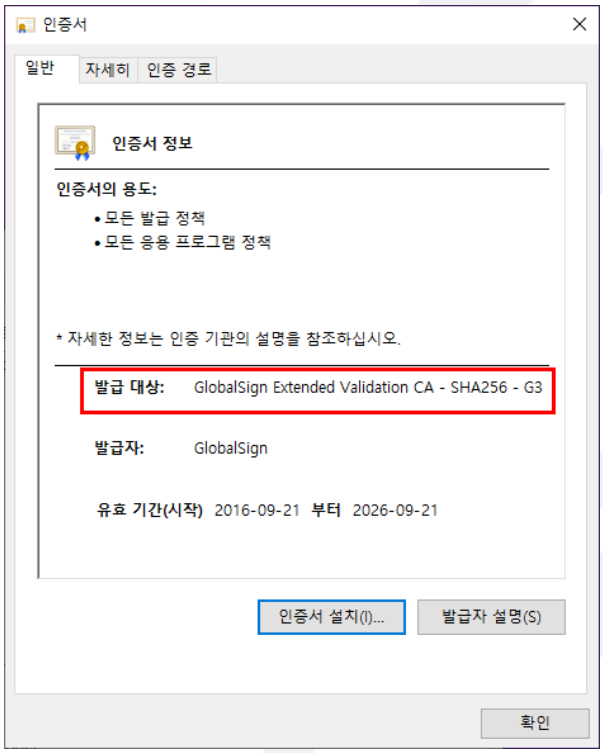
인증서 FAQ

[고객센터]
한국기업보안. 유서트 기술팀
02-512-5495

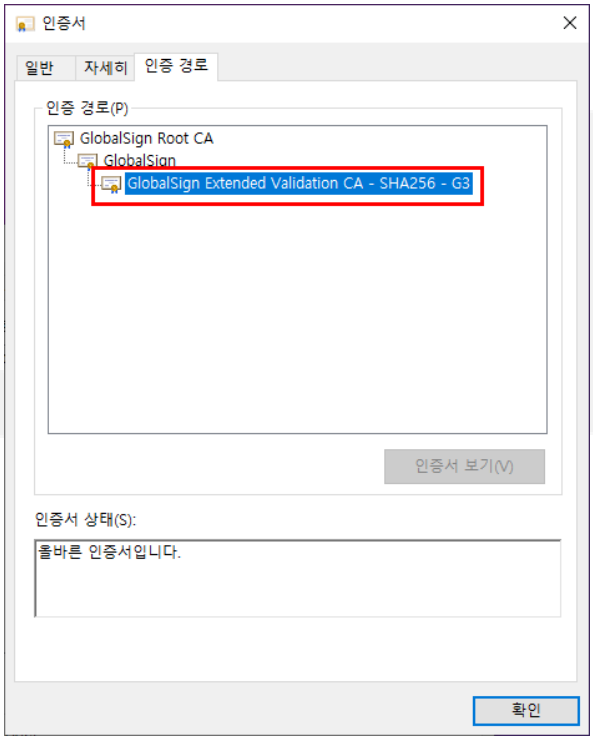
1. 발급한 인증서 중 어떤 인증서가 chain / root 인가요?

인증서의 통신 시 기본적인 구조는 public key(도메인) / chain / root 순의 트리구조로 되어 있으며, 인증서 발급시, private key(비밀키)와 함께 총 4개의 인증서가 발급됩니다.

1. 발급 받으신 인증서를 더블클릭 하여 인증서를 오픈합니다.
   "발급 대상"을 확인 합니다.

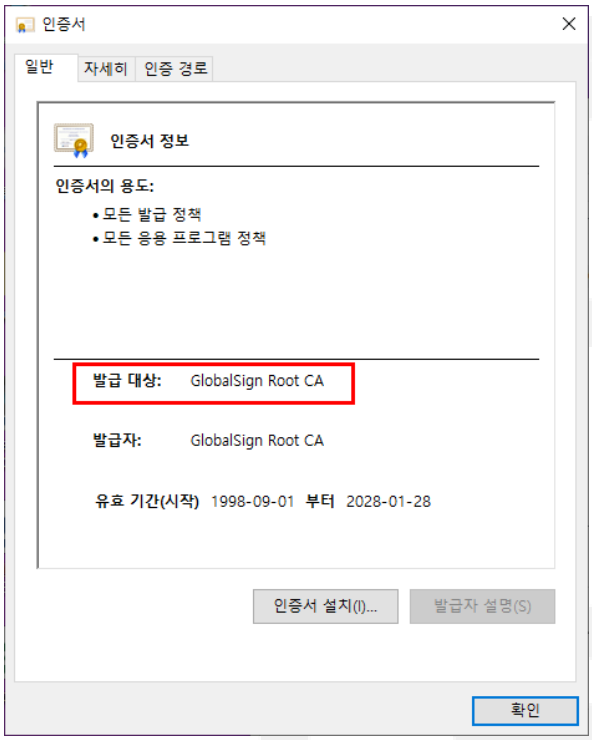


2. 아래와 같이 "인증경로"에 트리구조가 존재하면 chain 인증서 입니다.

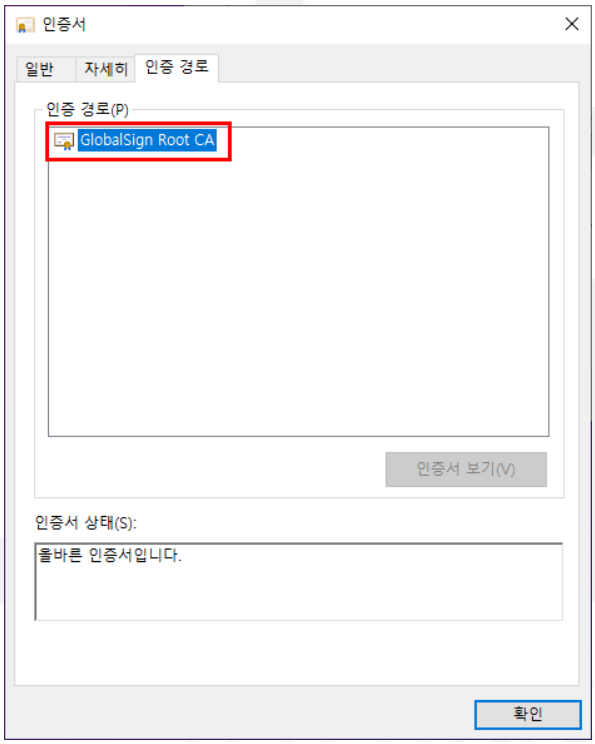


3. 최상위에 존재하고 트리구조가 존재 하지 않다면 root 인증서 입니다.

3.1 "발급대상" 확인



3.2 "인증경로" 확인



2. Webserver-WAS(ex 아파치/톰캣) 일 경우 어디에 인증서 설치를 해야하나요?

일반적으로 WAS는 보통 내부망에 구성되어 있기 때문에 DMZ 구간에 존재하는 웹서버에 인증서를 설치 합니다.

3. Webtob(.pem) 인증서가 필요한데 apache(.crt) 인증서를 받았습니다.

인증서의 ".crt" 확장자를 ".pem"으로 파일명을 리네임하여 사용하셔도 무방합니다.

4. 기존에 설정된 인증서 파일명과 새로발급한 인증서 파일명이 다릅니다.

기존 설정된 인증서를 모두 백업 하신 후, 새로발급한 인증서 파일명을 기존 발급한 인증서파일명으로 변경하여 사용 해 주시거나, 설정파일(ssl.conf 또는 httpd-ssl.conf 등)의 인증서 옵션 부분에서 파일명을 변경하여 설정해주시면 됩니다.

5. 웹서버 설정파일에 chian 옵션은 없는데 설정을 안해도 되나요?

TLS/SSL 인증서는 브라우저 및 모바일 등의 호환성과 보안성성 향상을 위해 Root / Chain 모두 설정하는 것을 권장드리고 있습니다.
추가로 설정구문을 이용하여 Chain 옵션을 설정하여 인증서 설치를 권장드립니다.

6. 루트/체인 인증서도 교체 해야하나요 ?

TLS/SSL 인증서를 발급 하는 인증기관은 보안성 향상을 위해 주기적으로 Root 및 Chain 을 업데이트 하고 있습니다.
브라우저 및 모바일 등의 호환성을 위해 Root / Chain 모두 설정하는 것을 권장드립니다.

7. 싱글 인증서를 여러 개 구매하였는데 도메인들에 대하여 같은 포트로 사용이 가능한가요?

기본적으로 같은 포트에는 서로 다른 인증서를 적용할 수 없습니다.
포트를 구분하여 적용하거나 멀티/와일드 인증서를 사용하시면 같은 포트로 사용 가능합니다.
추가로 SNI 기능을 사용할 수 있는 서버의 버전이라면 중복포트 사용은 가능하지만
일부 SNI 기능을 지원하지 않는 버전이 낮은 PC(XP, IE6등)에서 오류가 발생 할 수 있습니다.

8. 인증서 적용 후 재기동 시, "SSL Library Error : Pass phrase incorrect" 오류 발생

윈도우 환경의 아파치를 사용중이실 경우, 패스워드를 제거하여 사용 해 주셔야합니다.
제거하는 방법은 openssl 명령어로 가능하십니다. (openssl 설치 필요)
openssl rsa -in ucert.co.kr.key -out ucert_new.co.kr.key
(*명령어 형식 : openssl rsa -in "제거할 key 파일" -out "제거된 key 새 파일명")

9. IP 변경 및 서버 이전을 할 예정입니다. 인증서는 재발급 받아야 하나요?

인증서는 일반적으로 도메인을 기준으로 발급이 되기 때문에 도메인이 변경되지 않는 이상 발급 받으신 인증서로 사용이 가능합니다.

10. 인증서를 적용 하였는데, 여전히 기존 인증서가 보입니다.

Linux서버는 인증서가 정상적으로 갱신이 되었는지 서버 내에서 확인합니다.

openssl s_client -connect localhost:443 | openssl x509 -noout –dates

(*명령어 형식 : openssl s_client -connect [도메인 or IP]:[포트번호] | openssl x509 -noout –date)

Windows 서버는 서버 내에서 웹브라우저로 접속(localhost:ssl포트)하여 인증서를 확인 합니다.

서버내에 적용이 잘 되었다면,

서버 앞 단에 웹 방화벽등 장비 유무를 확인하여 장비에도 인증서를 설치 해 주셔야 합니다.

11. 브라우저 주소창에 "! 주의요함"의 문구가 발생합니다.

브라우저사의 보안 강화로 인해 웹소스상에 http와 https가 혼합되어있는 경우, 발생합니다.

"주의요함" 문구가 발생하는 웹페이지에서

개발자도구(F12) > “Console” 를 클릭해보면 “Mixed Content” 문구가 출력되는 경우, 홈페이지의 소스를 상대경로 또는 https 절대경로로 수정 하시기 바랍니다.