SSL 인증서 적용
체크리스트

본 문서는 주식회사 한국기업보안에서 SSL보안서버인증서 설치를 위해 작성된 문서로
주식회사 한국기업보안의 동의 없이 무단으로 사용하실 수 없습니다.

[고객센터]
한국기업보안. 유서트 기술팀
02-512-9375

한국기업보안
Korea Corporation Security

목 차

인증서 교체 전 체크 사항 - 체크리스트

서버 작업 시 유의 사항

1. 서비스 중인 프로세스 및 활성화 포트 확인	☐
2. 작업 도메인 확인	☐
3. 루트 디렉터리 및 인증서 경로 확인	☐
4. 서버 ip, 포트 설정 여부 확인.	☐
5. 서버 별 정상 인증서 형식 확인	☐
6. 서버에 인증서 업로드가 필요한지 여부 확인	☐
7. 인증서 패스워드 확인 및 설정	☐
8. 서버 실행 파일 경로 확인 및 실행 스크립트 파일 확인. (프로세스 목록)	☐
9. 각 웹 서버에 맞는 설정 구문 및 인증서 파일 설정 작업 진행	☐
10. 설치 가이드와 관련 자료 참고하여 인증서 설치 진행	☐
11. 고객의 요청에 맞춰 프로세스 재 구동 – 각각의 서버에 맞게 프로세스 실행	☐
12. 재시작 후 서비스 이상 및 현황 확인.	☐

인증서 교체 전 체크 사항	서버에서 폐쇄망(내부망)으로 (Port 443) 해제.	□

인증서 교체 후 폐쇄망에서 발생할 수 있는 현상

1. 인증서 교체 이후 브라우저 접속 시 신뢰할 수 없는 인증서 오류 메시지 호출

2. https 로 접속 시 해당 웹사이트에 접속 delay 현상 발생.
3. 폐쇄망 또는 내부망 에서 인증서 상품이 변경되거나 인증기관이 변경되면 나타날 수 있는 현상

해결 방안

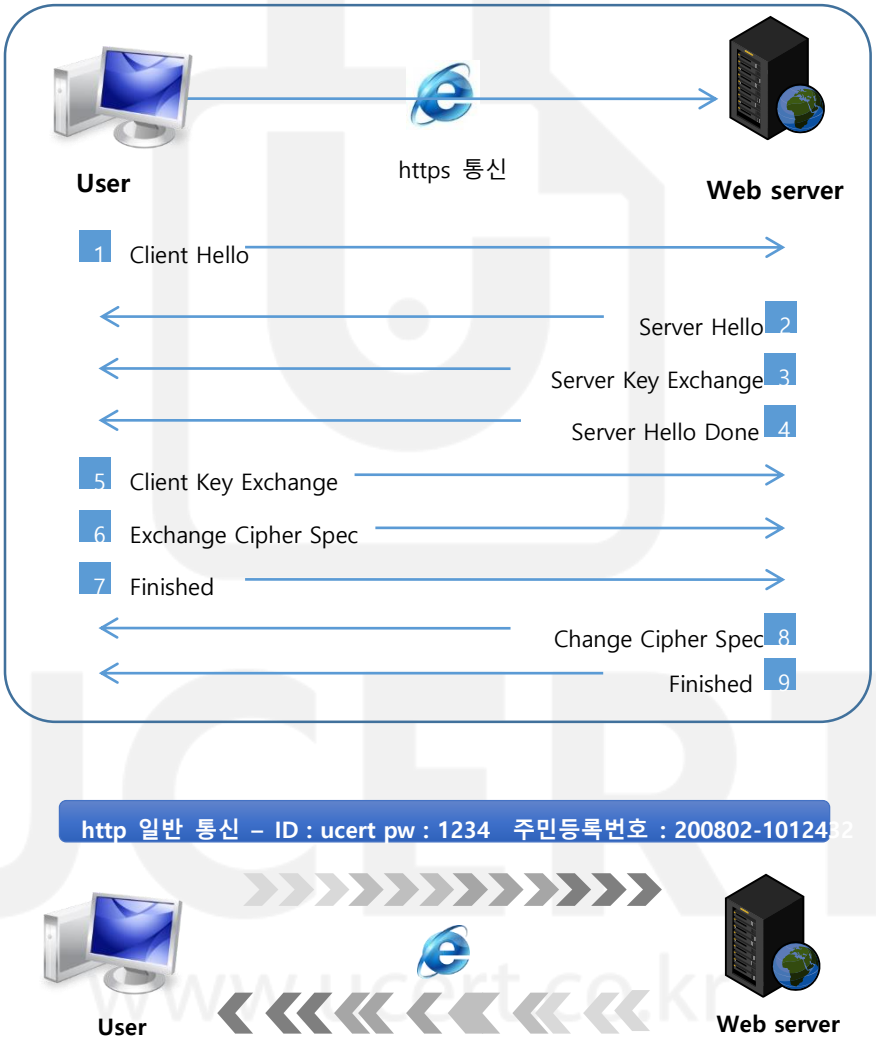
인증서는 3 자 통신으로써 인증서 상품마다 인증서의 유효성을 확인하는 URL 이 기재되어 있기 때문에 https 통신 시 인증기관과의 통신을 위해 인증기관에서 제공하는 URL 정보를 서버 또는 방화벽에 등록이 되어야 합니다.

인증서 교체 전 체크 사항 – 폐쇄망(내부망)

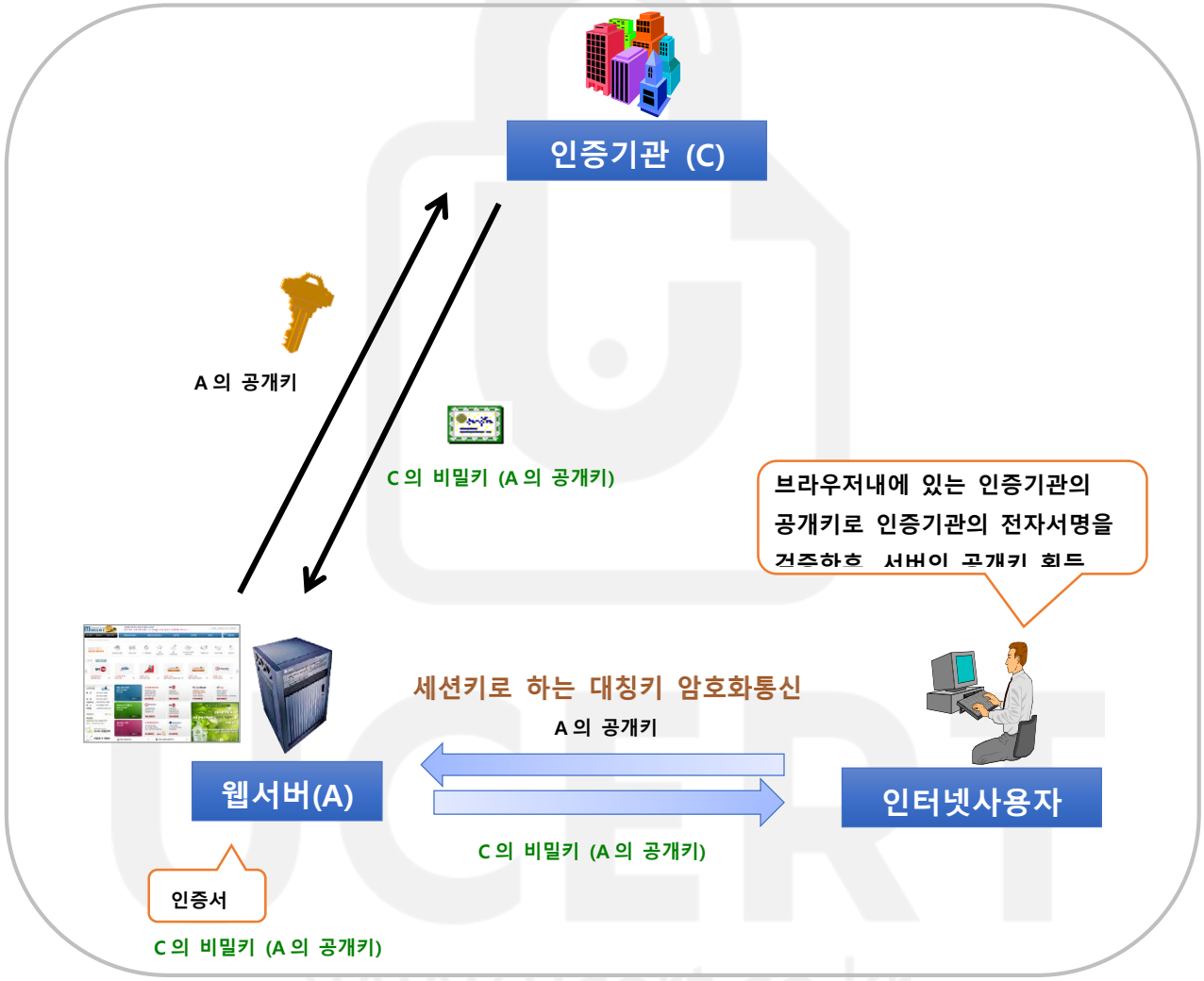
인증기관 URL 주소(예시)

인증서		인증기관 통신 URL
Chain 인증서	온라인 인증서 상태 프로토콜(OCSP)	http://ocsp.globalsign.com/rootr1
	인증서 정책	https://www.globalsign.com/repository/
	CRL 배포	http://crl.globalsign.net/root.crl
Seed 인증서	온라인 인증서 상태 프로토콜(OCSP)	http://ocsp2.globalsign.com/gsalphasha2g2
	인증서 정책	https://www.globalsign.com/repository
	인증서 CRL 배포지점	http://crl2.alphassl.com/gs/gsalphasha2g2.crl

SSL 보안인증서 통신 구조

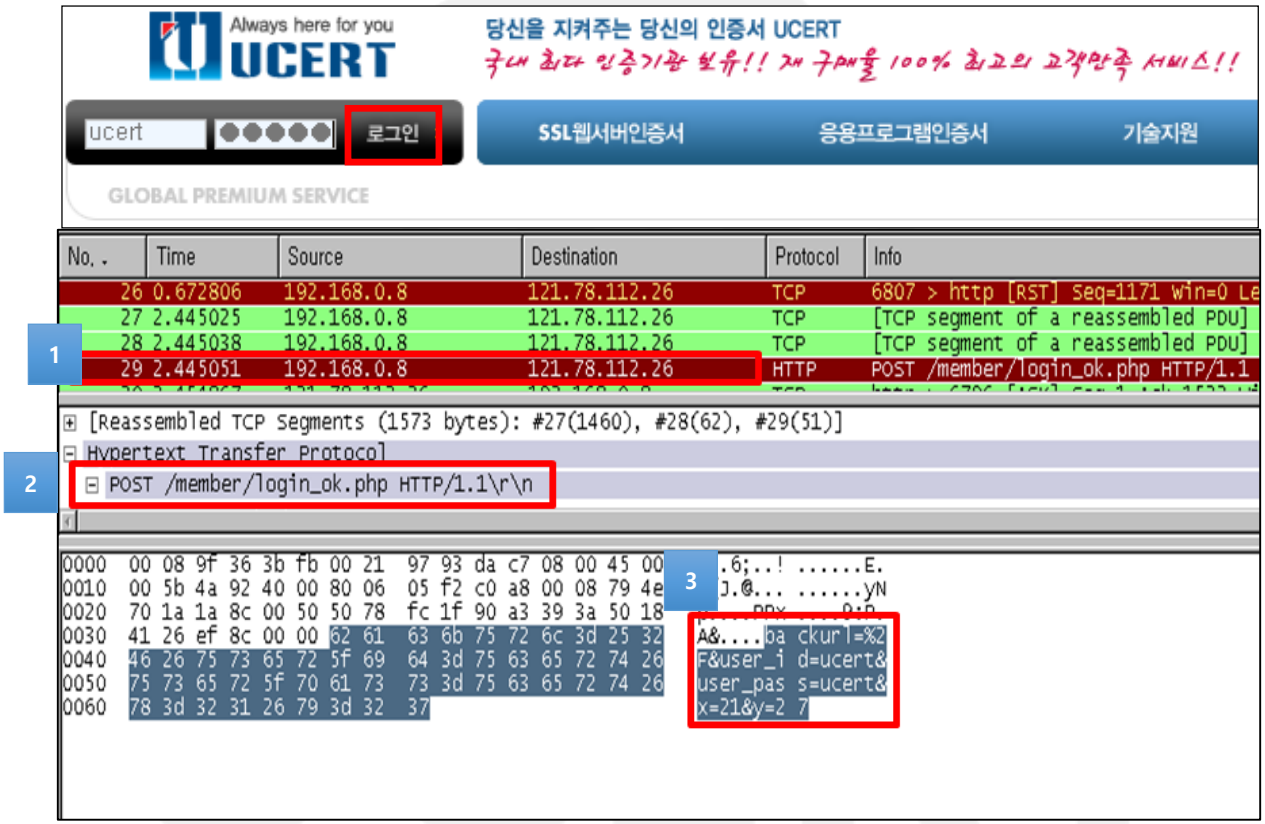


SSL 보안인증서 암호화 과정



위와 같은 과정을 통하여 암호화 된 데이터를 서버에 전송 할 수 있으며
데이터의 변조 여부를 확인 할 수 있습니다. (기밀성, 무결성)

일반 통신 (DEFAULT 80)



1) *목적지 IP: 121.78.112.26 *출발지 IP: 192.168.0.8
2) 로그인 시 POST 방식으로 /member/login_ok.php 로 데이터 전송
3) 스니핑 된 데이터 (ID / PW 획득)

일반 통신과 SSL 통신의 차이점

SSL 통신 (DEFAULT 443)

Korea Corporation Security Co.,Ltd. [KR] | https://www.ucert.co.kr/myucert/login.html

아이디

비밀번호

remember me Forgot ID/password?

로그인

ssl && (ip.src==121.78.88.70 || ip.dst==121.78.88.70) Expression…

No.	Time	Source	Destination	Protocol	Length	Info
13	1.948170	192.168.0.4	121.78.88.70	TLSv1.2	571	Client Hello
18	1.958265	121.78.88.70	192.168.0.4	TLSv1.2	191	Server Hello, Change Cipher Spec, Encrypted Handshake Mess…
20	1.958880	192.168.0.4	121.78.88.70	TLS	105	Change Cipher Spec, Hello Request, Hello Request
21	1.961845	192.168.0.4	121.78.88.70	TLS	1002	Application Data
29	1.982160	121.78.88.70	192.168.0.4	TLSv1.2	877	Application Data, Application Data
47	2.022921	192.168.0.4	121.78.88.70	TLSv1.2	745	Application Data

1

> hernet II, Src: AsustekC_e7:e5:36 (40:16:7e:e7:e5:36), Dst: EfmNetwo_24:45:d4 (00:26:66:24:45:d4)
> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 121.78.88.70
> Transmission Control Protocol, Src Port: 12760, Dst Port: 443, Seq: 1, Ack: 1, Len: 517

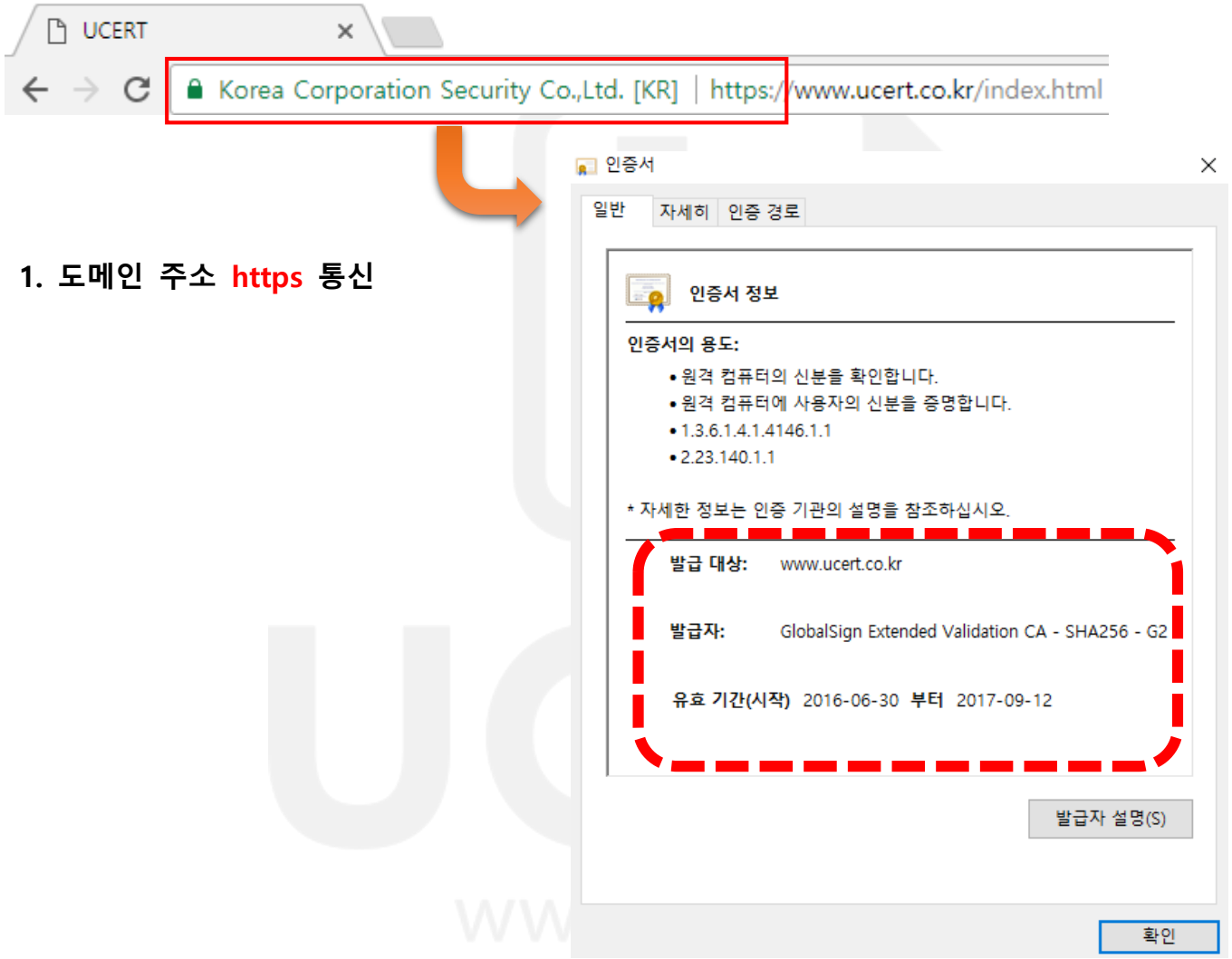
2

3

4

```
0020  58 46 31 d8 01 bb f9 f9  fa 53 b3 7a fd 93 50 18   XF1..... .S.z..P.
0030  fa f0 35 72 00 00 16 03  01 02 00 01 00 01 fc 03   ..5r.... ........
0040  03 8e cd 05 30 39 4b f1  23 67 f5 9e fa f0 d4 e2   ....09K. #g......
0050  47 9d 81 43 47 a3 1d 0f  ac 97 97 df da e7 8f f7   G..CG... ........
0060  35 20 60 e7 8a 9f 43 87  38 f3 e8 07 fd a2 21 f8   5 `...C. 8.....!.
0070  a6 19 c9 4f fb b9 52 16  26 97 1c ac 7e 4e b0 37   ...O..R. &...~N.7
0080  2f b8 00 1c 8a 8a c0 2b  c0 2f c0 2c c0 30 cc a9   /......+ ./.,.0..
0090  cc a8 c0 13 c0 14 00 9c  00 9d 00 2f 00 35 00 0a   ........ .../.5..
00a0  01 00 01 97 0a 0a 00 00  ff 01 00 01 00 00 00 00   ........ ........
00b0  14 00 12 00 00 0f 77 77  77 2e 75 63 65 72 74 2e   ......ww w.ucert.
00c0  63 6f 2e 6b 72 00 17 00  00 00 23 00 d0 c0 78 a0   co.kr... ..#...x.
00d0  de 21 32 30 e9 ab 79 95  81 0a 01 6d 78 b3 9f cb   .!20..y. ...mx...
00e0  27 38 7b 3c fa ac e6 35  60 c2 a8 3d 2c 6e 11 68   '8{<...5 `..=,n.h
```

SSL 보안 인증서 확인 (PC)



1. 도메인 주소 https 통신

2. 인증서 정보 확인