설정 및 보안 가이드 문서

# WebtoB, WebtoB Proxy

# 서버 클라이언트 상호 인증 가이드

IMS 107342
2016. 01.22

# 목차

# WebtoB ProxySSL, WebtoB Server 상호인증 설정 및 테스트 가이드

최근 사이버 공격은 대부분 홈페이지 보안 취약점을 악용한 해킹을 통해 정보시스템 파괴, 개인정보 유출, 홈페이지 위·변조 등의 피해를 발생시켜 정보시스템을 운영하는 기관의 대외 신뢰 하락과 많은 손실을 끼치고 있습니다. 이에 따라, 홈페이지 관리자는 홈페이지 및 웹 서버에서 발생하는 보안취약점에 대한 점검과 대응방안에 대해 숙지하고 미리 제거해 홈페이지 서비스의 안전성과 신뢰성을 확보하는 것이 매우 중요합니다. 본 가이드는 WebtoB를 기준으로 다른 웹 서버와 상호인증에 대한 설정 방법을 담고 있으며 해당 설정에 대한 옵션 설명이 일부 포함되어 있습니다. 해당 테스트는 WebtoB 4.1.8.1 -B291.33.0 이상 버전으로 테스트 되었습니다.

## 1. 테스트 인증서 생성

### 1.1 CertificateKey, CACertificateFile, PrivateKey

#### *1. 테스트 인증서 성생 및 WebtoB 버전 안내*

***x509 타입의 인증서를 통해 웹서버 간 상호 클라이언트 인증서를 요구할 수 있습니다.***

테스트 인증서 및 내부 어플리케이션 체계를 위한 용도라면 굳이 돈을 주고 GPKI(Government Public Key Infrastructure) 와 같은 공개키 기반 구조의 인증서를 발급 받으실 필요가 없습니다. WebtoB 에서는 WBSSL을 통해 테스트 인증서를 생성하는 방법을 제공하고 있습니다. 다음 안내하는 WebtoB의 환경설정은 WebtoB 4.1.8.0 이상의 버전에서 수행하였습니다.

#### *2. 테스트 인증서 생성 절차*

1) WebtoB가 설치된 cmd 창에서 아래의 절차를 수행합니다. 인증서를 생성하는 방법은 다양하지만 본 문서에서는 아래의 내용을 따르도록 하겠습니다. 아래의 명령어로 하나의 키 쌍을 생성한 후 생성된 newcert.pem 파일에서 PublicKey와 PrivateKey의 내용을 분리합니다.

$>wbssl req -config C:₩TmaxSoft₩WebtoB4.1₩ssl₩wbssl.cnf -new -x509 -keyout newcert.pem -out newcert.pem -days 365

```
C:₩Users₩lim>CA -newcert

C:₩Users₩lim>wbssl req -config C:₩TmaxSoft₩WebtoB4.1₩ssl₩wbssl.cnf -new -x509 -keyout newcert.pem -out newcert.pem -days 365
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
..............................................................................................+++
.....................................................................................................+++
writing new private key to 'newcert.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

2) 위에서 생성한 newcert.pem 내용에서 -----BEGIN ENCRYPTED PRIVATE KEY----- 에서 -----END ENCRYPTED PRIVATE KEY----- 내용까지 별도의 파일로 NewPrivateKey.txt 로 저장합니다. 생성된 개인키를 통해 CA 인증서를 생성할 것 입니다. 아래의 명령어로 CA 인증서를 생성하기 위한 CSR 요청 파일을 생성합니다.

$>wbssl req -new -key NewPrivateKey.txt -out ca.csr

```
C:₩TmaxSoft₩WebtoB4.1₩ssl>wbssl req -new -key NewPrivateKey.txt -out ca.csr
Enter pass phrase for NewPrivateKey.txt:
Loading 'screen' into random state - done
```

3) 생성된 ca.csr 은 미리 생성된 NewPrivateKey.txt 파일로 인증하여 ca.crt 즉 자가 인증된 셀프 인증서를 생성할 수 있습니다.

$>wbssl x509 -req -days 1280 -in ca.csr -signkey NewPrivateKey.txt -out ca.crt

```
C:₩TmaxSoft₩WebtoB4.1₩ssl>wbssl x509 -req -days 1280 -in ca.csr -signkey NewPrivateKey.txt -out ca.crt
Loading 'screen' into random state - done
Signature ok
subject=/C=KR/O=Tmax Ltd/CN=reverse.co.kr
Getting Private key
Enter pass phrase for NewPrivateKey.txt:
```

4) 각 웹 서버의 CACertificateFile이 완성되었습니다. 각 WebtoB의 설정에 다음의 환경설정에 추가될 것 입니다.

$>WebtoB Proxy(클라이언트) 환경설정 경로 : $WEBTOBDIR/config/http.m
$>WebtoB(Server) 환경설정 경로 : $WEBTOBDIR/config/http.m

5) 서버인증서(server.crt)를 기존의 NewPrivateKey.txt 를 통해 요청파일(csr)을 만들고 해당 csr을 통해 서버인증서(server.crt)를 만들고 위에서 만들어진 ca.crt 인증서를 통해 자가 인증하는 방법을 안내합니다.

$>wbssl req -new -key NewPrivateKey.txt -out server.csr
$>wbssl x509 -req -in server.csr -out server.crt -signkey NewPrivateKey.txt -CA ca.crt -CAkey NewPrivateKey.txt -CAcreateserial -days 365

```
C:₩TmaxSoft₩WebtoB4.1₩ssl>wbssl req -new -key NewPrivateKey.txt -out server.csr
Enter pass phrase for NewPrivateKey.txt:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
```

.

```
C:₩TmaxSoft₩WebtoB4.1₩ssl>wbssl x509 -req -in server.csr -out server.crt -signkey NewPrivateKey.tx
l -days 365
Loading 'screen' into random state - done
Signature ok
subject=/C=KR/O=Tmax Ltd/CN=reverse.ssl.co.kr
Getting Private key
Enter pass phrase for NewPrivateKey.txt:
Getting CA Private Key
Enter pass phrase for NewPrivateKey.txt:
```

6) 개인키에 적용된 패스워드를 제거하는 방법입니다. 윈도우용 아파치에만 적용하고 WebtoB에는 적용하지 않습니다. 아래의 명령어를 입력해주지 않으면 아파치 기동 시 정의되지 않는 패스워드로 인해 기동이 실패합니다. 개인키 패스워드를 삭제하지 않고 기동하는 방법도 있기 때문에 다른 문서를 참조하여 설정하시기 바랍니다.

$>wbssl rsa -in NewPrivateKey.txt -out NewPrivatekey2.txt

```
C:₩TmaxSoft₩WebtoB4.1₩ssl>wbssl rsa -in NewPrivateKey.txt -out NewPrivatekey2.txt
Enter pass phrase for NewPrivateKey.txt:
writing RSA key
```

7) 최종적으로 아래의 파일이 생성 되었습니다.

$>server.crt, ca.crt, NewPrivateKey2.txt

```
 C:₩TmaxSoft₩WebtoB4.1₩ssl 디렉터리

2015-11-22  오후 02:45             1,078 server.crt

 C:₩TmaxSoft₩WebtoB4.1₩ssl 디렉터리

2015-11-22  오후 02:36             1,074 ca.crt

 C:₩TmaxSoft₩WebtoB4.1₩ssl 디렉터리

2015-11-22  오후 02:57             1,675 NewPrivatekey2.txt
               3개 파일               3,827 바이트
               0개 디렉터리  413,576,658,944 바이트 남음
```

# 2. 환경설정

## 2.1 WebtoB, WebtoB Proxy 환경설정

### *1. WebtoB와 WebtoB Proxy의 최종설정 요약*

*상호인증 설정을 위한 최소 절차*

공공기술의 보안 향상이 대두되면서 각 제품군은 클라이언트를 식별하기 위한 강화된 보안기술을 제공합니다. 본 문서에서는 상호 인증을 위한 상호 인증 설정을 다루고 있기 때문에 그 밖에 SSL 설정에 대한 내용은 별도의 문서를 참조하시기 바랍니다.

### *2. WebtoB http.m 설정 및 WebtoB Proxy http.m 설정*

1) WebtoB Proxy Client 설정경로 : $WEBTOBDIR/config/http.m

tmax@TAC1:~/webtob/config

```
*VHOST
limpc_vhost     DOCROOT="/home/tmax/webtob/docs",
                PORT = "8080",
                NODENAME = "$(NODENAME)",
                HOSTNAME = "client.test.co.kr",
                HOSTALIAS = "192.168.41.151,127.0.0.1",
                ERRORDOCUMENT = "503",
                LOGGING = "log1",
                ERRORLOG = "log2"

*REVERSE_PROXY
limpc_reverse
                ServerAddress = "192.168.41.140:4430",
                PathPrefix = "/",
                ServerPathPrefix = "/",
                ProxySSLFlag = Y,
                ProxySSLName = client_ssl

*PROXY_SSL
client_ssl      Verify = 2,
                VerifyDepth = 3,
                CACertificateFile="$(WEBTOBDIR)/ssl/ca.crt",
                CertificateChainFile="$(WEBTOBDIR)/ssl/fake/CHAIN.crt",
                CertificateFile="$(WEBTOBDIR)/ssl/server.crt",
                CertificateKeyFile="$(WEBTOBDIR)/ssl/NewPrivateKey.txt",
                Protocols = "-SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2",
                RequiredCiphers = "HIGH:MEDIUM:!aNULL:!MD5"
```

※ RequiredCiphers 를 동일하게 맞춰주시기 바랍니다. 해당 값이 다른 경우 키 교환이 정상적으로 이루어지지 않을 수 있습니다.
※ 아래는 클라이언트가 되는 WebtoB의 입장에서 Proxy SSL Verify에 관한 설명입니다.

| 레벨 | 설명 |
|---|---|
| 0 | 내부 서버의 인증서 인증 과정을 진행하지 않는다. |
| 1 | 내부 서버는 사용 가능한 인증을 보여 주어야 하며 WebtoB가 내부 서버의 인증서를 받은 경우 인증서 인증 과정을 진행한다. |
| 2 | 내부 서버는 사용 가능한 인증을 반드시 보여 주어야 하며 WebtoB가 내부 서버의 인증서 인증 과정을 진행한다. |
| 3 | 내부 서버는 사용 가능한 인증을 보여 주어야 하며 WebtoB가 인증서를 가지고 있지 않은 상황에서는 내부 서버의 인증서 인증 과정을 진행하지 않는다. |

2) WebtoB Server 설정경로 : $WEBTOBDIR/config/http.m

tmax@TAC2:~/webtob/config

```
*VHOST
limpc_vhost     DOCROOT="/home/tmax/webtob/docs",
                PORT = "4430",
                NODENAME = "$(NODENAME)",
                HOSTNAME = "client.test.co.kr",
                HOSTALIAS = "192.168.41.152,127.0.0.1",
                ERRORDOCUMENT = "503",
                SslFlag = Y,
                SslName = "server_ssl",
                LOGGING = "log1",
                ERRORLOG = "log2"

*SSL
server_ssl      CertificateFile="$(WEBTOBDIR)/ssl/server.crt",
                CertificateKeyFile="$(WEBTOBDIR)/ssl/NewPrivateKey.txt",
                CACertificateFile="$(WEBTOBDIR)/ssl/ca.crt",
                CertificateChainFile="$(WEBTOBDIR)/ssl/fake/CHAIN.crt",
                VerifyDepth = 3,
                VerifyClient = 2,
                #Protocols = "TLSv1",
                Protocols = "-SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2",
                RequiredCiphers = "HIGH:MEDIUM:!aNULL:!MD5"
```

※ RequiredCiphers 를 동일하게 맞춰주시기 바랍니다. 해당 값이 다른 경우 키 교환이 정상적으로 이루어지지 않을 수 있습니다.
※ 아래는 Server가 되는 WebtoB의 입장에서 SSL VerifyDepth에 관한 설명입니다.

| 레벨 | 설명 |
|---|---|
| 0 | 아무런 인증 요청을 하지 않는다. |
| 1 | 사용자는 사용 가능한 인증을 서버에게 보여 주어야 한다. |
| 2 | 사용 가능한 인증을 반드시 서버에게 보여 주어야 한다. |
| 3 | 사용자는 사용 가능한 인증을 보여 주어야 하며 만일 서버가 인증서를 가지고 있지 않은 상황에서는 인증서 인증 과정이 필요 없다. |

## 2.2 테스트 절차

### *1. 테스트 시나리오*

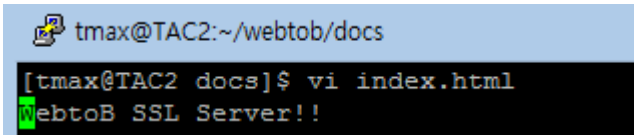
***본 문서에서는 브라우저를 통한 호출, 터미널을 통한 호출을 테스트합니다.***

상호인증에 필요한 클라이언트 인증서를 보유한 WebtoB ReverseProxySSL 을 통해 서버가 되는 아파치의 CA 인증 동작을 수행하는지 또한 wbssl s_client -connect 명령어를 통해 정상적으로 SSL 세션이 맺어지는지 확인하도록 하겠습니다.

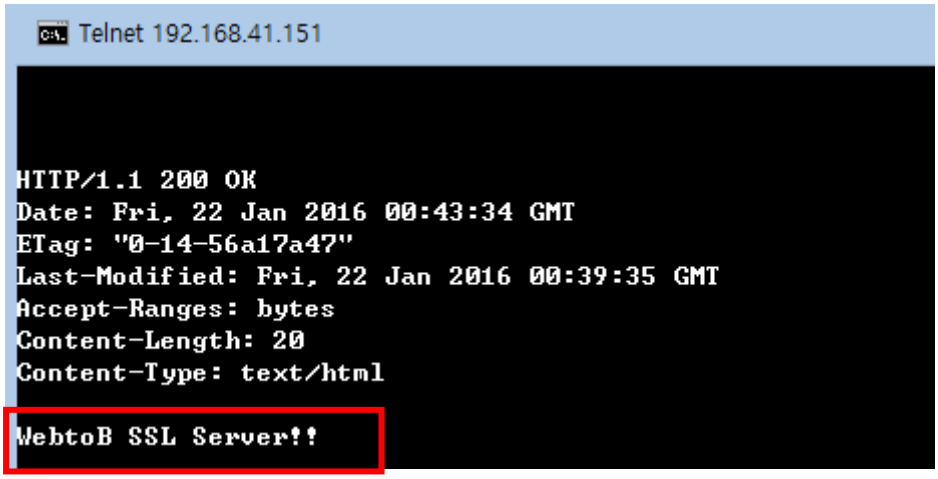
### *2. 터미널을 통한 호출 테스트*

1) telnet 192.168.41.151 8080을 활용한 호출

$>telnet 192.168.41.151 8080 GET / HTTP/1.1 Host : 192.168.41.151 을 통해 WebtoB Proxy에서 WebtoB로 호출을 시도합니다. 현재 WebtoB Server가 되는 152의 Index.html에는 다음과 같이 적혀 있습니다.



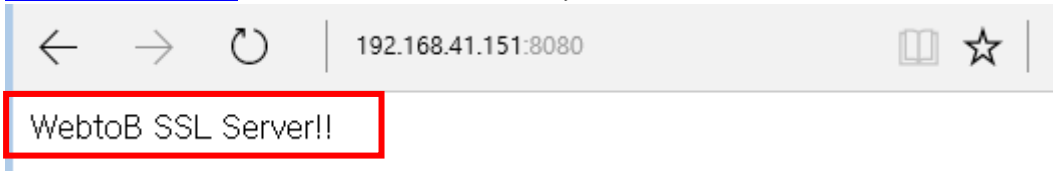

2) WebtoB Client ProxySSL이 Server SSL로 호출을 성공한 결과입니다.




### *3. 웹 브라우저를 통한 WebtoB Proxy SSL -> Server SSL 호출*

1) 익스플로러 호출

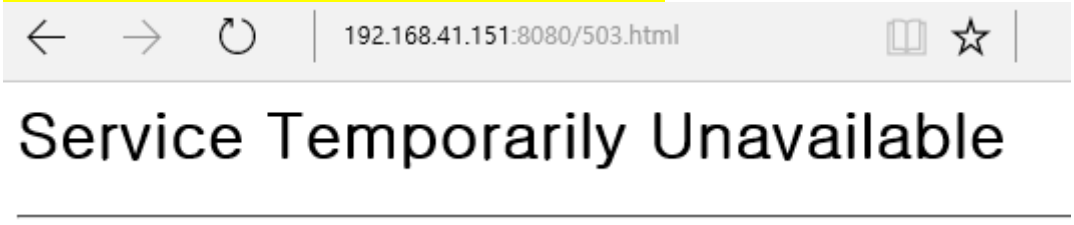
https://192.168.41.151:8080 호출을 통해 Client WebtoB에서 Proxy SSL을 통해 192.168.41.152 서버로 SSL 연결을 하게 됩니다.




2) 서버가 되는 192.168.41.152의 CACertificateFile 항목을 현재까지의 설정에서 제외하면 서비스가 되는가?

결과적으로 서비스가 되지 않는다고 볼 수 있습니다. 임의적으로 http.m 환경파일에 적용하지 않으면 내부서버의 인증을 원하는 클라이언트가 서버의 CA인증서로 인증을 받을 수 없기 때문에 정상적인 응답을 하지 않습니다.

※아래는 CACertificateFile를 서버에서 제외하고 테스트를 수행한 결과입니다.




## 3. 주요설정 참조

### 3.1 상호인증을 위한 주요설정

### *1. WebtoB ProxySSL(Client) 주요 환경설정*

```
*VHOST
limpc_vhost     DOCROOT="/home/tmax/webtob/docs",
                PORT = "8080",
                NODENAME = "$(NODENAME)",
                HOSTNAME = "client.test.co.kr",
                HOSTALIAS = "192.168.41.151,127.0.0.1",
                ERRORDOCUMENT = "503",
                LOGGING = "log1",
                ERRORLOG = "log2"

*REVERSE_PROXY
limpc_reverse
                ServerAddress = "192.168.41.140:4430",
                PathPrefix = "/",
                ServerPathPrefix = "/",
                ProxySSLFlag = Y,
                ProxySSLName = client_ssl

*PROXY_SSL
client_ssl      Verify = 2,
                VerifyDepth = 3,
                CACertificateFile="$(WEBTOBDIR)/ssl/ca.crt",
                CertificateChainFile="$(WEBTOBDIR)/ssl/fake/CHAIN.crt",
                CertificateFile="$(WEBTOBDIR)/ssl/server.crt",
                CertificateKeyFile="$(WEBTOBDIR)/ssl/NewPrivateKey.txt",
                Protocols = "-SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2",
                RequiredCiphers = "HIGH:MEDIUM:!aNULL:!MD5"
```

### *2. WebtoB SSL(Server) 주요 환경설정*

```
*VHOST
limpc_vhost     DOCROOT="/home/tmax/webtob/docs",
                PORT = "4430",
                NODENAME = "$(NODENAME)",
                HOSTNAME = "client.test.co.kr",
                HOSTALIAS = "192.168.41.152,127.0.0.1",
                ERRORDOCUMENT = "503",
                SslFlag = Y,
                SslName = "server_ssl",
                LOGGING = "log1",
                ERRORLOG = "log2"

*SSL
server_ssl      CertificateFile="$(WEBTOBDIR)/ssl/server.crt",
                CertificateKeyFile="$(WEBTOBDIR)/ssl/NewPrivateKey.txt",
                CACertificateFile="$(WEBTOBDIR)/ssl/ca.crt",
                CertificateChainFile="$(WEBTOBDIR)/ssl/fake/CHAIN.crt",
                VerifyDepth = 3,
                VerifyClient = 2,
                #Protocols = "TLSv1",
                Protocols = "-SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2",
                RequiredCiphers = "HIGH:MEDIUM:!aNULL:!MD5"
```

Trademarks
Tmax, WebtoB, WebT, JEUS, ProFrame, SysMaster and OpenFrame are registered trademarks of TmaxSoft Co., Ltd. Other products, titles or services may be registered trademarks of their respective companies.

Contact Information
TmaxSoft can be contacted at the following addresses to arrange for a consulting team to visit your company and discuss your options for legacy modernization.

Korea – TmaxSoft Co., Ltd.
Corporate Headquarters
272-6 Seohyeon-dong, Bundang-gu, Seongnam-si, South Korea, 463-824
Tel : (+82) 31-8018-1708 Fax : (+82) 31-8018-1710
Website : http://tmaxsoft.com

U.S.A. – TmaxSoft Inc.
560 Sylvan Avenue Englewood Cliffs, NJ 07632, USA
Tel : (+1) 201-567-8266 Fax : (+1) 201-567-7339
Website : http://us.tmaxsoft.com

Japan –TmaxSoft Japan Co., Ltd.
5F Sanko Bldg, 3-12-16 Mita, Minato-Ku, Tokyo, 108-0073 Japan
Tel : (+81) 3-5765-2550 Fax: (+81) 3-5765-2567
Website : http://jp.tmaxsoft.com

China –TmaxSoft China Co., Ltd.
Room 1101, Building B, Recreo International Center, East Road Wang Jing, Chaoyang District, Beijing, 100102, P.R.C
Tel : (+86) 10-5783-9188 Fax: (+86) 10-5783-9188(#800)
Website : http://cn.tmaxsoft.com

China(JV) – Upright(Beijing) Software Technology Co., Ltd
Room 1102, Building B, Recreo International Center, East Road Wang Jing, Chaoyang District, Beijing, 100102, P.R.C
Tel : (+86) 10-5783-9188 Fax: (+86) 10-5783-9188(#800)
Website : www.uprightsoft.com