#SHAREorg

SHARE
Technology · Connections · Results

Secure Managed File Transfer with Connect:Direct®

Mike Watley

Advisory Software Engineer

IBM Software Group – Industry Solutions

August 16, 2013

Session 13423

SHARE in Boston

Agenda

- What is Secure Plus?
- What are the components of Secure Plus?
- What are the keys to success?
- What elements are required to secure the transfer?
- How should I configure my Secure Plus?

Security Components

- Cryptography
  - Authentication
    - Server Authentication by default
    - Client Authentication is configurable
  - Non-repudiation
    - Digital Signatures & Stats
  - Data integrity
    - Data Encryption/Decryption
  - Data confidentiality
    - Encryption/Decryption with exchanged keys

Secure Plus Components

- Administration Tool
  - Designed to function even if C:D is not initialized
  - Designed as Point-and-Shoot
  - Designed to Run as ISPF/GUI
- Secure Parameter File
  - Secure Local Node record
  - Secure Remote Node record
  - Optional Secure records
    - Secure Client record
    - Secure Password record
    - External Authentication Server record

Secure Plus Components – Continued

- Secure Access File
  - Secures Keys for PARMFILE
  - Restrict Access to this file
    - UACC of None
    - Secure Plus Admin – Update/Alter
    - C:D Task id – Read
- Backup Secure Parameter file & Access file

Secure Plus Protocols

- Transport Layer Security (TLS 1.0)
- Secure Socket Layer (SSL 3.0)
- Station-to-Station (STS)

Keys to Success

- Be Prepared
- Have Completed Worksheet to use as a Guide
- Perform “SAVE AS” Function Often
- Backup Parmfile & Access file

Planning the Configuration

- Review the S+ Implementation Guide
  - Chapter 16 – Definitions of Certificate Parameters
    - Very useful information
- Identify Security Administrator
  - Unix System Services
  - ICSF and Crypto Hardware
  - System Security Application
  - Working knowledge of Connect:Direct®

Assess Your Requirements

- Assess Security Requirements
  - Are you going to use a CA or Self-signed Certificate?
  - Do you need to acquire the Certificate ahead of time?
  - Is Client Authentication required?
  - What protocols are required?
  - What encryption ciphers are required?
  - How many Nodes require Secure Connections?
  - Are Processes allowed to override security settings?

Requirements

- UNIX System Services (USS)
- Access to LE, C/C++ and GSKSSL
  - CEE.SCEERUN (Language Environment)
  - CEE.SCEERUN2 (XPLINK Requirement)
  - CBC.SCLBDLL (C/C++ Run-time)
  - SYS1.SIEALNKE (System SSL)
- OMVS access
  - Home Directory

Additional Requirements for SSL/TLS

- Access to Key database or Keyring/Key Store
  - Gskkyman kdb
    - Full pathname and password
      - *i.e. /u/userid/MYCertFile.kdb*
    - Keyring Name
- Self-signed or CA Certificate
  - Label name
  - CA Root Certificate
- Client Authentication
  - Certificate's Common Name

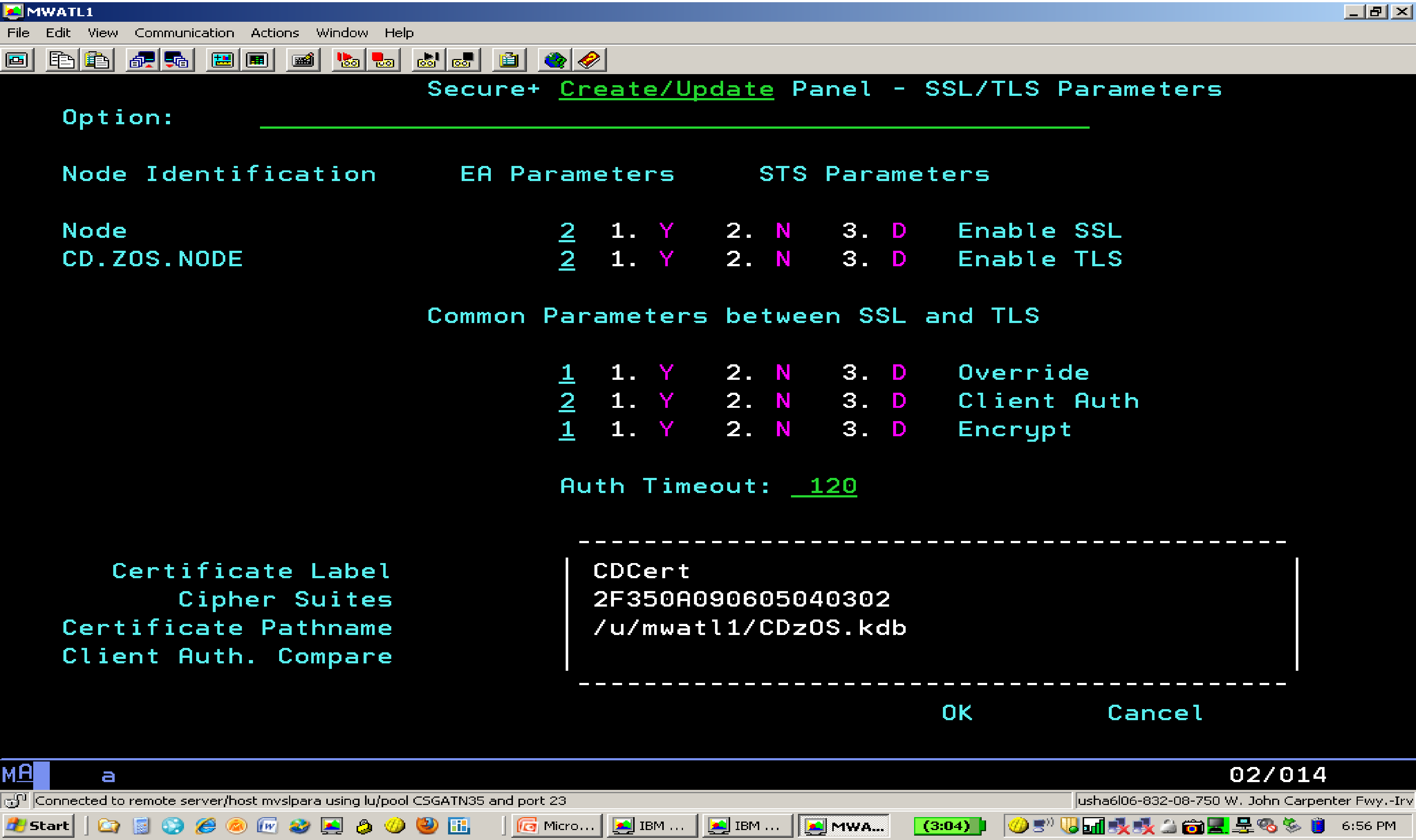
Configure Secure Nodes - Local Record

- Import from NETMAP or Manual Entry
- Define Secure LOCAL Node record with DEFAULTS
  - Enable Override
  - Disable All Protocol specific switches
  - Define Certificate Label
  - Define Cipher Suites
  - Define Certificate Pathname
  - Create Auth Pub key
  - Create Sig Pub key

Configure the Remote Record

- Define Secure REMOTE Node record with Overrides
  - Enable, Disable and Define Appropriate Overrides
    - Override
    - Autoupdt
    - Enable Any Protocol specific switches
    - Define Certificate Label
    - Define Cipher Suites
    - Create Auth Pub key
    - Create Sig Pub key
- Inappropriate Settings for Secure Remote Node record
  - Certificate Pathname
  - External Auth Server

Sample Configuration - Local Record

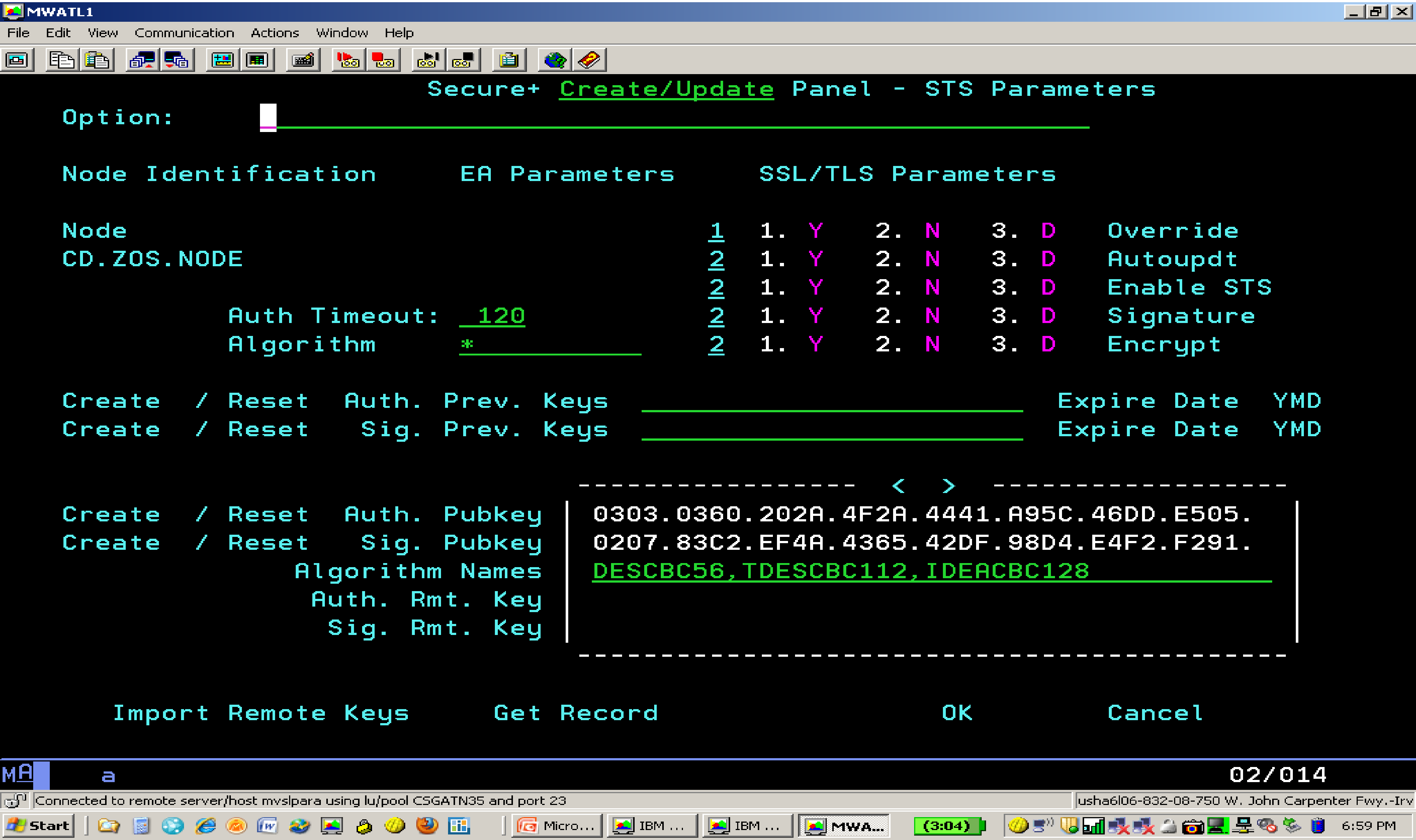


```
                 Secure+ Create/Update Panel - SSL/TLS Parameters
  Option: ___________________________________________________

  Node Identification     EA Parameters     STS Parameters

  Node                          2  1. Y   2. N   3. D   Enable SSL
  CD.ZOS.NODE                   2  1. Y   2. N   3. D   Enable TLS

                        Common Parameters between SSL and TLS

                                1  1. Y   2. N   3. D   Override
                                2  1. Y   2. N   3. D   Client Auth
                                1  1. Y   2. N   3. D   Encrypt

                                Auth Timeout:  120

                                 -------------------------------------------
     Certificate Label          | CDCert                                    |
         Cipher Suites          | 2F350A090605040302                        |
  Certificate Pathname          | /u/mwatl1/CDzOS.kdb                       |
  Client Auth. Compare          |                                           |
                                 -------------------------------------------
                                                    OK         Cancel

MA      a                                                              02/014
```

Connected to remote server/host mvslpara using lu/pool CSGATN35 and port 23

usha6l06-832-08-750 W. John Carpenter Fwy.-Irv

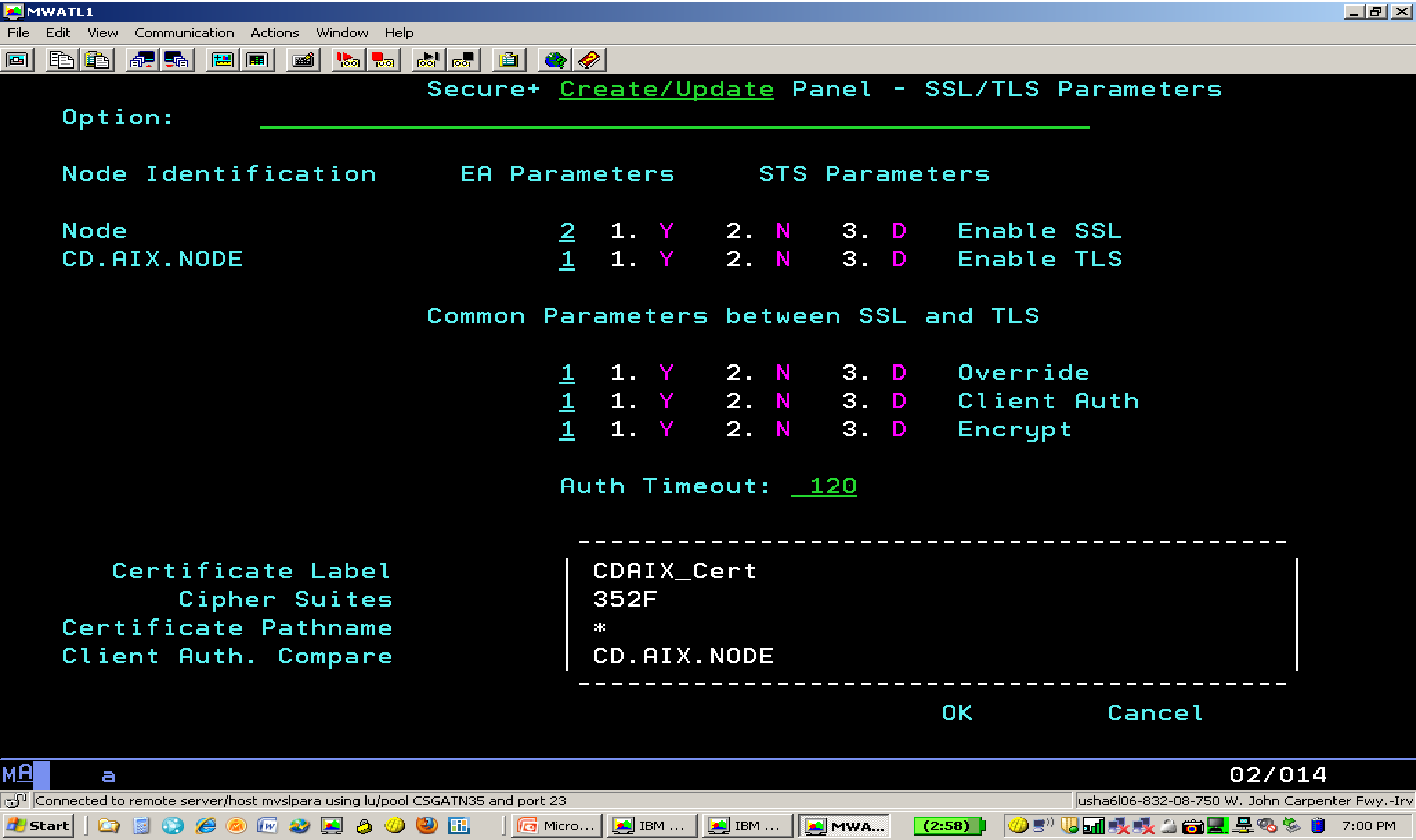
Sample Configuration - Local Record



```
                      Secure+ Create/Update Panel - STS Parameters
Option:     _

Node Identification     EA Parameters     SSL/TLS Parameters

Node                                   1  1. Y  2. N  3. D  Override
CD.ZOS.NODE                            2  1. Y  2. N  3. D  Autoupdt
                                       2  1. Y  2. N  3. D  Enable STS
          Auth Timeout: _120           2  1. Y  2. N  3. D  Signature
          Algorithm     *              2  1. Y  2. N  3. D  Encrypt

Create / Reset  Auth. Prev. Keys  ______________________  Expire Date  YMD
Create / Reset   Sig. Prev. Keys  ______________________  Expire Date  YMD

                               -------------------  <  >  -------------------
Create / Reset  Auth. Pubkey  | 0303.0360.202A.4F2A.4441.A95C.46DD.E505.   |
Create / Reset   Sig. Pubkey  | 0207.83C2.EF4A.4365.42DF.98D4.E4F2.F291.   |
              Algorithm Names | DESCBC56,TDESCBC112,IDEACBC128             |
               Auth. Rmt. Key |                                            |
                Sig. Rmt. Key |                                            |
                               ---------------------------------------------

   Import Remote Keys     Get Record                 OK         Cancel

MA     a                                                                02/014
```

Connected to remote server/host mvslpara using lu/pool CSGATN35 and port 23 | usha6l06-832-08-750 W. John Carpenter Fwy.-Irv

Sample Configuration - Remote Record

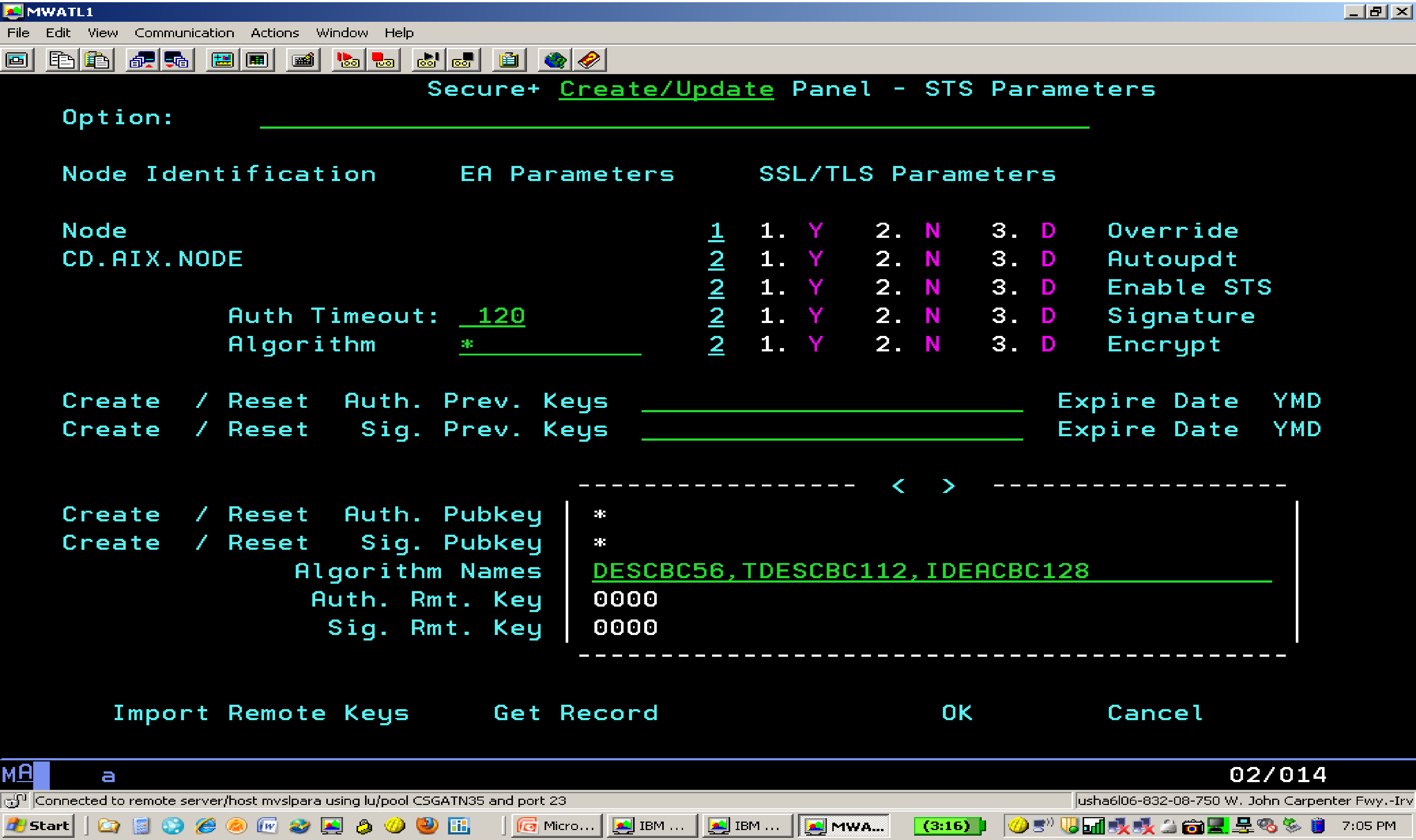


```
                 Secure+ Create/Update Panel - SSL/TLS Parameters
  Option: ________________________________________________

  Node Identification      EA Parameters     STS Parameters

  Node                                2  1. Y   2. N   3. D   Enable SSL
  CD.AIX.NODE                         1  1. Y   2. N   3. D   Enable TLS

                          Common Parameters between SSL and TLS

                                      1  1. Y   2. N   3. D   Override
                                      1  1. Y   2. N   3. D   Client Auth
                                      1  1. Y   2. N   3. D   Encrypt

                                      Auth Timeout: _120

                                   -------------------------------------------
     Certificate Label             | CDAIX_Cert                               |
         Cipher Suites             | 352F                                     |
  Certificate Pathname             | *                                        |
  Client Auth. Compare             | CD.AIX.NODE                              |
                                   -------------------------------------------
                                                       OK        Cancel

MA      a                                                              02/014
```

Connected to remote server/host mvslpara using lu/pool CSGATN35 and port 23

usha6l06-832-08-750 W. John Carpenter Fwy.-Irv

Sample Configuration - Remote Record



```
                  Secure+ Create/Update Panel - STS Parameters
   Option: __________________________________________________

   Node Identification      EA Parameters     SSL/TLS Parameters

   Node                                       1  1. Y  2. N  3. D   Override
   CD.AIX.NODE                                2  1. Y  2. N  3. D   Autoupdt
                                              2  1. Y  2. N  3. D   Enable STS
             Auth Timeout: _120               2  1. Y  2. N  3. D   Signature
             Algorithm     *__________        2  1. Y  2. N  3. D   Encrypt

   Create  / Reset  Auth. Prev. Keys ________________________  Expire Date  YMD
   Create  / Reset   Sig. Prev. Keys ________________________  Expire Date  YMD

                                  -----------------  <  >  -----------------
   Create  / Reset  Auth. Pubkey | *
   Create  / Reset   Sig. Pubkey | *
                 Algorithm Names | DESCBC56,TDESCBC112,IDEACBC128__________
                  Auth. Rmt. Key | 0000
                   Sig. Rmt. Key | 0000
                                  -----------------------------------------

      Import Remote Keys     Get Record                OK         Cancel

MA     a                                                              02/014
Connected to remote server/host mvslpara using lu/pool CSGATN35 and port 23    usha6l06-832-08-750 W. John Carpenter Fwy.-Irv
```

Securing the Connection

- During Process execution
  - Secure Parameter File read to obtain security parameters
    - Remote record does not exist and Local record enabled overrides and does not enable a Secure protocol,
      - *continue as a non-secure connection*
    - Parameters from Local and Remote records are merged
      - *No enabled protocol results in non-secure connection*
    - Apply Process overrides, if allowed

Securing the Connection

- During Process execution - Continued
  - After an initial application exchange, SSL handshake is performed
    - Performed by System SSL using C:D callback routines
    - On successful handshake
      - *Optional verification of Common Name string and/or Sterling External Authentication Server*
      - *All further communications is over a secured connection*

Summary

- Be Prepared, Be Patient
- Have the Completed Worksheet to use as a Guide
- Define Local Record with Defaults
- Define Remote Record with Appropriate Overrides
- Don’t Hesitate to ask for Help

Question and Answer