



IBM Software Group

Troubleshooting guidelines for TLS/SSL problems in WebSphere Cast Iron

Vani Madupu (vmadupu@us.ibm.com)
WebSphere Cast Iron L2 support, Team Lead
10th July 2014



WebSphere® Support Technical Exchange



Agenda

- Terms
- Certificates in Cast Iron
- TLS/SSL problem diagnosis part 1: understand the scenario
- TLS/SSL problem diagnosis part 2: isolate the cause
 - Server authentication with Cast Iron in the client role
 - Server authentication with Cast Iron in the server role
 - Mutual authentication with Cast Iron in the client role
 - Mutual authentication with Cast Iron in the server role
- SSL considerations for different form factors
 - Studio
 - Cast Iron Live
- New feature in V7- Cryptoservice
- Summary
- Q&A

Terms

- Secure Sockets Layer (SSL) – the original name of the protocol developed by Netscape® for securing network communication at the TCP® layer.
- Transport Layer Security (TLS) – the new name of the protocol given by the IETF (obsoletes SSL)
- Certificate – throughout this presentation, this means a digital certificate as described by the X.509 standard.
- X.509 - an ITU-T standard for a public key infrastructure (PKI)
- Public Key Infrastructure (PKI) - a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates
- Certificate Authority: A certificate authority (CA) is an authority in a network that issues and manages security credentials and public keys for message encryption

Certificates in Cast Iron -Factory Supplied Identity

- A self-signed certificate is generated on first boot for the appliance/HVE, when a Live tenant environment is provisioned and when Studio is installed. This is called the “factory supplied identity”.
- The factory supplied identity has an associated private key. These are stored together in the Key Store.
- The factory supplied identity represents the Cast Iron endpoint to SSL peers at least until a different certificate and private key is imported or generated.

Key Store (2)					
<input type="checkbox"/>	Alias	Issued To	Issued By	From Date	To Date
<input type="checkbox"/>	factory supplied identit	C=US,ST=CA,L=Mountain View,O=Cast Iron Systems,CN=Cast Iron	C=US,ST=CA,L=Mountain View,O=Cas	03/18/2014	03/17/2016
<input type="checkbox"/>	factory supplied identit	C=US,ST=CA,L=Mountain View,O=Cast Iron Systems,CN=Cast Iron	C=US,ST=CA,L=Mountain View,O=Cas	03/19/2014	03/18/2016

Generate Delete Import

Certificates in Cast Iron -Certificate Authority (CA) Certificates

- Well-known CA certificates are installed on first boot for the appliance/HVE, when a Live tenant environment is provisioned and when Studio is installed.
- The well-known CA certificates are obtained from the Java Runtime Environment (e.g. \$JAVA_HOME/jre/lib/security/cacerts).
- CA certificates are stored in the Trust Store.

Trust Store (76)			
<input type="checkbox"/>	Alias	Issued To	Issued I
<input type="checkbox"/>	addtrustclass1ca	CN=AddTrust Class 1 CA Root,OU=AddTrust TTP Network,O=AddTrust	CN=Add
<input type="checkbox"/>	addtrustexternalca	CN=AddTrust External CA Root,OU=AddTrust External TTP Network,O=	CN=Add
<input type="checkbox"/>	addtrustqualifiedca	CN=AddTrust Qualified CA Root,OU=AddTrust TTP Network,O=AddTru:	CN=Add
<input type="checkbox"/>	aolrootca1	CN=America Online Root Certification Authority 1,O=America Online I	CN=Ame
<input type="checkbox"/>	aolrootca2	CN=America Online Root Certification Authority 2,O=America Online I	CN=Ame
<input type="checkbox"/>	baltimorecodesigningca	CN=Baltimore CyberTrust Code Signing Root,OU=CyberTrust,O=Baltir	CN=Balt
<input type="checkbox"/>	baltimorecybertrustca	CN=Baltimore CyberTrust Root,OU=CyberTrust,O=Baltimore,C=IE	CN=Balt
<input type="checkbox"/>	certplusclass2primaryca	CN=Class 2 Primary CA,O=Certplus,C=FR	CN=Clas
<input type="checkbox"/>		CN=Cl	CN=Cl

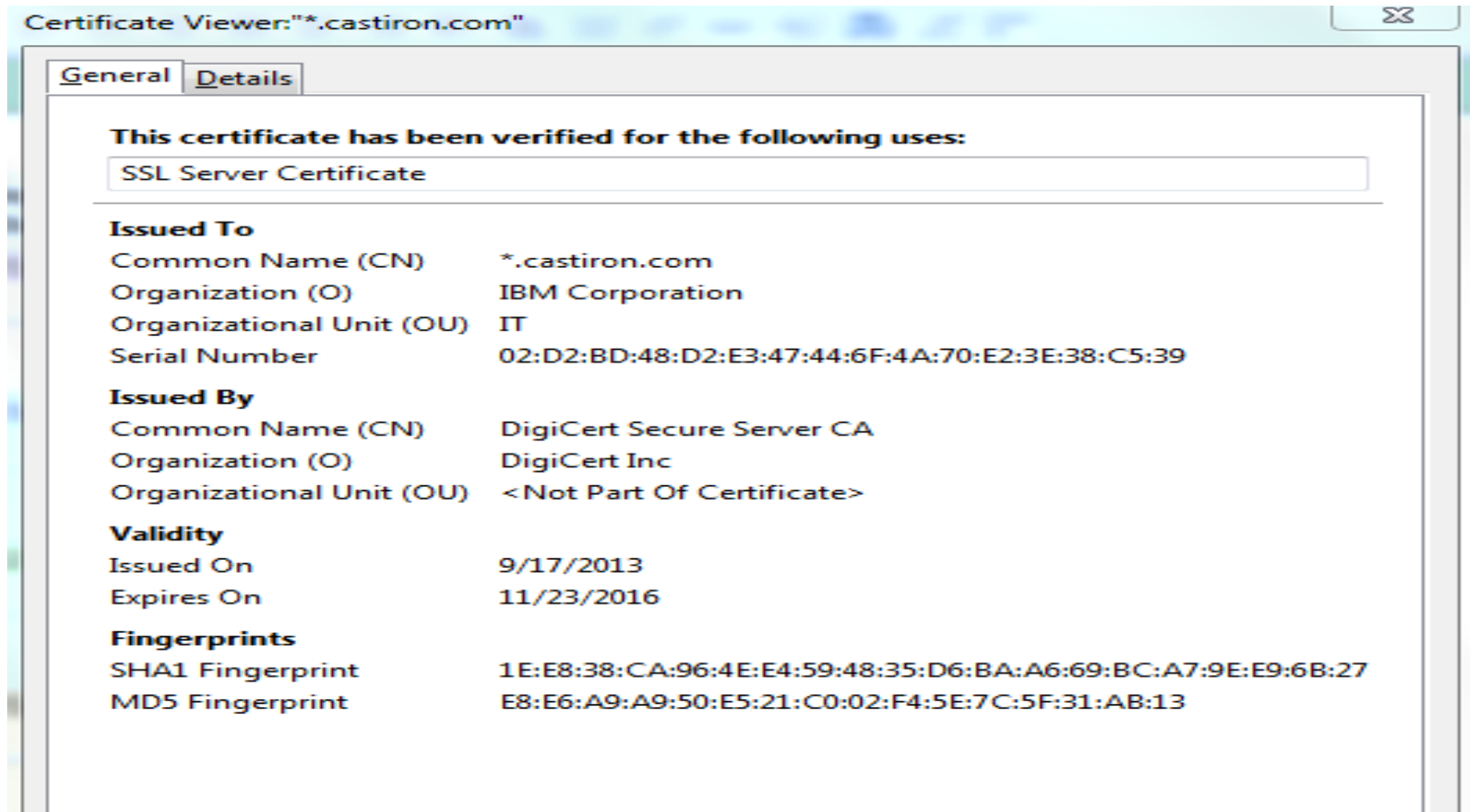
Certificates in Cast Iron -Live certificate

- All Cast Iron Live offerings have a publicly accessible web site that requires HTTPS.
- These web sites need a certificate signed by a well-known CA. Otherwise, users will see pop-ups in their web browsers saying that the site is not trusted.
- Cast Iron uses the same certificate for all cloud web sites.
- Most browsers allow you to see the certificate details of the sites you connect to

Website Identity

Website: **cloud2.castiron.com**
Owner: **This website does not supply ownership information.**
Verified by: **DigiCert Inc**

Certificates in Cast Iron Live certificate general contents



Certificate Viewer: "*.castiron.com"

General Details

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	*.castiron.com
Organization (O)	IBM Corporation
Organizational Unit (OU)	IT
Serial Number	02:D2:BD:48:D2:E3:47:44:6F:4A:70:E2:3E:38:C5:39

Issued By

Common Name (CN)	DigiCert Secure Server CA
Organization (O)	DigiCert Inc
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	9/17/2013
Expires On	11/23/2016

Fingerprints

SHA1 Fingerprint	1E:E8:38:CA:96:4E:E4:59:48:35:D6:BA:A6:69:BC:A7:9E:E9:6B:27
MD5 Fingerprint	E8:E6:A9:A9:50:E5:21:C0:02:F4:5E:7C:5F:31:AB:13

Certificates in Cast Iron -Importing certificates

- Users can generate certificates outside of Cast Iron and then import them.
- Understand the use-case before you import certificates into Cast Iron.
- Understand which store (the Key Store or the Trust Store) the certificates belong in.
- Hint: you can only import PKCS12 files into the Key Store.
- Hint: you can only import PEM/CER, DER or PKCS7 files into the Trust Store.
- PKCS12 files contain both a certificate and a private key and they have a password (to protect the private key).
- PEM/CER, DER and PKCS7 files do not contain private keys (only certificates).
 - PEM/CER is cut-and-pasteable text
 - DER is binary
 - PKCS7 is a binary chain of certificates

Certificates in Cast Iron -Importing certificates

Key Store (2)		
<input type="checkbox"/>	Alias	Issued To
<input type="checkbox"/>	factory supplied id	C=US,ST=CA,L=Mountain View,O=Cast Iron Systems,CN=
<input type="checkbox"/>	factory supplied id	C=US,ST=CA,L=Mountain View,O=Cast Iron Systems,CN=

Generate Delete **Import**

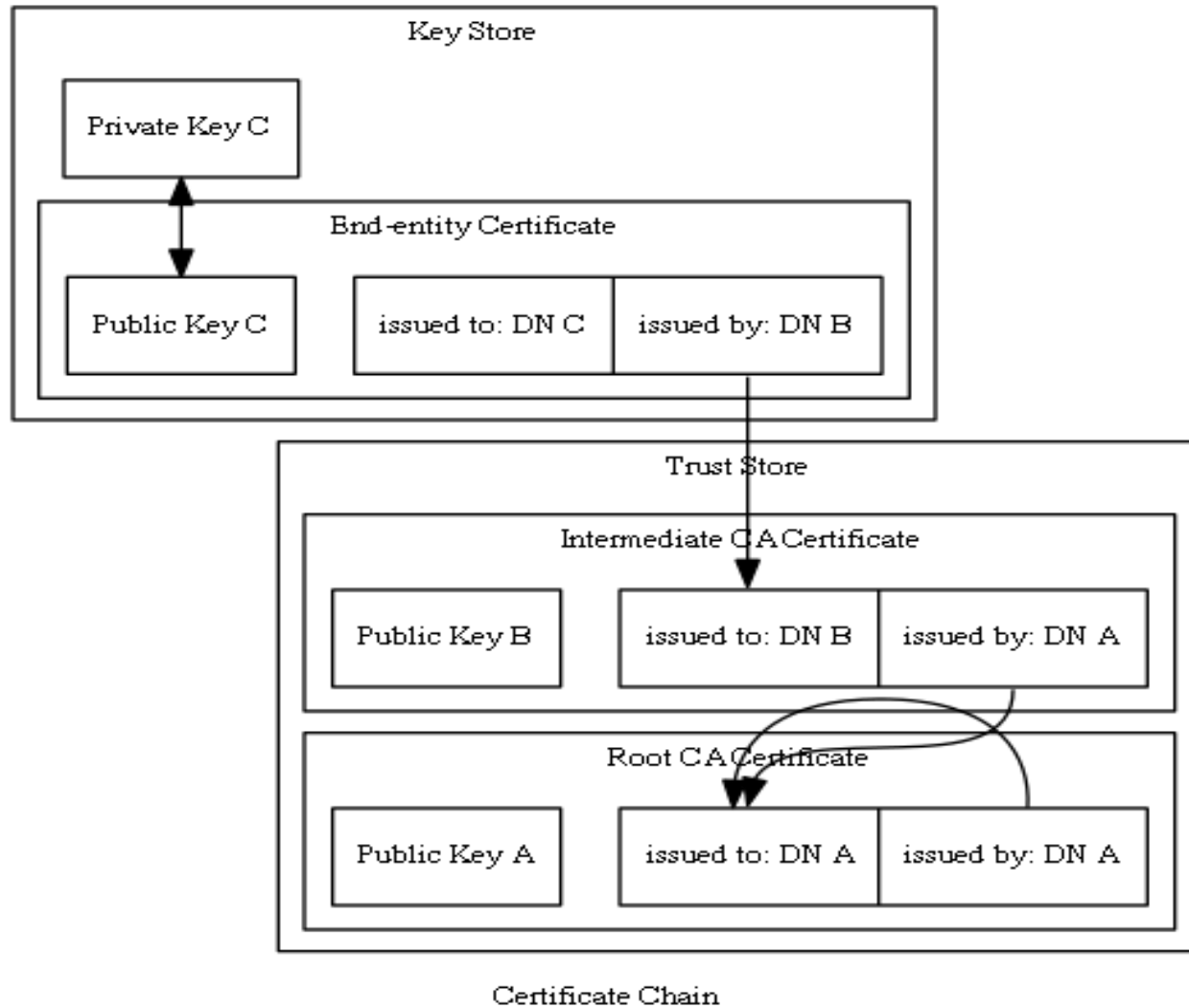
Trust Store (76)		
<input type="checkbox"/>	Alias	Issued To
<input type="checkbox"/>	addtrustclass1ca	CN=AddTrust Class 1 CA Root,OU=AddTrust
<input type="checkbox"/>	addtrustexternalca	CN=AddTrust External CA Root,OU=AddTrust

Delete **Import**

- Click on a certificate alias in the Key Store and you will have an option to “Upload” a certificate to replace the one with the given alias

Certificate Details - factory supplied identity s...	
Issued To	
Common Name (CN)	Cast Iron Appliance VMWBIS6R7YS5TABK
Organization (O)	Cast Iron Systems
Country (C)	US
State (ST)	CA
Locale (L)	Mountain View
Serial Number	77:77:89:51
Issued By	
Common Name (CN)	Cast Iron Appliance VMWBIS6R7YS5TABK
Organization (O)	Cast Iron Systems
Country (C)	US
State (ST)	CA
Locale (L)	Mountain View
Validity	
Issued On	03/19/2014
Expires On	03/18/2016
Fingerprints	
SHA1 Fingerprint	15:C2:77:CF:70:E8:AA:8B:DF:32:30:BE:AE:5F:E7:E3:B0:59:0C:E1
MD5 Fingerprint	E7:1D:ED:7F:2C:89:35:61:F6:70:54:E0:29:1B:0F:F3
Rename Generate CSR Upload Export Close	

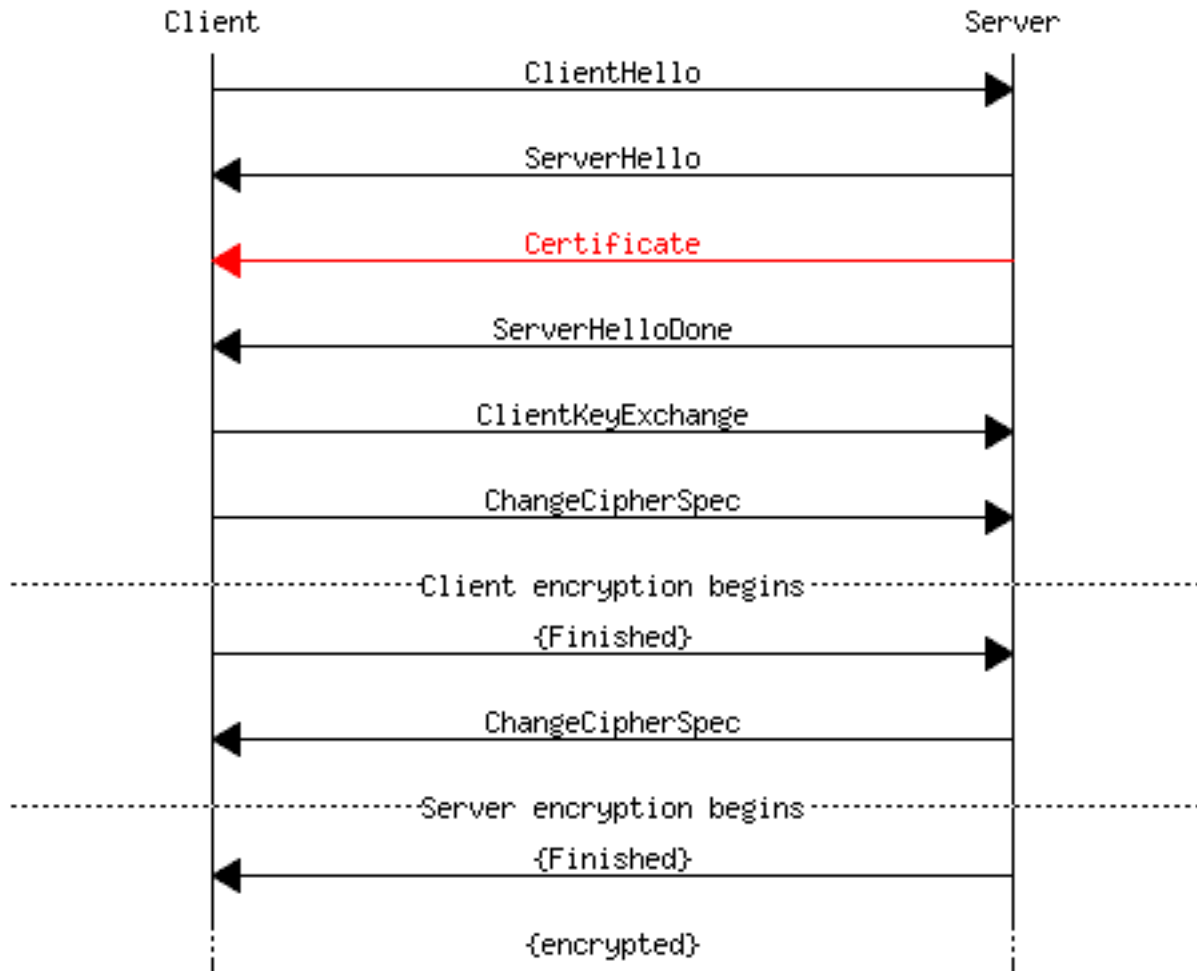
Certificates in Cast Iron -Certificate Chains



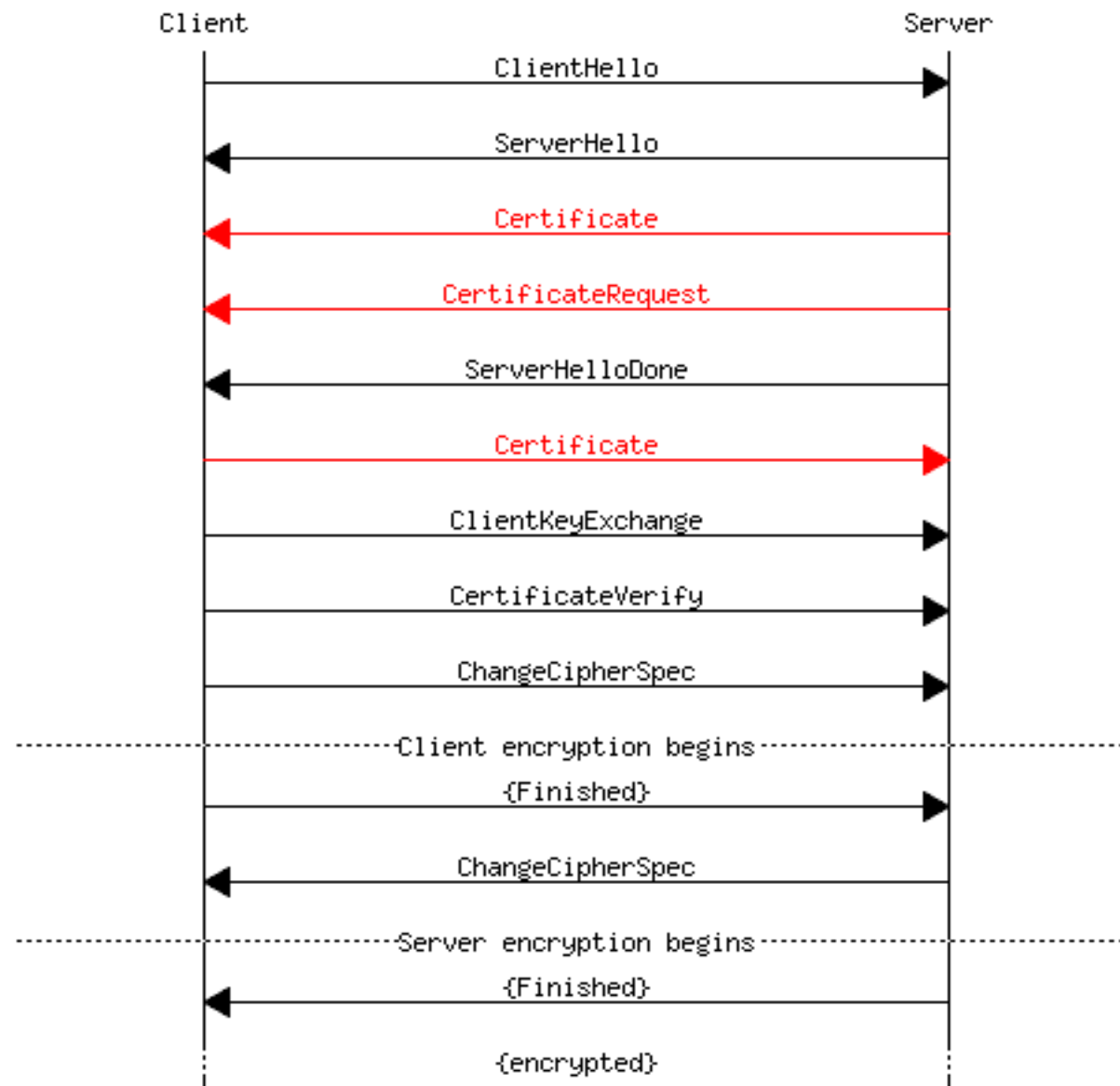
Certificates in Cast Iron - Peer authentication

- Cast Iron can be either the client or the server in an SSL connection.
- When either the client or the server sends a certificate, the purpose is to identify itself to the peer.
- The recipient of a certificate in an SSL session is responsible for verifying the contents. This is called peer authentication.
- When neither the client nor the server sends a certificate, the SSL session is called “anonymous”. Cast Iron does not support anonymous SSL.
- When both the client and the server send a certificate, the SSL session is said to have mutual authentication.
- If the SSL session is not anonymous, the server is required to send a certificate.
- There is no “client only” authentication method in SSL.

Certificates in Cast Iron -Server authentication illustrated



Certificates in Cast Iron - Mutual authentication illustrated



Peer Authentication -Server authentication with Cast Iron in the client role

- Servers that Cast Iron connects to must send certificates identifying themselves to Cast Iron.
- In order for Cast Iron to verify the certificate received from the server, the VPeer checkbox must be checked on the Client SSL row in the WMC Security->Certificates->Settings panel.
- If the received certificate is self-signed, it must be imported into the Trust Store.

Settings				
SSL Usage Type	Certificate Alias	VPeer	VHost	Cipher Strength
Client SSL	factory supplied identity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Strong
Server SSL over data NIC	factory supplied identity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Strong
Server SSL over mgmt NIC	factory supplied identity	<input type="checkbox"/>	<input type="checkbox"/>	Strong

Edit

Peer Authentication -Server authentication with Cast Iron in the client role (VHost)

- Cast Iron can be configured to verify that the domain name contained in a verified server certificate matches the hostname in the URL that Cast Iron connected to
- This check can be enabled by checking the VHost check box on the Client SSL row. The VPeer check box must also be checked. The setting does not apply for any other row.
- The certificate to be checked must contain a subjectAltName extension of type dNSName or the Common Name field of the certificate Subject field must contain a domain name.
- The rule of thumb is that the server should have a certificate that is valid for every DNS name configured to point to it (i.e. containing multiple domain names if necessary).

Settings				
SSL Usage Type	Certificate Alias	VPeer	VHost	Cipher Strength
Client SSL	factory supplied identity	✓	<input checked="" type="checkbox"/>	Strong
Server SSL over data NIC	factory supplied identity	✓		Strong
Server SSL over mgmt NIC	factory supplied identity			Strong

Edit

Peer Authentication -Server authentication with Cast Iron in the server role

- Cast Iron must send a certificate identifying itself to clients.
- In order for Cast Iron to send a certificate to clients, a certificate alias must be specified that matches one in the Key Store.
- A server certificate alias can be specified at the appliance level in the WMC on the Server SSL over data NIC row in the WMC Security->Certificates->Settings panel.
- A server certificate alias can also be specified at the activity level in Studio.
- The Server SSL over data NIC row does not exist for Cast Iron Live. The cloud certificate is the one that is sent.

Settings				
SSL Usage Type	Certificate Alias	VPeer	VHost	Cipher Strength
Client SSL	factory supplied identity	✓	✓	Strong
Server SSL over data NIC	factory supplied identity	✓		Strong
Server SSL over mgmt NIC	factory supplied identity			Strong

Edit

Peer Authentication - Mutual authentication with Cast Iron in the client role

- Some servers can be configured to require that the client send a certificate identifying itself.
- In order for Cast Iron to send a certificate to a server, a certificate alias must be specified that matches one in the Key Store.
- A client certificate alias can be specified at the appliance level in the WMC on the Client SSL row in the WMC Security->Certificates->Settings panel.
- A client certificate alias can also be specified at the activity level in Studio.

Settings				
SSL Usage Type	Certificate Alias	VPeer	VHost	Cipher Strength
Client SSL	factory supplied identity	✓	✓	Strong
Server SSL over data NIC	factory supplied identity	✓		Strong
Server SSL over mgmt NIC	factory supplied identity			Strong

Edit

Peer Authentication - Mutual authentication with Cast Iron in the server role

- For the appliance (physical / hypervisor only), Cast Iron can be configured to require that clients connecting to Cast Iron send a certificate. This is called client authentication with Cast Iron in the server role.
- To enable this configuration, check the VPeer check-box on the Server SSL over data NIC row.
- If the certificate that the client sends to Cast Iron is self-signed, it must be imported into the Trust Store.

Settings				
SSL Usage Type	Certificate Alias	VPeer	VHost	Cipher Strength
Client SSL	factory supplied identity	✓	✓	Strong
Server SSL over data NIC	factory supplied identity	✓		Strong
Server SSL over mgmt NIC	factory supplied identity			Strong

SSL considerations for different form factors - Studio

- There is no interface in Studio for managing the Key Store and Trust Store. You must use the Java keytool command from the command line.
- By default, the Key Store and Trust Store are located in the security subdirectory of the Studio installation directory.
- The default Key Store name is “certs” and the default password is “Key Store admin”.
- The default Trust Store name is “cacerts” and the default password is “changeit”.
- There are no “VPeer” or “VHost” selections in Studio. Those options can only be enabled in the WMC.
- For importing certificates into the Studio Key Store, see:
http://pic.dhe.ibm.com/infocenter/wci/v7r0m0/topic/com.ibm.wci.doc/SSL_import_a_end_entity_certif.html
- For importing certificates into the Studio Trust Store, see:
http://pic.dhe.ibm.com/infocenter/wci/v7r0m0/topic/com.ibm.wci.doc/SSL_import_a_certif_authority_certif.html

SSL considerations for different form factors - Cast Iron Live

- There is no “Server SSL over Data NIC” row or “Server SSL over Mgmt NIC” row in the WMC for Cast Iron Live. Cast Iron Live doesn't have the concept of a “Data NIC” and a “Mgmt NIC”.
- Impacts:
 - Live tenants cannot configure mutual authentication with Cast Iron in the server role.
 - Live tenants cannot configure CipherStrength or Certificate Alias with Cast Iron in the server role.

TLS/SSL problem diagnosis part 1: understand the scenario

- Gather information about the TLS/SSL session end points.
 - Gather information about the TLS/SSL client end point.
 - Is Cast Iron the client?
 - Identify the client IP address.
 - Identify the client platform.
 - Identify the client activity.
 - Gather information about the TLS/SSL server end point.
 - Is Cast Iron the server?
 - Identify the server IP address.
 - Identify the server platform.
 - Identify the server activity.
- Determine the TLS/SSL session peer authentication scenario

TLS/SSL problem diagnosis part 2: Isolate the cause scenario: Server authentication with Cast Iron in the client role

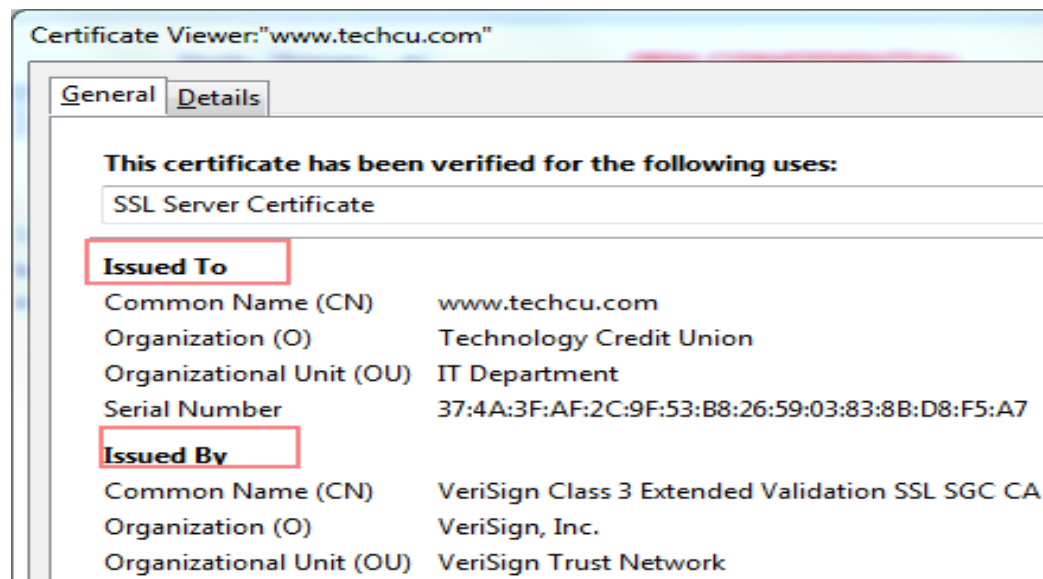
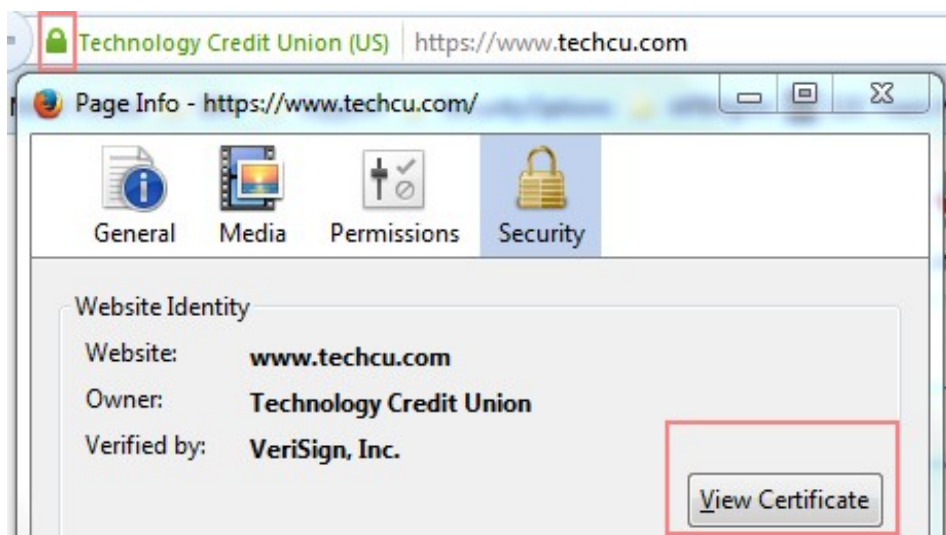
- Servers that Cast Iron connects to must send certificates to Cast Iron.

➤

Settings				
SSL Usage Type	Certificate Alias	VPeer	VHost	Cipher Strength
Client SSL	factory supplied identity	✓	✓	Strong
Server SSL over data NIC	factory supplied identity	✓		Strong
Server SSL over mgmt NIC	factory supplied identity			Strong

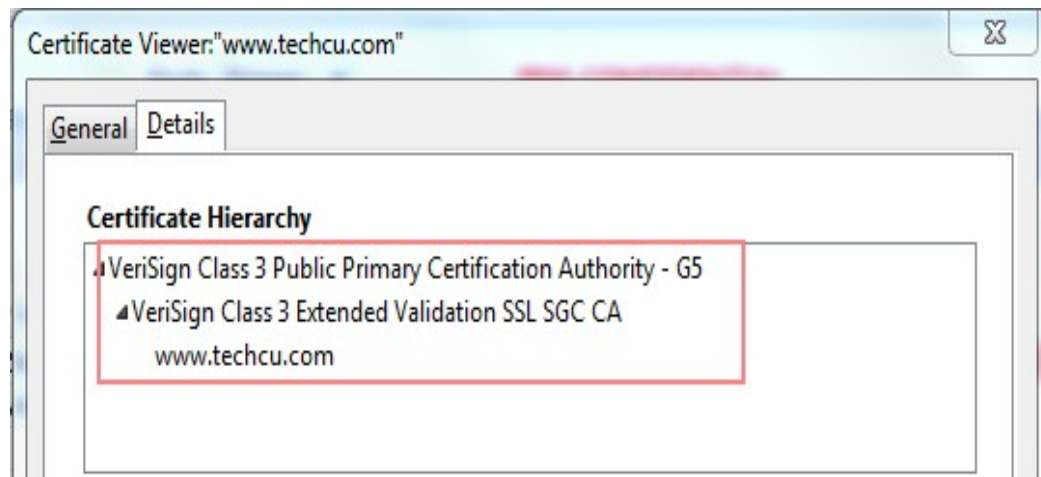
Edit

- Obtain the server certificate. If the server has a public HTTPS URL, use your browser to connect and view the certificate.



TLS/SSL problem diagnosis part 2: Isolate the cause scenario: server authentication with Cast Iron in the client role

- If the server certificate is self-signed, it must be stored in the Cast Iron trust store.
 - Check if it is expired
- If the server certificate is not self-signed,
 - Identify the the chain of certificates involved
 - Certificates for all the certificates in the chain must be stored in the Cast Iron trust store



TLS/SSL problem diagnosis part 2: Isolate the cause

scenario: Server authentication with Cast Iron in the server role

- Cast Iron must send a certificate identifying itself to clients.
- A server certificate must be imported in the Cast Iron Key Store. Check if it is expired
- This server certificate alias can be specified

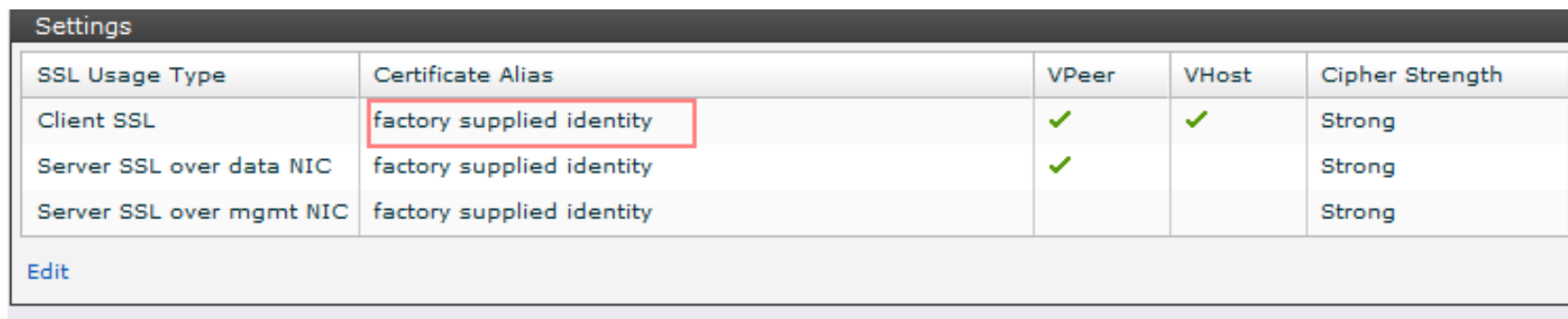
Settings				
SSL Usage Type	Certificate Alias	VPeer	VHost	Cipher Strength
Client SSL	factory supplied identity	✓	✓	Strong
Server SSL over data NIC	factory supplied identity	✓		Strong
Server SSL over mgmt NIC	factory supplied identity			Strong

Edit

- At the activity level in Studio.
- The Cast Iron cloud certificate is sent in Cast Iron Live.
- If the server certificate is self-signed, it must be stored in the client trust store
- If the server certificate is not self-signed,
 - Identify the chain of certificates involved
 - Certificates for all the certificates in the chain must be stored in the Cast Iron trust store

TLS/SSL problem diagnosis part 2: Isolate the cause scenario: mutual authentication with Cast Iron in the client role

- Cast Iron must send a certificate identifying itself to the server.
- A certificate must be imported in the Cast Iron Key Store. Check if it is expired
- This certificate alias can be specified



SSL Usage Type	Certificate Alias	VPeer	VHost	Cipher Strength
Client SSL	factory supplied identity	✓	✓	Strong
Server SSL over data NIC	factory supplied identity	✓		Strong
Server SSL over mgmt NIC	factory supplied identity			Strong

Edit

- At the activity level in Studio.
- If the client certificate is self-signed, it must be stored in the server trust store
- If the client certificate is not self-signed,
 - Identify the the chain of certificates involved
 - Certificates for all the certificates in the chain must be stored in the Cast Iron trust store.

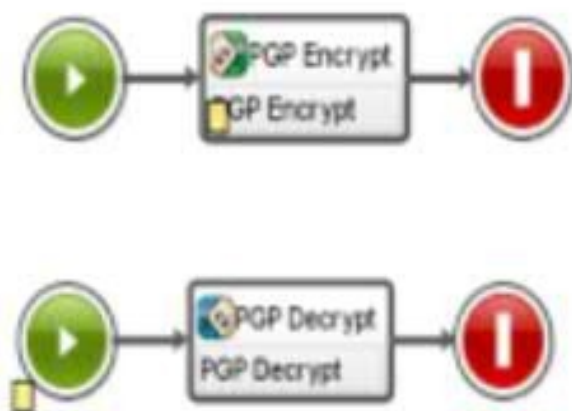
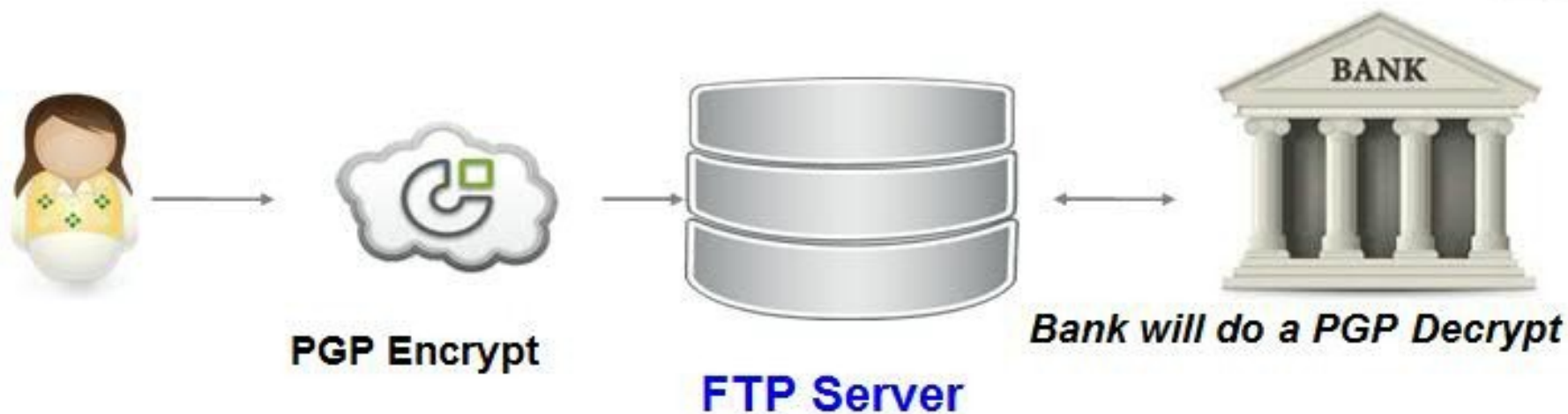
TLS/SSL problem diagnosis part 2: Isolate the cause scenario: mutual authentication with Cast Iron in the server role

- Clients connecting to Cast Iron must send a certificate.
- To enable this configuration, check the VPeer check-box on the Server SSL over data NIC row.

Settings				
SSL Usage Type	Certificate Alias	VPeer	VHost	Cipher Strength
Client SSL	factory supplied identity	✓	✓	Strong
Server SSL over data NIC	factory supplied identity	✓		Strong
Server SSL over mgmt NIC	factory supplied identity			Strong

- If the server certificate is self-signed, it must be stored in the client trust store. Check if it is expired.
- If the server certificate is not self-signed,
 - Identify the the chain of certificates involved
 - Certificates for all the certificates in the chain must be stored in the Cast Iron trust store

Support for PGP™ Encryption and Decryption – New feature in V7.



Summary

- Understand the Use-case to identify the Cast Iron role in the SSL communication.
- Determine the TLS/SSL session peer authentication scenario
- Follow the problem isolation steps discussed based on the scenario.
- Use the browser's Windows Certificate viewer to examine the details of the certificate
- Support for PGP encryption and decryption is available in V7.

Reference Material

- WebSphere Cast Iron Infocenter:
<http://pic.dhe.ibm.com/infocenter/wci/v7r0m0/index.jsp>
- WebSphere Cast Iron Support Page for updates:
http://www.ibm.com/support/entry/portal/product/websphere/websphere_cast_iron_cloud_integration
- Cast Iron Community forums:
<http://www.ibm.com/developerworks/forums/category.jspa?categoryID=305>
- Follow us on Twitter @
<http://twitter.com/CastIronSystems> to receive timely updates

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at:
http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:
<http://www.ibm.com/developerworks/websphere/community/>
- Join the Global WebSphere Community:
<http://www.websphereusergroup.org>
- Access key product show-me demos and tutorials by visiting IBM Education Assistant:
<http://www.ibm.com/software/info/education/assistant>
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically:
<http://www.ibm.com/software/websphere/support/d2w.html>
- Sign up to receive weekly technical My Notifications emails:
<http://www.ibm.com/software/support/einfo.html>

Connect with us!

1. Get notified on upcoming webcasts

Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe

2. Tell us what you want to learn

Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com

Questions and Answers