of these hardware SSL Accelerator devices is, in principle, the same as the process for requesting and installing the Digital Certificate for the Apache server on the Win2K Middle Tier
- Generate a private key
- Apply for a certificate
  - Generate a CSR (Certificate Signing Request)
  - Use the public name of the SSL Accelerator (network device) server (public DNS Name)

Option 2: Installing a Digital Certificate SSL Accelerator (2)

- Send CSR to the Certifying Authority (CA)
  - Usually uploaded to the CA's website or sent via e-mail
- Receive genuine certificate from the CA
  - Usually received via e-mail from the CA
- Install genuine certificate from the Certifying Authority into SSL Accelerator's configuration files

Option 2: Understanding the importance of Public DNS Names

- This type of configuration introduces a problem that did not necessarily exist in the public facing middle tier scenario, Option 1.
- When the public facing middle tier requested a certificate via its CSR, it used its own public DNS name. In other words, that Windows Middle Tier was assigned a name and an IP address which was known to the entire Internet.

Option 2: Understanding the importance Public DNS Names (2)

- However, with a hardware accelerator and integrated firewall and proxy server, this is no longer true. This hardware device will contain the Digital Certificate and also be public facing. This hardware device will be associated with a Public DNS Name and a Public IP address that will be known to the entire Internet.
- The W2K Middle Tiers should be protected and their names and IP addresses should not be known to the outside (Internet) world.
- But at installation time, the 9iAS Software and the OPA 4.5 code on the W2K Middle Tier only know the W2K server’s name, and not the public DNS name. So how can connectivity be established?

Generating URLs from OPA to use the external DNS Name

- Set the following Registry keys to use the <Public_DNS_Server_name.Domain>
  - HKEY_LOCAL_MACHINE->SOFTWARE->ORACLE->OPA_LOCALHOST
  - HKEY_LOCAL_MACHINE->SOFTWARE->ORACLE->OPA_SERVER

Generating URLs from OPA to use the external DNS Name (2)

- Change the following Registry Keys to use the URLs of the form https://<Public_DNS_Server_Name.Domain>, replacing the existing http://<Middle_Tier_Server.Domain> part:
  - OPA_DOC_DIR
  - OPA_CUSTOM_DOC_DIR
  - OPA_RQM_URL
  - OPA_XMLTEMP_HTTP
    - Each of these Registry keys has some additional components which must remain intact. OPA_XMLTEMP_HTTP is absolutely required for RDC 4.5 PDF Mode to work.

Options 1 and 2: Generate all URL requests with https

- In addition to getting the URLs generated with the Public DNS Server name so that the requests from the external OPA client can be routed to either a SSL hardware accelerator or a public-facing middle tier, they must also **all start with https** for a truly secure environment.
- In other words, **the external or public facing SSL Accelerator device must *not* and should *not* accept any http:// URLs, but only https:// URLs.**

Options 1 and 2: Generate all URL requests with https (2)

- Change the Registry Keys:
  - HKEY_LOCAL_MACHINE->SOFTWARE->ORACLE->OPA_HTTPS_ENABLED to 1
  - HKEY_LOCAL_MACHINE->SOFTWARE->ORACLE->OPA_PORT to 443 (the default value for SSL connections)
    - If the SSL Accelerator is integrated with a firewall and proxy server, and a different port has been chosen as the listening port for SSL connections, **use this port number instead**.
    - If the SSL Accelerator has been configured to use https/SSL for external connections, but then re-route connections to port 80 on the existing Middle Tiers, **this port number must still be changed!**

Options 1 and 2: Generate all URL requests with https (3)

- Modify the formsweb.cfg file in the %ORACLE_806_HOME%\forms60\server path on the Middle Tier to use
  - connectMode = https (from http originally)
  - serverHost = <Public_DNS_Server_name.Domain> from <Middle_Tier_Name.Domain>
- Modify the opa45_basejini.htm in the %OPA_HOME%\html path on the Middle Tier to use:
  - "java_progressimage" from http://<Middle_Tier>/ to https://<Public_DNS_Name>/ with the remaining part intact. Note there are two occurrences of this parameter. This is the parameter which displays the icon when a new f60jinit_all.jar file must be downloaded when connecting to a new OPA 4.5 site.

Options 1 and 2: Generate all URL requests with https (4)

- %OPA_HOME%\j2ee\home\applications\opardc\opardcweb\WEB-INF\web.xml
  - Change OPA_DOC_DIR from http://<Middle_Tier.Domain>/ to https://<Public_DNS_Server_Name>/

Option 1: Change the OPA Specific httpd.conf files

- Change the opa45_httpd.conf, tms_httpd.conf and rdc_httpd.conf in the %OPA_HOME%\config path
  - <IfModule mod_proxy.c> sections to https://<Middle_Tier_Name.Domain>/.
  - This is because this file is used to forward requests from Apache to the OPA servlet engine, which is the OPA OC4J Server Service, which listens on the Middle Tier same server on Port 7881 (by default). The change to https is only necessary if Apache itself on the middle tier listens only to https

Option 2: Change the httpd.conf file and Set a Local Host entry

- The %ORACLE_iSuites_HOME%\Apache\Apache\conf\httpd.conf file should be changed to have all references of <Middle_Tier.Domain> and http://<Middle_Tier.Domain>/ changed to <Public_DNS_Server_Name> and https://<Public_DNS_Server_Name>/.
- However, many of these Apache components actually communicate with the Middle tier server itself, so an entry in %SystemRoot%\system32\drivers\etc\hosts of the form:
  - <local.ip.address> <Public_DNS_Server_Name.Domain>

  Is also necessary.

Option 1 and 2: Change the Directory Mappings

- The Oracle Clinical -> Admin -> Directory Mappings will need to have a new set of Directory mappings added for the https protocol where https://<Public_DNS_Server_Name>/log_directory is mapped to the UNC path of the share which contains the respective log and output files for the Report Server
- Currently, ftp access to the UNIX server does not require an additional entry, but https will be available in OC 4.5.1, which could then be mapped in a similar fashion.

Option 1 and 2: Set default route from the UNIX Server to the Middle Tier

- The RDC PDF 4.5 Data Entry mode needs to resolve and communicate correctly from an Oracle RDBMS package to the Middle Tier server. Therefore, a clear network path (default route) must exist from the UNIX database server to the Middle Tier server.

Testing the configuration

- Always backup the registry before making registry changes
- Always backup each file before modification
- Always reboot the middle tier after changes
- Always use the Java Console to very only https traffic and encrypted connections.

Additional configuration for Multiple Middle Tiers

- If there are multiple Middle Tiers behind a integrated SSL Accelerator/Proxy/Firewall network device, some additional changes need to be made:
  - HKEY_LOCAL_MACHINE->SOFTWARE->ORACLE->OPA_XMLTEMP_UNC should refer to a UNC temporary path on one of the servers
  - HKEY_LOCAL_MACHINE->SOFTWARE->ORACLE->RDC_DCIF_IMAGES should refer to a UNC path on %OPA_HOME%\HTML\RDC\DCIF_IMAGES on one of the servers
- Also, if this network device serves as a load balancer, then it should have its persistence mode or stickiness parameter set to keep OPA sessions from switching between server to server during a single OC or RDC Data Entry session (for example)

Is dual https connectivity required from client to Proxy, and then from Proxy to Middle Tier?

- In my opinion, no. This is because the entire goal of https/SSL communication is to protect **external** network traffic which is part of the **public internet**. But after the network traffic passes the public-facing entry point (Proxy Server/SSL Accelerator/Firewall) it is no longer visible to the public network, and therefore does not need to be encrypted.
- One of the primary advantages of having a single public-facing point of a network is that certificates only need to be acquired for that specific device, and not all of the internal servers. This represents both a cost and performance advantage. Both of these advantages are lost by having redundant https/SSL communications.

Conclusions

- https/SSL communication can be established either directly to a public facing middle tier or to an hardware SSL accelerator device
- This type of integrated hardware SSL Accelerator device integrated with a firewall and proxy server is the most common configuration for deploying OPA on the public internet.

Other Useful Sources

- Oracle Applications Performance Tuning Handbook by Andy Tremayne
- Metalink (Article 123718.1)
- Metalink (Article 274358.1)
- OCUG 2001 A&CM Focus Group Presentation by Sunil G. Singh on Configuration of https/SSL in an OC/TMS/RDC Environment: http://www.clinicalserver.com/data/ocug2001/oc_ssl/DBMS_OCUG2001OC_SSL.zip

Additional Questions ?

- Electronic copies will be posted on the OCUG Intranets Site and www.clinicalserver.com
- Additional copies will be available at DBMS Consulting's Vendor Exhibit Booth along with OPA 4.5 Architecture Posters and other giveaways