

Canadian Trade Repository

This topic provides an overview of CME's Canadian Trade Repository (CTR). It details supporting functions, workflows, message flows, and interfaces to allow registered users to submit and retrieve swap data in the CTR. CTR leverages existing CME repository and clearing services connectivity, functionality, and processes in order to accept, store, and report swap data.

- [Revision History](#)
- [Prerequisites](#)
- [Access to the CME CTR](#)
 - [Registering for CTR Test Environment Access](#)
 - [Registering for CTR Production Environment Access](#)
 - [Additional User Access Requests](#)
 - [Access Levels](#)
- [Trade Submissions to CME CTR](#)
 - [Transport Overview](#)
 - [MQ](#)
 - [Web Services](#)
 - [Contact repositorysupport@cmegroup.com](mailto:repositorysupport@cmegroup.com)
 - [URLs](#)
 - [Web User Interface Upload](#)
 - [SFTP](#)
 - [About SFTP](#)
 - [Getting Access to SFTP](#)
 - [New Client](#)
 - [Existing Client](#)
 - [Technical Set-Up Information](#)
 - [SFTP via CME WAN connectivity](#)
 - [SFTP via Internet](#)
 - [CME Public Key Installation](#)
 - [CME SFTP Directory and Path Structure](#)
 - [Submitting Files to SFTP](#)
 - [File Naming Convention for CSV files](#)
- [CTR Messages Flows](#)
 - [CME Cleared Trade Submissions to CME TR](#)
 - [Agency Clearing Model](#)
 - [Principal Clearing Model](#)
 - [CME Bilateral \(Non-Cleared\) Trade Submissions to CME CTR](#)
 - [Life-Cycle \(Continuation\) Data Reporting](#)
 - [Reporting Continuation Data for all other Trades \(Bilateral and Cleared at other Clearing Agencies\)](#)
- [Generate Authentication Token](#)
- [Importing Certificate in Local Java Store](#)

Revision History

Date	Version	Description
October 1, 2014	1.0	Initial publication.
October 1, 2016	2.0	Revised.
June 24, 2019	2.0	Replaced PDF with wiki. Added support for Equity asset class. Added FAQ and sFTP details.

Prerequisites

This topic assumes the user has basic trade repository flow knowledge. For more information, please refer to the relevant Canadian provincial derivatives regulations or contact our team:

Contact Information

CTR Business Team: repository@cmegroup.com

CTR Support Team: repositorysupport@cmegroup.com

CTR Support Team Phone number:

- Chicago +1 (312) 580 5352
- London +44 (0) 203 379 3180
- Singapore +65 6593 5592

Additional Information

www.cmegroup.com/ctr

Access to the CME CTR

Registering for CTR Test Environment Access

To assist clients with preparation for various Canadian provincial reporting regulations, CME CTR provides a test environment. Access to the test environment can be granted prior to execution of the CME CTR User Agreement by completing an informational form. Production environment access may only be granted to users and service providers with completed registrations and legal agreements. A full CTR user registration also includes access to the test environment. Service providers do not have a test environment only option, and must complete the full Service Provider Agreement, which includes test environment access.

Steps to request access to the CME ETR test environment:

1. Complete the **User Agreement** or Test Environment form (single form to gain access to any of CME's Global Trade Repositories) from www.cmegroup.com/ctr.

 Fill out the registration form electronically (do not print and complete).

2. Use the form's submit button; your system's default email program prepares an email to the CTR Registration Team. If you prefer a different email program, copy the email attachment and email address to your preferred program.
3. Once the form is received, CME processes the request. Upon completion, CME CTR sends an email to the administrator contact confirming the registration and provides information on how to get started.

 The URL <https://ctrui.rn.cmegroup.com.ctrui> for the test environment is different from the production environment.

For assistance during or following the registration process; please send an email to CME Global Repository Client Services repositorysupport@cmegroup.com.

Registering for CTR Production Environment Access

Access to the production environment is granted only to fully registered users and authorized service providers. The following steps outline the registration process to submit and access derivative data in the CME CTR for Canadian reporting compliance.

1. Obtain a Legal Entity Identifier (LEI).

An LEI is strictly required at the time of full registration. An LEI is required for each separate legal entity for whom data will be submitted or retrieved in the CME CTR. Users may acquire a LEI through one of the authorized LEI issuers listed in <http://www.lei.org>. An LEI obtained previously for a legal entity to satisfy other business purposes (including trade reporting in a different global jurisdiction) may be used in the CME CTR registration if the issuer is recognized on the LEI ROC website.

CME Central Counterparty (CCP) LEI's provided for reference:

- **CME Chicago Mercantile Exchange Inc. (US Clearing House)**
 - CME Inc. LEI: **SNZ2OJLJK8MNNCLQOF39**
 - CME Inc. UTI Namespace: 1010000023
2. Execute the agreement (User Agreement or Service Provider Agreement).

User Agreement: Entered into by a party to a derivatives transaction; the agreement enables the registered user to (1) submit, (2) analyse/filter, (3) extract, and (4) authorize their counterparty or service provider (not a party to the transaction) to view its derivative data stored in CME CTR. In order to execute the CME CTR User Agreement:

- Download the agreement from the CME CTR website www.cmegroup.com/ctr. Complete the user agreement and click the send button to electronically submit the agreement to the CME CTR Registration team.
- The user agreement is received and processed by the CME CTR Registration team. Notification of receipt of the submission is provided, and a subsequent notification is sent when the registration is completed. In the registration complete email, instructions are provided to contact the CME registration team to receive the login information over the phone (for security reasons).
- Schedule A (CME CTR registration entity details): A required form as part of CME CTR registration. Firms are required to specify at least one Verification Officer upon registration. The Verification Officer acts as the account administrator--approving any new requests, access modifications, etc. In addition to a Verification Officer, regular users are also requested. Verification Officers have a choice of admin roles or view only roles. Admin roles allow users to upload, amend, and view; whereas a View Only role allows for read only access to the CTR.
- Schedule C: bulk registration for investment advisors or multiple entities under the same corporate structure. Schedule C is available from www.cmegroup.com/ctr.

Service Provider Agreement: Applies to entities that are not party to the trade and are providing services to facilitate the trade report in some capacity on behalf of one or both of the obligated counterparties to the reportable derivatives trade. Parties interested in a Service Provider registration should send an email to CME CTR repository@cmegroup.com

Additional User Access Requests

Once registered, accounts may authorise additional users to access the data (i.e. internal staff, fund administrators, other intra-group entities, etc.). Please follow the instructions on the additional user access request form from www.cmegroup.com/ctr.

Access Levels

CMECTRAdministrator:

- Rights to create, modify, and remove user accounts
- Rights to view data for all accounts
- Rights to upload data for all accounts
- Rights to run all reports and download the results for all accounts

CMECTRFullAccess:

- Rights to view data for accounts
- Rights to upload data for accounts
- Rights to run all reports and download the results for accounts

CMECTRViewOnlyAccess:

- Rights to view data for accounts

CMECTRViewOnlyAccess:

- Queries regarding permissioning for Regulatory Authorities should be emailed to repositorysupport@cmegroup.com.

Trade Submissions to CME CTR

Swaps are submitted to CME CTR via the following methods:

Format	Transport
FIX API	MQ
FIX File	HTTPS web services
CSV File	Website upload
CSV File	HTTPS web services
CSV File	sFTP

Transport Overview

MQ

FIXML API submission via MQ is a full service option for submitting, cancelling, or amending derivative data to CME CTR.

MQ is an IBM product that facilitates software messaging between two computer systems. In order to use MQ based messaging system, firms require installation of IBM MQ client software. Please note that IBM is an independent company from CME, and therefore, firms will need to appropriately license the software.

A prerequisite to facilitate MQ connectivity is establishing connectivity into the CME network. This is accomplished via either a Virtual Private Network (VPN) or a leased line connection to CME. Existing direct connectivity to the CME network maintained by the User/Service Provider for access to other CME systems may be leveraged for using CME CTR services.

For more information on establishing an MQ connection or leveraging an existing MQ connection with CME, please send an email to repositorysupport@cmegroup.com.

Web Services

CME CTR allows programmatic submissions, cancellations, and amendments via secure http web services. This web service submission facilitates connection to the CME CTR via the internet, removing the need for any other type of connectivity infrastructure (such as MQ). Either FIXML or CSV formatted data may be passed via this transport method. Full technical details are available below:

FIXML API

Please contact repositorysupport@cmegroup.com

CSV

Authentication Token	Refer to Appendix A
Data Capture Generate	Contact repositorysupport@cmegroup.com
Importing Certificate in Local Java Keystore	Refer to Appendix B
Submitting CSV Message File	Refer to CSV Specs here

URLs

UAT/NR:

<https://ctrwsnr.cmegroup.com/datacapture-ws/ctr/submitCSV/CMDTY>
<https://ctrwsnr.cmegroup.com/datacapture-ws/ctr/submitCSV/FX>
<https://ctrwsnr.cmegroup.com/datacapture-ws/ctr/submitCSV/EQUITY>
<https://ctrwsnr.cmegroup.com/datacapture-ws/ctr/submitCSV/IRS>
<https://ctrwsnr.cmegroup.com/datacapture-ws/ctr/submitCSV/CDS>

PROD:

<https://ctrws.cmegroup.com/datacapture-ws/ctr/submitCSV/CMDTY>
<https://ctrws.cmegroup.com/datacapture-ws/ctr/submitCSV/FX>
<https://ctrws.cmegroup.com/datacapture-ws/ctr/submitCSV/EQUITY>
<https://ctrws.cmegroup.com/datacapture-ws/ctr/submitCSV/IRS>
<https://ctrws.cmegroup.com/datacapture-ws/ctr/submitCSV/CDS>

Web User Interface Upload

Users or service providers may use the CME CTR secure web User Interface (UI) to upload CSV formatted files. On-screen confirmations are provided on acceptance or identify required corrective actions. Full documentation on this option (including the asset class specific CSV templates and samples) are available [here](#).

SFTP

About SFTP

Secure File Transfer Protocol (SFTP), is a method of transferring data between to end points using strong encryption and authentication. We utilize this to allow confidential and easy transfer of files between our clients and our CME Repositories.

Getting Access to SFTP

New Client

For any client who wishes to use CME for their TR needs they will need to complete a User Agreement, within this agreement they will be presented the below question to which you must select "Secure FTP CSV" (to note you can select as many methods as you like or specify none for view only access if someone is reporting on your behalf)

Fig.1 Taken from CTR User Agreement

5. Transaction Submission

Please select how you plan to submit transactions to the CME Canadian Trade Repository. Check all that apply.

- Participant User Interface (includes CSV file upload)
- Secure FTP CSV
- Web Services CSV delivery
- Web Services FIXML delivery
- None – I do not plan to submit any trades to CTR

Once all the onboarding is complete Client Services will provide your chosen Verification Officer the folder Username & Password.

Existing Client

Please have your Verification Officer reach out to repositorysupport@cmegroup.com with your request to have an SFTP folder and then someone will reach back out to your Verification Officer with the folder Username & Password. Note, if your firm has a pre-existing SFTP folder for other CME business services, another SFTP account will still need to be created specifically for your firms CME Repository submissions.

Technical Set-Up Information

CME supports file transfer through Secure FTP available via Wide Area Network connection as well as via the Internet. Please have your IT Staff facilitate the below connectivity and provide access through your firewall for our IPs as required.

SFTP via CME WAN connectivity

This requires firms to have direct access to the CME network via circuit.

Production IP: 167.204.41.33 (port 22)

Disaster Recovery: Same as Production IP address above.

CME will whitelist IP addresses connecting via this method. A gateway range will have been provided to a contact within your firm when direct circuit access to CME was established.

In the event of a DR situation, the failover will not require firms to switch access or manage additional entries to their firewall.

SFTP via Internet

Web based without a direct connection to CME.

When using SFTP, SSH encrypted software is required for the connection.

CME does not require firms to enter the internet based SFTP IP address into their firewall to access the site. CME only require users to utilize an sftp tool and a valid CME provided SFTP account and password.

Environment	IP	DNS	Port
Production	164.74.122.33	sftpng.cmegroup.com	22
Disaster Recovery	204.10.15.24	sftpng.cmegroup.com	22
UAT (testing)	164.74.123.120	sftpcert.cmegroup.com	22

CME Public Key Installation

CME allows the use of public/private key authentication. (SSH Public Key File format RFC4716). Firms who require the use of public keys are responsible for the installation themselves.

Please note: Public key may not be required as it is dependant of the connection method you use

CME uses *SSH Public Key File Format (RFC4716)*

The location of your public key should be installed to:

"YOUR_CME_SFTPNG_HOMEDIR"/.ssh/"USERNAME"

Example, where username is "USERNAME":

```
sftp> ls .ssh  
.ssh/USERNAME
```

If you already have an RFC4716 Public Key file yet installed at CME

Here's the steps, you'll need to update the Public Key named "USERNAME" at CME:

1. Sftp to the site
2. Run the command, `sftp> get .ssh/"USERNAME"` where "USERNAME" is your login name.
3. Append new key(s) to the Public key file.
4. Put the key file up, `sftp> put .ssh/"USERNAME"` where "USERNAME" is your login name.

If you don't have an RFC4716 Public Key file yet installed at CME

Here are the steps, you'll need to have the Public Key file named "USERNAME" which contains the keys in the local directory on your source host in order for these steps to work:

1. `ssh-keygen -t rsa -b 2048 -f id_rsa -N "" && ssh-keygen -e -f id_rsa > USERNAME`
2. sftp to the site
3. Put the key file up, `sftp> put .ssh/"USERNAME"` where "USERNAME" is your login name.
NIST expects that a 2048 key size will be secure until 2030 (<http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>). You can opt for 4096, but it is not required.
More about RFC 4716 <https://tools.ietf.org/html/rfc4716>

CME SFTP Directory and Path Structure

Regardless how firms connect to their CME sftp account, there are 3 default directories that each firm is provided when their sftp account is added. Each folder is utilized for a specific purpose as outlined below including the directory path, note that 123 represents the firm's sftp account ID:

cme/ftp/123/Incoming (with upper case I)
cme/ftp/123/Outgoing (with upper case O)
cme/ftp/123/PUB (all upper case)

When a user logs into their sftp account, the default maps to the user account root directory where the above 3 folders securely accessed by the account. Firms then can navigate between the folders and sub-folders based on their data upload or download requests.

Incoming: Used for confidential data files submitted by firms to CME. Firms will upload the required files to the Incoming directory as required by CME.

Outgoing: Used for confidential files that CME makes available for firms. Firms will be able to download files when they are ready to be retrieved.

PUB: Used for shared files that CME makes available for firms into specific sub-directories. Firms will be able to download files when they are ready to be retrieved from the sub-directories.

Submitting Files to SFTP

The folder will have two sections: Incoming and Outgoing. Files must be dropped for upload into the incoming section, and reports can be pulled from the outgoing section. There will be a response file in the outgoing file which is prefixed with 'res_' to the data file. There is an acknowledgment for each file; if the data is successful the response file will simply contain 'success'. If there are errors the response file will be larger and will contain 'error' and give a detailed message explaining the failure. Duplicate submitted records are rejected with an appropriate error message and for every 1 file submitted into incoming there will be 2 files in outgoing (the original file submitted and the results file). Files dropped in the incoming folder to upload in the TR should be asset class specific.

- All submitted files must be in .csv format.
- All response files will be in .txt format.

File Naming Convention for CSV files

Each file submission must begin with the asset class prefix as shown below, then any free text is allowed to follow to help clients identify their submission activity more effectively. E.g. trade, position, amendments, date etc.

<<AssetClass>>_<<Free Text>>.csv

Examples:

IRS_CLC01_NEWTRD_20190331183400.csv (for Interest Rates)
FX_CLC01_NEWTRD_20190331183400.csv (for FX)
CDS_CLC01_NEWTRD_20190331183400.csv (for Credit)
CMDTY_CLC01_NEWTRD_20190331183400.csv (for Commodity)
EQUITY_CLC01_NEWTRD_20190331183400.csv (for Equity)

CTR Messages Flows

This section illustrates select high level message flows between CME CTR and users.

CME Cleared Trade Submissions to CME TR

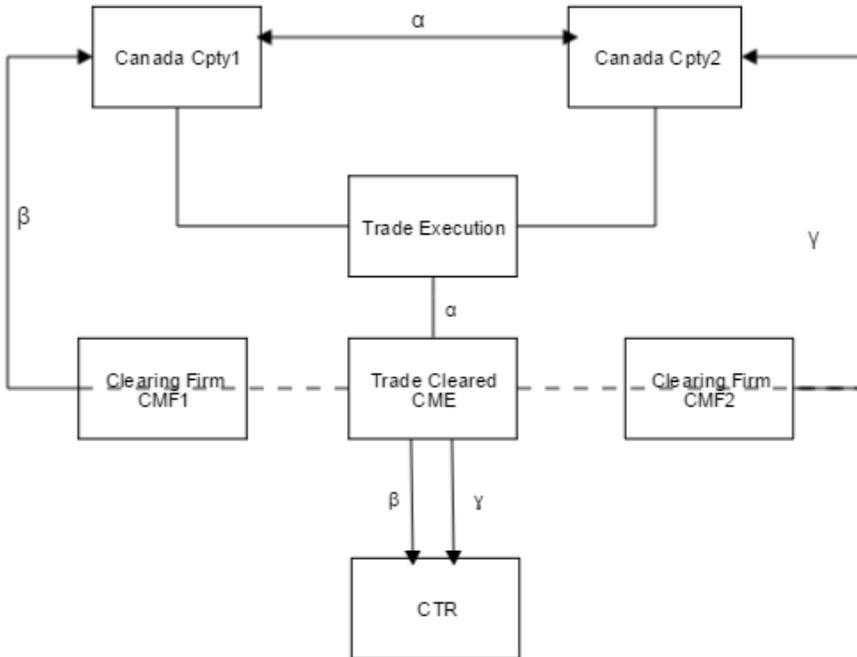
The following diagrams depict the flow when a trade is transacted on a platform, and is subsequently submitted to a clearing agency. It is assumed that initial bilateral trade is submitted to CME CTR and that the cleared novated trades are also submitted to CME CTR. The figures below depict submissions for two scenarios: i) Creation and Lifecycle data are submitted to CME CTR on separate messages, and ii) Creation and Lifecycle data are submitted to CME CTR on the same message.

Agency Clearing Model

Scenario 1

Two Canadian counterparties execute a bilateral (aka 'alpha') transaction intended for clearing and submitted to a Clearing Agency, such as CME Clearing for acceptance. Simultaneously the designated counterparty must report the original bilateral/alpha transaction to a Trade Repository, unless the responsibility has been delegated to a Service Provider. Once the bilateral/alpha trade is accepted for clearing, the transaction is terminated and replaced with two new equal and opposite resulting cleared trades, beta and gamma. Beta and gamma are reported by the Clearing Agency to CME CTR.

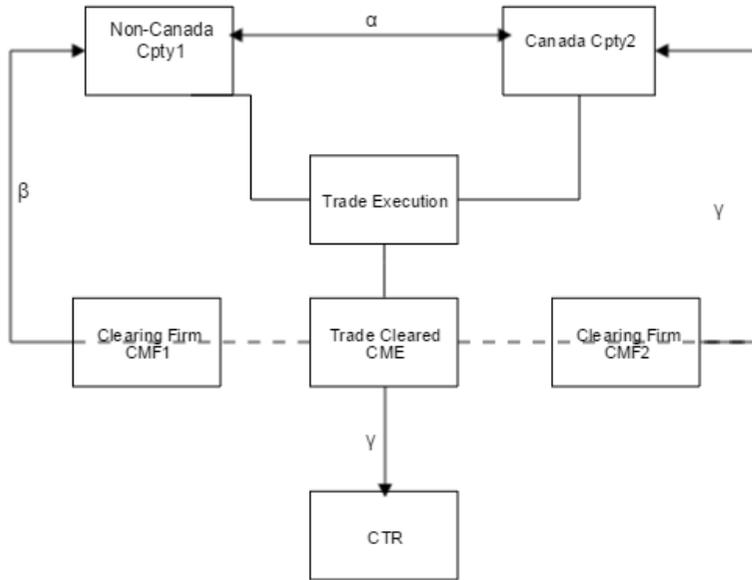
Canadian Counterparty Vs Canadian Counterparty
Trade Cleared CME - (Agency Model)



Scenario 2

A Canadian counterparty and a non-Canadian counterparty execute a bilateral (aka 'alpha') transaction intended for clearing and submitted to a clearing agency such as CME clearing for acceptance. Simultaneously, the Canadian counterparty must report the original bilateral/alpha transaction to a trade repository, unless the responsibility has been delegated to a Service Provider. Once the bilateral/alpha trade is accepted for clearing, the transaction is terminated and replaced with two new equal and opposite resulting cleared trades, beta and gamma. The gamma trade that pertains to the Canadian counterparty is reported by the Clearing Agency to CME CTR and the beta transaction that relates to a non-Canadian entity is not required to be reported under any in force Canadian trade reporting rules.

Non-Canadian Counterparty vs. Canadian Counterparty
Trade Cleared CME - (Agency Model)

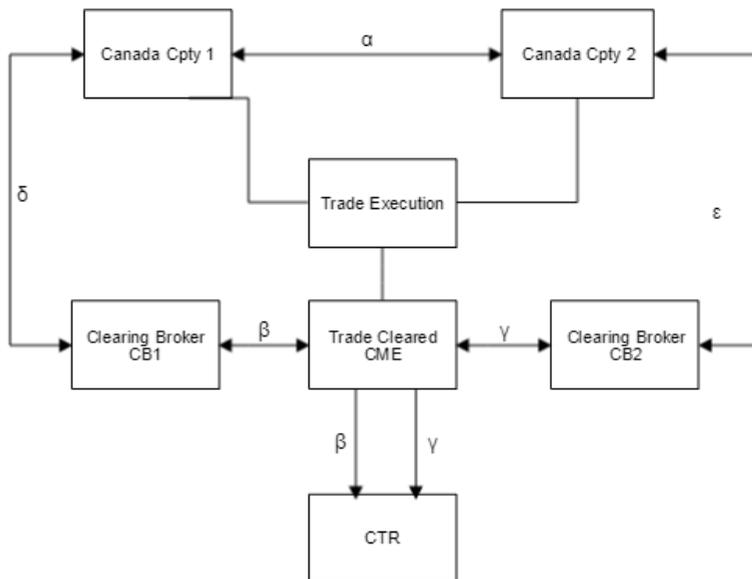


Principal Clearing Model

Scenario 3

Two Canadian counterparties execute a bilateral (aka 'alpha') transaction intended for clearing and submitted to a clearing agency such as CME clearing for acceptance. Simultaneously, the designated Canadian counterparty must report the original bilateral/Alpha transaction to a trade repository, unless the responsibility has been delegated to a Service Provider. Once the bilateral/alpha trade is accepted for clearing, the transaction is terminated and replaced with two new equal and opposite resulting cleared trades, beta and gamma. The clearing agency will report the beta and gamma transactions to CME CTR and will include on the trades reported that CB1 and CB2 are the Principals on the trade.

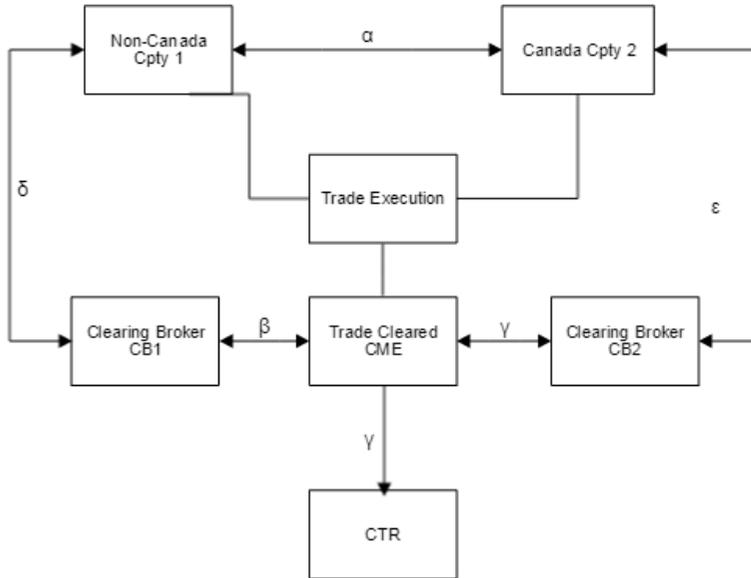
Canadian Counterparty vs Canadian Counterparty
Trade Cleared CME - (Principal Model)



Scenario 4

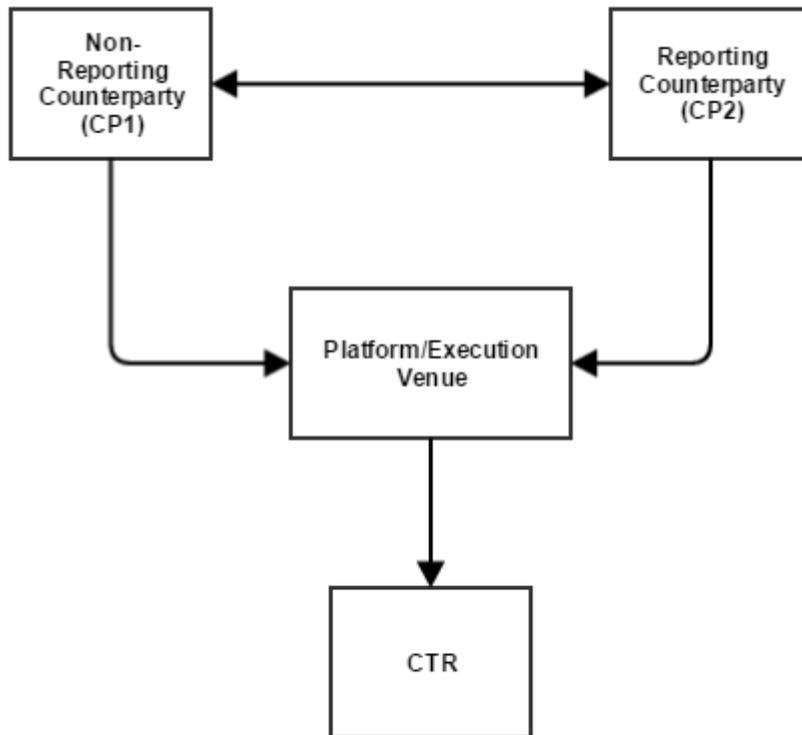
A Canadian counterparty and a non-Canadian counterparty execute a bilateral (aka 'alpha') transaction intended for clearing and submitted to a clearing agency such as CME clearing for acceptance. Simultaneously, the Canadian counterparty must report the original bilateral/Alpha transaction to a trade repository, unless the responsibility has been delegated to a Service Provider. Once the bilateral/alpha trade is accepted for clearing, the transaction is terminated and replaced with two new equal and opposite resulting cleared trades, beta and gamma. The clearing agency will report the beta and gamma transactions to CME CTR and will include on the trades reported that CB1 and CB2 are the Principals on the trade.

Non-Canadian Counterparty vs. Canadian Counterparty
Trade Cleared CME - (Principal Model)



CME Bilateral (Non-Cleared) Trade Submissions to CME CTR

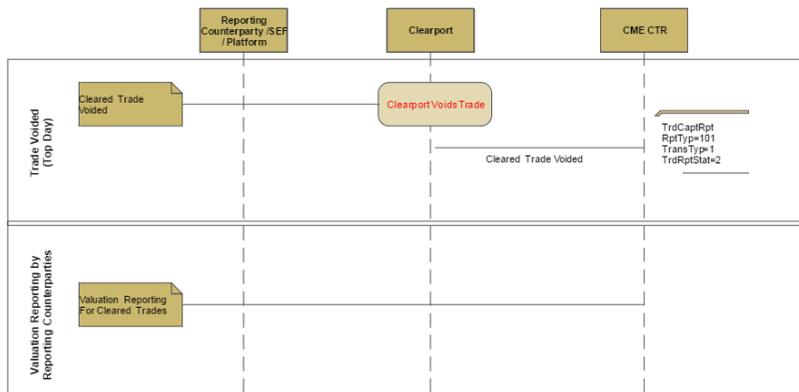
The following diagrams depict the flow in which a bilateral trade is transacted on a platform, and is subsequently reported to the CTR.



Life-Cycle (Continuation) Data Reporting

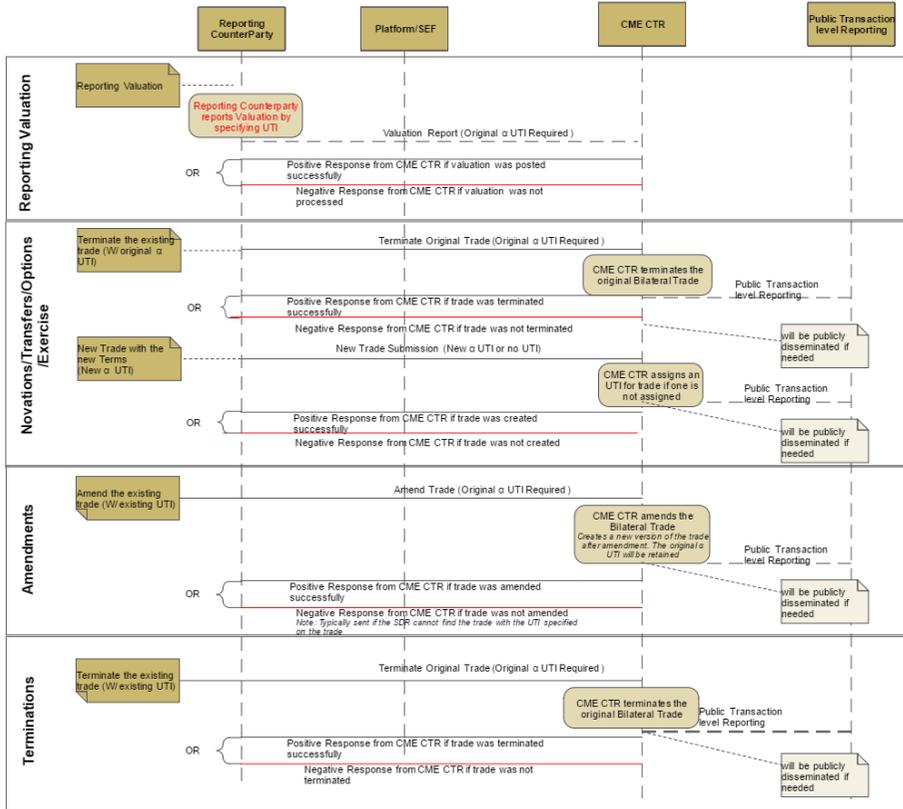
Life-cycle event data reporting can be reported either using the life-cycle approach, or using a snapshot approach. The life-cycle approach involves reporting all life-cycle events affecting the terms of a swap. The snapshot approach requires reporting of a daily snapshot of all primary economic terms of a swap including any changes to such terms occurring since the previous snapshot. The life-cycle event data reporting also includes valuation data.

Reporting Continuation Data for trades cleared at CME



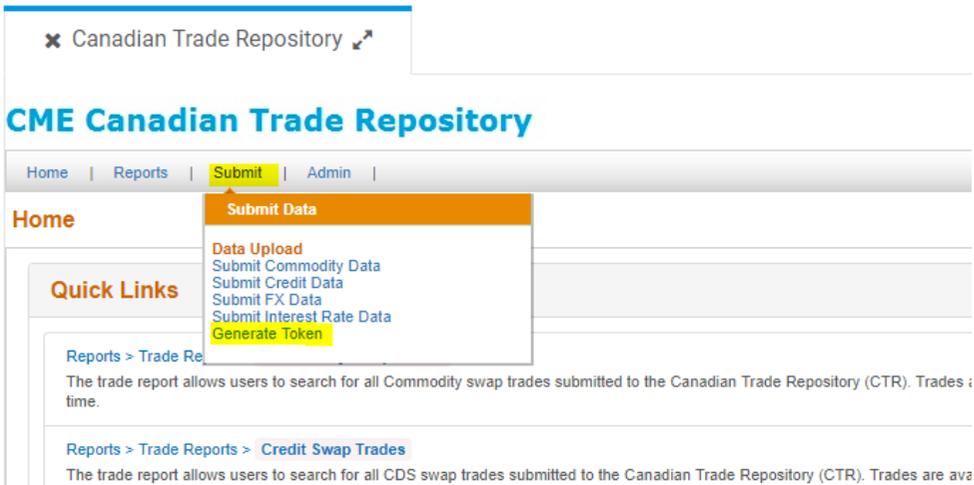
Reporting Continuation Data for all other Trades (Bilateral and Cleared at other Clearing Agencies)

Reporting Continuation Data to CME CTR by Reporting Counterparties/SEF/Platforms



Generate Authentication Token

1. Login to <https://ctrui.cmegroup.com> with your CME Group Login ID and password
2. Navigate to **Submit>Generate Token** menu as shown in screen shot below:



3. Enter your username and password and click “Generate Token”. It should give you your authentication code for using web service in Token text field. You will have to use valid username and password which is authorized by CME Repository Support Group during Registration. (Make sure you have already changed the temporary password provided during registration. You can use <https://ctrui.cmegroup.com/ctrui/> to change your temporary password. It will prompt you to change the password when you login first time)

Generate Token

[Home](#) / [Uploads](#) / [Generate Token](#)

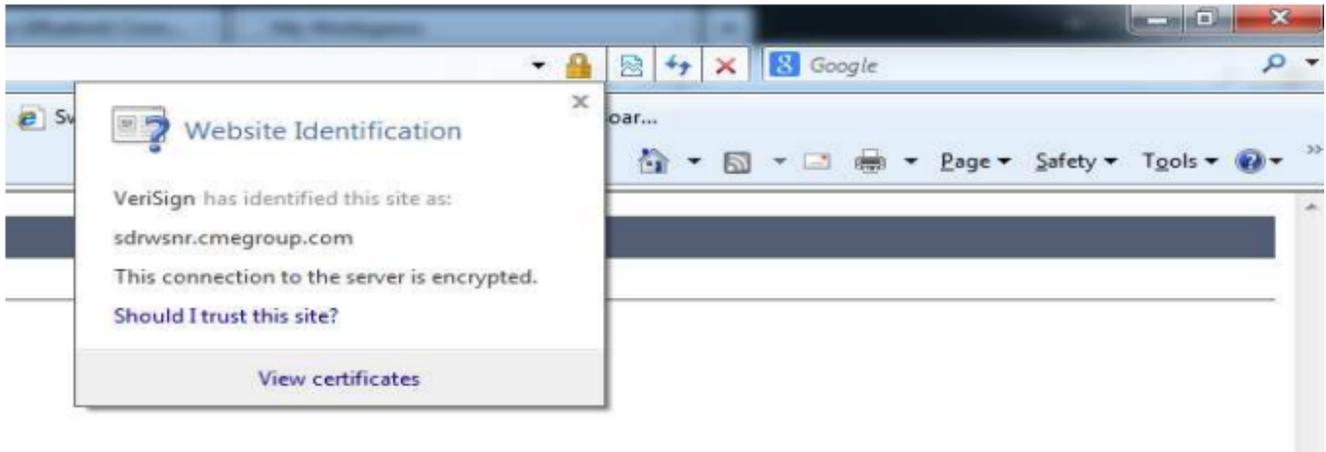
Generate Token

Username :	<input type="text" value="Enter Username"/>
Password :	<input type="password" value="Enter Password"/>
Token :	<input type="text"/>
	<input type="button" value="Generate Token"/>

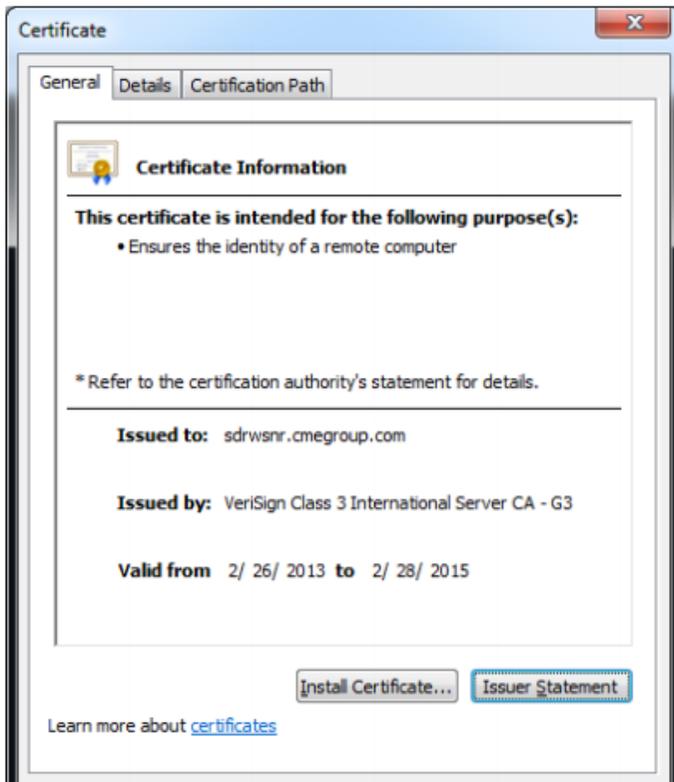
4. You are ready to use this token for your web service client code to submit FIXML or CSV messages to CME TR. This token will be used as a value for http header name "Authorization" (Please refer to DataCaptureWSClient.java code).

Importing Certificate in Local Java Store

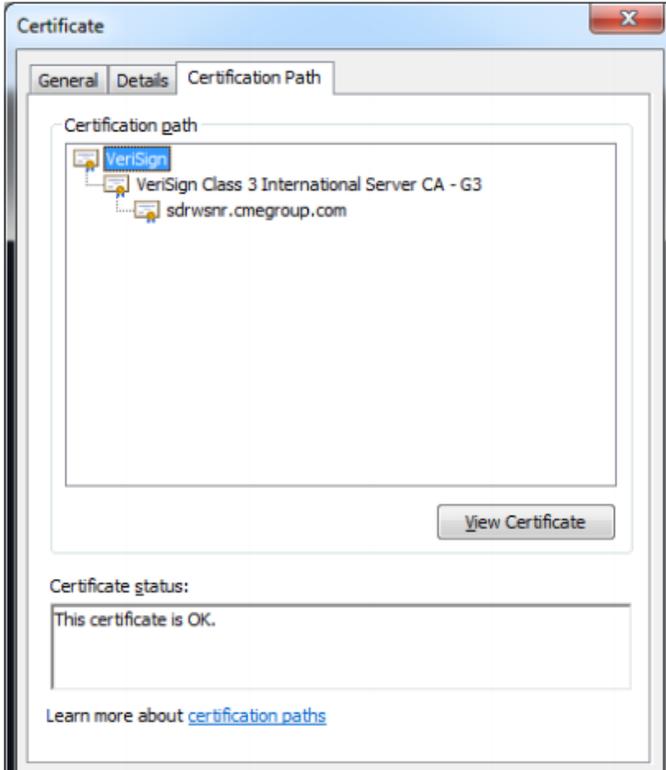
1. Open <https://ctrws.cmegroup.com/datacapture-ws/ctr/submitCSV/CMDTY> URL in IE.
2. Click on Lock image and click on View Certificate. You will see following dialog box



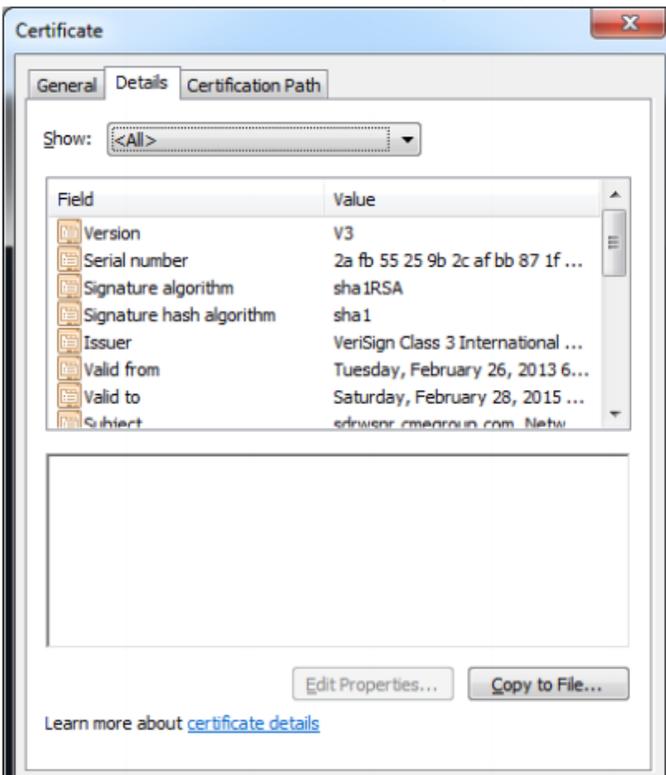
3. Open Certificate Path Tab and select VeriSign as shown in image below.



4. Select Details tab and click “Copy to File” and Click Next



5. Select first format option of “DER encoded binary X.509 (.CER) on “Certificate Export Wizard” dialog and click Next as shown in below screen shot



6. Specify file name and local path to store the certificate on your local machine (e.g C:/etrwsnr.cer)

7. Click Next and Finish. It will save the certificate locally on your machine in C:/etrwsnr.cer file which we will import to your local java keystore.

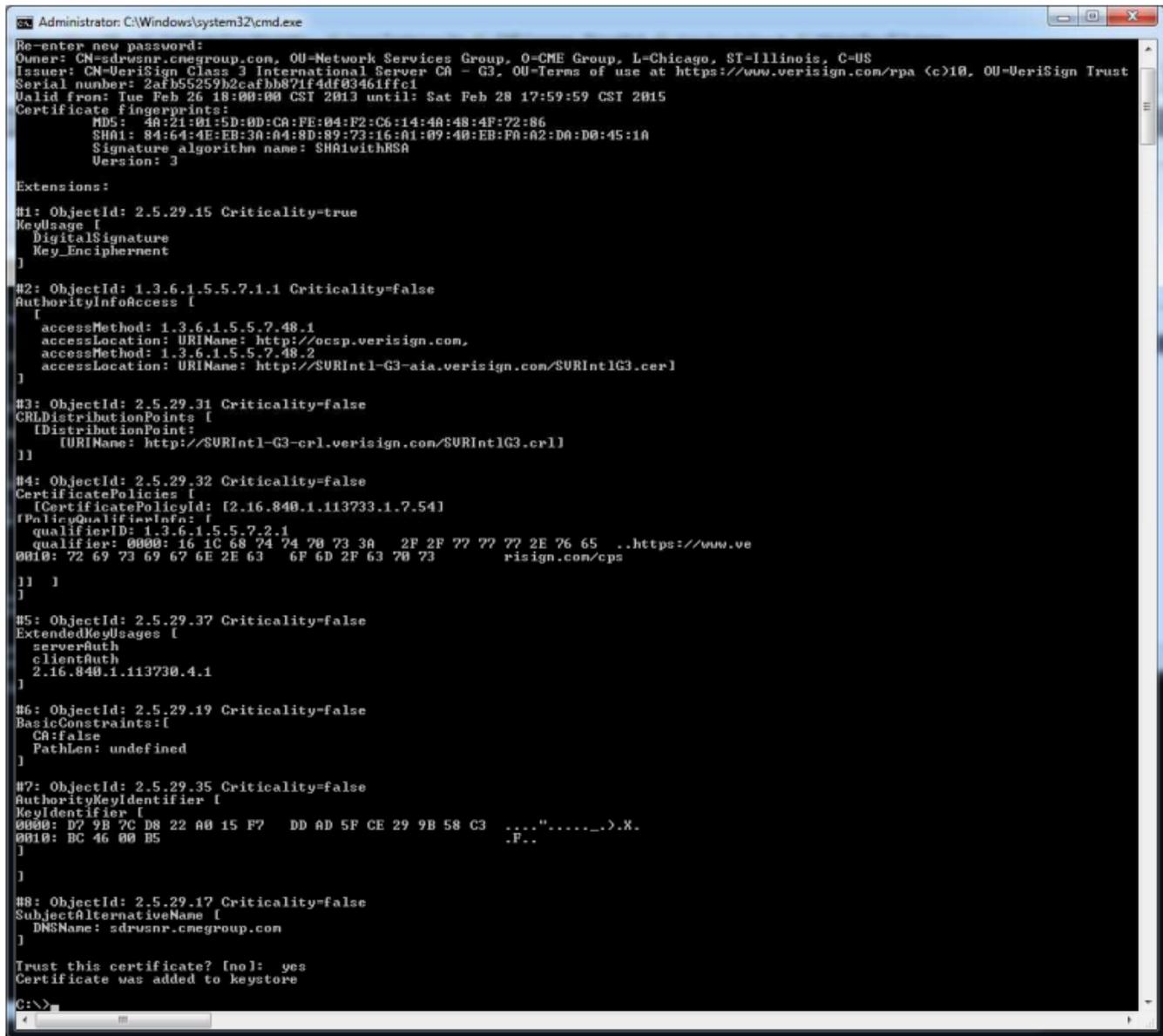
8. Open DOS command window

9. Type following command at DOS prompt to create and import the certificate in local keystore.

```
keytool -import -trustcacerts -alias root -file c:/etrwsnr.cer -keystore c:/etrwsnr.jks
Hit Enter Key
```

10. It will prompt you for password for your keystore. Enter any password which you will be passing later to your Web Service client along with path to the keystore you will be creating (e.g password "trwsnrclient"). Hit enter key. Retype same password and hit enter key again.

11. Type "yes" for Trust this certificate? [no]. Hit enter key. You should see last line as "Certificate was added to keystore" as shown in following screen shot.



```
Administrator: C:\Windows\system32\cmd.exe
Re-enter new password:
Owner: CN=sdrwsnr.cnegroup.com, OU=Network Services Group, O=CME Group, L=Chicago, ST=Illinois, C=US
Issuer: CN=VeriSign Class 3 International Server CA - G3, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust
Serial number: 2afb5259b2cafb871f4df03461ffc1
Valid from: Tue Feb 26 18:00:00 CST 2013 until: Sat Feb 28 17:59:59 CST 2015
Certificate fingerprints:
    MD5: 4A:21:01:5D:0D:CA:FE:04:F2:C6:14:4A:48:4F:72:86
    SHA1: 84:64:4E:EB:3A:A4:8D:89:73:16:A1:09:40:EB:FA:A2:D0:D0:45:1A
    Signature algorithm name: SHA1withRSA
    Version: 3

Extensions:
#1: ObjectID: 2.5.29.15 Criticality=true
KeyUsage [
    DigitalSignature
    Key_Encipherment
]
#2: ObjectID: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
    accessMethod: 1.3.6.1.5.5.7.48.1
    accessLocation: URIName: http://ocsp.verisign.com,
    accessMethod: 1.3.6.1.5.5.7.48.2
    accessLocation: URIName: http://SURIInt1-G3-aia.verisign.com/SURIInt1G3.cer1
]
#3: ObjectID: 2.5.29.31 Criticality=false
CRLDistributionPoints [
    DistributionPoint:
    [URIName: http://SURIInt1-G3-crl.verisign.com/SURIInt1G3.crl]
]
#4: ObjectID: 2.5.29.32 Criticality=false
CertificatePolicies [
    CertificatePolicyId: [2.16.840.1.113733.1.7.54]
    PolicyQualifierInfo: [
    qualifierID: 1.3.6.1.5.5.7.2.1
    qualifier: 0000: 16 1C 68 74 74 70 73 3A 2F 2F 77 77 77 2E 76 65 ..https://www.ve
0010: 72 69 73 69 67 6E 2E 63 6F 6D 2F 63 70 73 risign.com/cps
]
]
#5: ObjectID: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
    serverAuth
    clientAuth
    2.16.840.1.113730.4.1
]
#6: ObjectID: 2.5.29.19 Criticality=false
BasicConstraints:[
    CA:false
    PathLen: undefined
]
#7: ObjectID: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
    KeyIdentifier [
    0000: D7 9B 7C D8 22 A0 15 F7 DD AD 5F CE 29 9B 58 C3 ....".....>.X.
    0010: BC 46 00 B5 .F..
]
]
#8: ObjectID: 2.5.29.17 Criticality=false
SubjectAlternativeName [
    DNSName: sdrwsnr.cnegroup.com
]
Trust this certificate? [no]: yes
Certificate was added to keystore
C:\>
```