測試手冊

相關問題說明

一、如何判斷是否有用到 ICS 服務？

1. 若貴單位為正副本受文者，即代表曾以貴單位名義申請開通 ICS 服務。
2. 若系統在註冊或登入等步驟，需要讀取使用者自然人憑證卡並核對到使用者完整身份證字號，則有可能是使用 ICS 服務。
3. 若仍無法確認，請將本公文及附件提供給貴單位的系統開發人員或系統開發廠商協助確認。

二、如果有用到 ICS 服務但未配合更換憑證？

可能會導致系統無法執行登入或註冊等動作。

三、有用到 ICS 的系統要在什麼時候配合更換作業？

本部預計於**民國 109 年 7 月 4 日(星期六)中午 12:00-12:10** 更換 SSL 憑證，屆時 ICS 服務會中斷 10 鐘。建議各系統同步於 7 月 4 日中午 12:10 過後立即作業，若提前或延後可能導致系統無法正常運作。

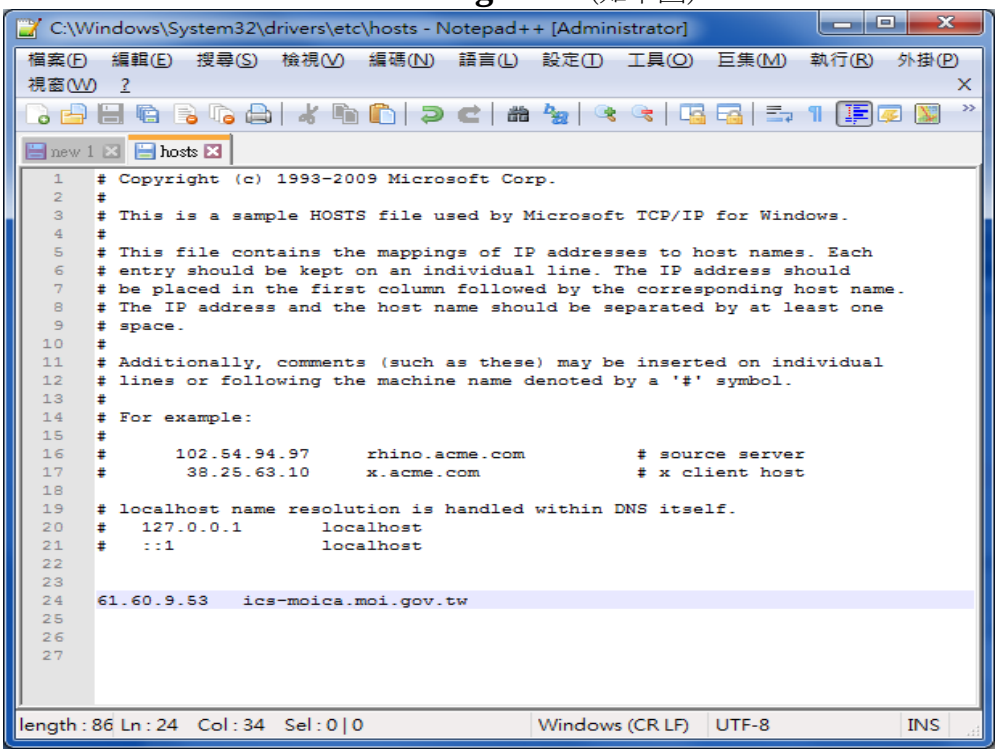
四、新 ICS domain：**ics-moica.moi.gov.tw**

ICS 連線環境設定說明

一、 測試環境設定：

更改測試主機作業系統(WINDOWS/Linux) etc**hosts** 內容，請加入設定：

61.60.9.53　ics-moica.moi.gov.tw (如下圖)



[注意!] **正式環境的主機請勿加入 hosts 設定**!以上設定只供測試機使用。

二、 新增身分確認服務系統主機 SSL 連線通道 GTLSCA 的 SSL 憑證鏈資訊(正式環境及測試環境皆需設定)

(一) 使用 C 語言 API：

1. 先將原本 ICS 主機的 IP：61.60.9.50 →改成 domin： **ics-moica.moi.gov.tw**
2. 將原本舊的 SSL 憑證鏈資訊檔案(GCA.pem)更新為新檔案(GTLSCA.pem)
   例如：

```
char ip[] = "ics-moica.moi.gov.tw";
char serverCA[] = "GTLSCA.pem";//指定檔案路徑位置 原本GCA.pem --> GTLSCA.pem
//連結到ICS伺服器
iRet =  iSSL_SendThenRecv(ip, "443", serverCA, url , SzRetPKT.Length, SzRetPKT,
& reszRetPKT_len, & reszRetPKT);
if (iRet != 0) // error
```

3. .pem 檔案下載連結： https://api-hisecurecdn.cdn.hinet.net/icsexample/GTLSCA.zip

(二) 使用 Java 語言 API：

1. 先將原本 ICS 主機的 IP：61.60.9.50 →改成 domin： **ics-moica.moi.gov.tw**
2. Java CertStore 憑證匯入

I. 請至 GTLSCA 網站下載已經壓縮打包好的憑證串鏈檔案，下載網址為 ：https://api-hisecurecdn.cdn.hinet.net/icsexample/GTLSCA_All.zip ， 將 GTLSCA.crt 拷貝到<JAVA_HOME>/jre/lib/security 的目錄下。

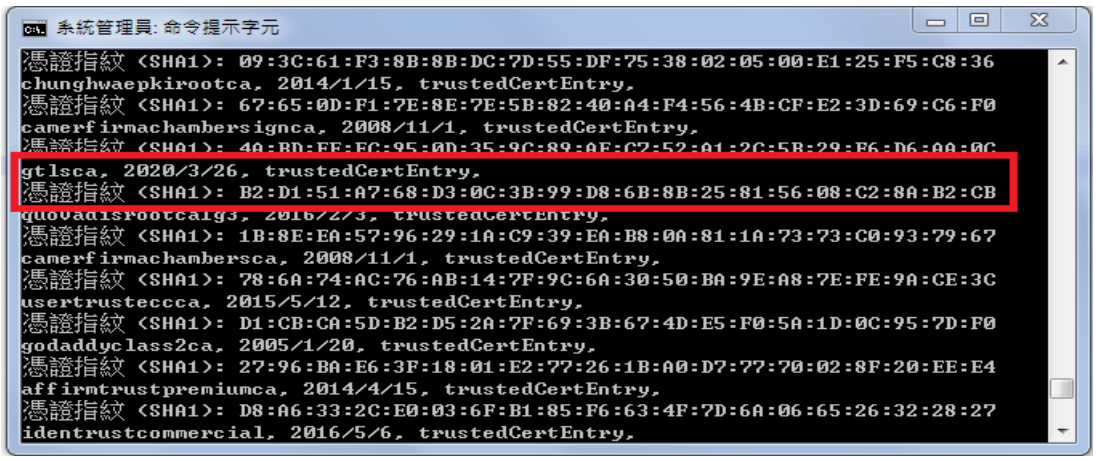
II. 開啓 Dos 視窗並變更目錄到<JAVA_HOME>/jre/lib/security。執行以下命令：

(預設密碼為 changeit)

keytool -import -file GTLSCA.crt -alias gtlsca -keystore cacerts -trustcacerts

註：若要查看剛剛滙入的 GTLSCA 憑證(別名即為 gtlsca)，可執行以下指令： (預設密碼為 changeit)

keytool -list -keystore cacerts



(三) 測試身分確認服務連線：

請注意，測試主機只供連結測試，故查詢不會回應請求資訊的結果，只會回應 1022 訊息(ERR_ConnectDB_Fail,連線到資料庫失敗)、或是 1020 訊息 (ERR_ClientID_Incorrect,系統不認可的 ClientID,系統無此 ClientID 的資訊)，出現以上回應訊息，即代表身分確認服連線成功了。

錯誤訊息排除方式

1. 使用 Java 語言如果出現下圖錯誤訊息表示尚未更改 host 設定

```
SERIALNUMBER=0000000010056812, CN=61.60.9.50, OU=資訊中心, OU=內政部, O=行政院, L=臺灣, C=TW
java.io.IOException: HTTPS hostname wrong:  should be <ics-moica.moi.gov.tw>
        at sun.net.www.protocol.https.HttpsClient.checkURLSpoofing(Unknown Source)
        at sun.net.www.protocol.https.HttpsClient.afterConnect(Unknown Source)
        at sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(Unknown Source)
        at sun.net.www.protocol.http.HttpURLConnection.getOutputStream0(Unknown Source)
        at sun.net.www.protocol.http.HttpURLConnection.getOutputStream(Unknown Source)
        at sun.net.www.protocol.https.HttpsURLConnectionImpl.getOutputStream(Unknown Source)
        at tw.com.chttl.ics.ICSCJApi.iSSL_SendThenRecv(ICSCJApi.java:190)
        at tw.com.chttl.ics.ICSCJApi.iQuery(ICSCJApi.java:415)
        at icscjtest.main(icscjtest.java:222)
```

2. 使用 Java 語言如果出現下圖訊息表示尚未匯入 GTLSCA.crt 到 <JAVA_HOME>/jre/lib/security/cacerts，請參考匯入方式。

```
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException:
d valid certification path to requested target
        at sun.security.ssl.Alerts.getSSLException(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.fatal(Unknown Source)
        at sun.security.ssl.Handshaker.fatalSE(Unknown Source)
        at sun.security.ssl.Handshaker.fatalSE(Unknown Source)
        at sun.security.ssl.ClientHandshaker.serverCertificate(Unknown Source)
        at sun.security.ssl.ClientHandshaker.processMessage(Unknown Source)
        at sun.security.ssl.Handshaker.processLoop(Unknown Source)
        at sun.security.ssl.Handshaker.process_record(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.readRecord(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)
        at sun.security.ssl.SSLSocketImpl.startHandshake(Unknown Source)
        at sun.net.www.protocol.https.HttpsClient.afterConnect(Unknown Source)
        at sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(Unknown Source)
        at sun.net.www.protocol.http.HttpURLConnection.getOutputStream0(Unknown Source)
        at sun.net.www.protocol.http.HttpURLConnection.getOutputStream(Unknown Source)
        at sun.net.www.protocol.https.HttpsURLConnectionImpl.getOutputStream(Unknown Source)
        at tw.com.chttl.ics.ICSCJApi.iSSL_SendThenRecv(ICSCJApi.java:190)
        at tw.com.chttl.ics.ICSCJApi.iQuery(ICSCJApi.java:415)
        at tw.com.chttl.ics.icscjtest.icscjtest.main(icscjtest.java:237)
Caused by: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certi
 to requested target
        at sun.security.validator.PKIXValidator.doBuild(Unknown Source)
        at sun.security.validator.PKIXValidator.engineValidate(Unknown Source)
        at sun.security.validator.Validator.validate(Unknown Source)
        at sun.security.ssl.X509TrustManagerImpl.validate(Unknown Source)
        at sun.security.ssl.X509TrustManagerImpl.checkTrusted(Unknown Source)
        at sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(Unknown Source)
        ... 16 more
Caused by: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
        at sun.security.provider.certpath.SunCertPathBuilder.build(Unknown Source)
```

3. 使用 C 語言呼叫 **iSSL_SendThenRecv** 函式回傳代碼出現 **-12**，表示尚未修改 host 設定或尚未指定新的 SSL 憑證鏈資訊檔案(GTLSCA.pem)