THE ULTIMATE TRUST ACROSS THE NET
Goverment Licensed Certification Authority

SHA-2 알고리즘 변경 공지

Nov 2015

SSL 인증서의 SHA-2 알고리즘 변경 알림

Microsoft (Internet Explorer)

→ 기존: 2017년 1월 1일부터 SHA-1 지원 중단

→ **변경: 2016년 6월 1일 SHA-1 지원 중단 예상**

Mozilla (Firefox)

→ 기존: 2017년 1월 1일부터 SHA-1 지원 중단

→ **변경: 2016년 7월 1일 SHA-1 지원 중단 예상**

Google (Chrome)

→ 기존: 2017년 1월 1일부터 SHA-1 지원 중단

→ **변경: 2016년 1월부터 SHA-1 웹 사이트 접근 시 '안전하지 않은 웹사이트'라는 경고 문구를 노출할 예정**
2017년 1월 1일부터 SHA-1 지원 중단 예상

Apple (Safari)

→ **아직까지 중단 계획 없음**

〈관련 포스트〉

구글 : https://googleonlinesecurity.blogspot.kr/2014/09/gradually-sunsetting-sha-1.html

MS : http://blogs.windows.com/msedgedev/2015/11/04/sha-1-deprecation-update

모질라 : https://blog.mozilla.org/security/2015/10/20/continuing-to-phase-out-sha-1-certificates

대응 방안

- **SHA-2 알고리즘으로 변경**

: SHA-1 서명 해시 알고리즘을 사용하는 고객 사는 SHA-2 서명 해시 알고리즘 변경을 통해 SHA-1 취약점 및 주요 브라우저들의 SHA-1 지원 중단 을 해결할 것을 권고합니다.

- **SHA -2 전환 관련하여 고객 공지 필요**

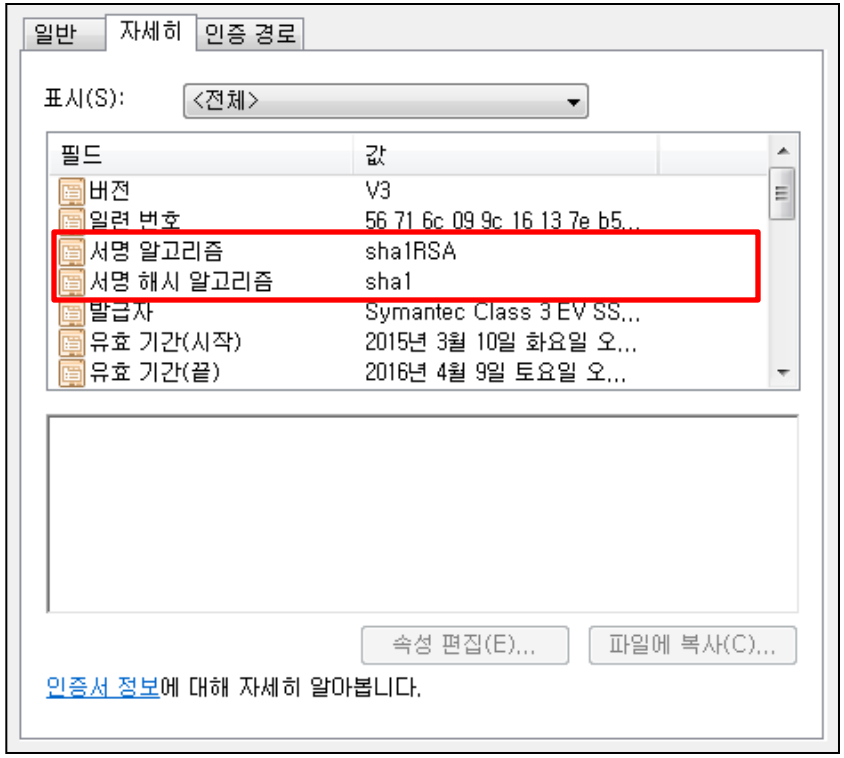
: SHA-2 서명 해시 알고리즘으로 상향함에 따라, 해당 알고리즘을 지원하지 않는 저사양 PC (Windows XP 서비스팩 2 이하) 이용자는 사이트 접속이 불가합니다. 운영체제(Windows XP 서비스팩 3 이상)로 업데이트 해야 합니다.

: SHA-2 전환 시 사전에 고객에게 공지가 필요합니다.

브라우저에서 SHA-1 또는 SHA-2 인증서 확인 방법(SSL 인증서)

Chrome & Internet Explorer

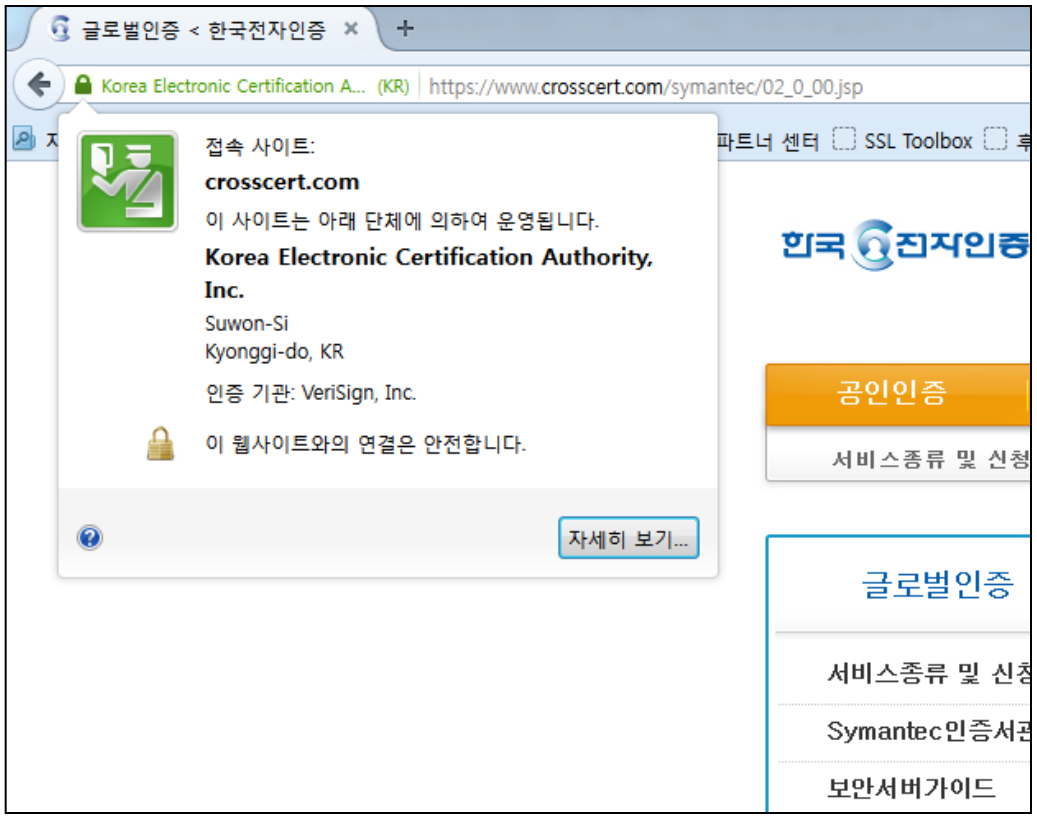
자물쇠 아이콘 클릭 -〉 “인증서 정보” -〉 서명 알고리즘 및 서명 해시 알고리즘을 통해 확인이 가능합니다.

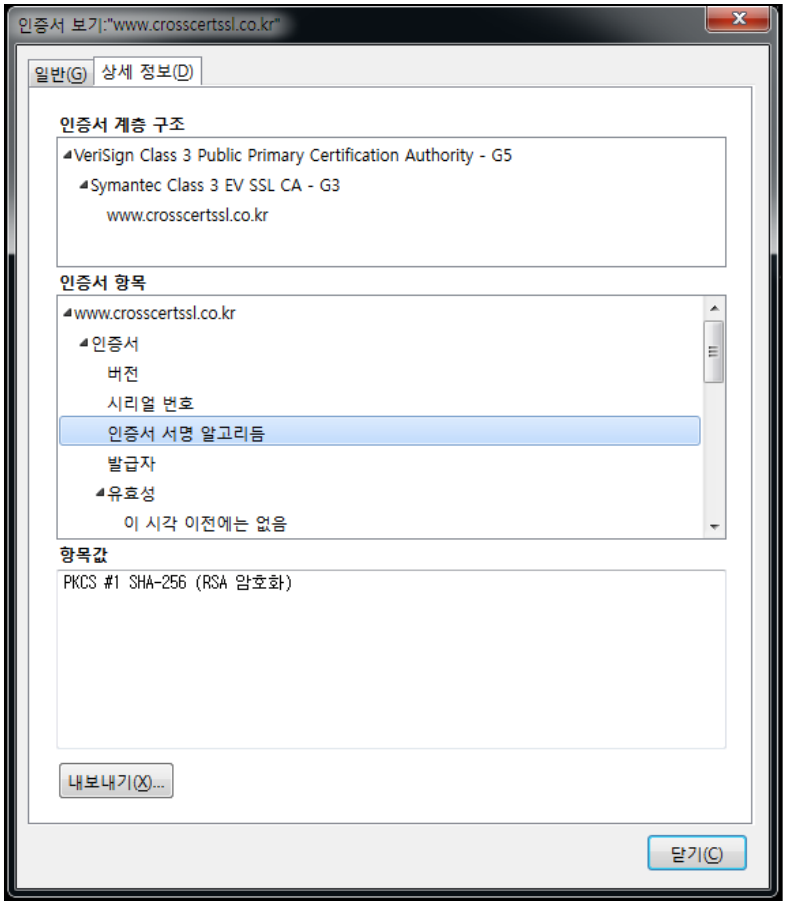


브라우저에서 SHA-1 또는 SHA-2 인증서 확인 방법(SSL 인증서)

Firefox

자물쇠 아이콘 클릭 -〉 “자세히 보기” -〉 인증서 서명 알고리즘을 통해 확인이 가능합니다.





SHA-2 알고리즘 지원 환경 목록(SSL 인증서)

브라우저	최소 브라우저 버전
Chrome	버전 26 이상
Firefox	버전 1.5 이상
Internet Explorer	반드시 Windows XP SP3 이상이면서 IE 6.0 이상 (권장사항은 IE 7.0 이상)
Java 기반 어플리케이션 및 제품	버전 1.4.2 이상
Konqueror	버전 3.5.6 이상
Netscape	버전 7.1 이상
Opera	버전 9.0 이상
Safari (Mac OS X)	버전 10.5 이상
Safari (Windows)	버전 3 이상
OpenSSL 기반 어플리케이션과 제품	버전 0.9.8o 이상

SHA-2 알고리즘 지원 환경 목록(SSL 인증서)

서버	최소 서버 버전
Apache	버전 2.0.63 이상 (openssl 0.9.8o 이상)
Nginx	openssl 0.9.8o 이상
Webtob	openssl 0.9.8o 이상
Windows Server 2003 (IIS 6.0)	서버는 다음 패치가 필요할 수도 있습니다. (KB 938397)
Windows Server 2003 이상 또는 XP	사용자(클라이언트는)는 다음 패치가 필요할 수도 있습니다. (KB 968730)
Windows Server 2008 (IIS 7.0)	✓
Windows Server 2008 R2 (IIS 7.5)	✓
Windows Server 2012 (IIS 8.0)	✓
Windows Server 2012 R2 (IIS 8.5)	✓
Windows Vista	✓
Windows 7	✓

SHA-2 알고리즘 지원 환경 목록(SSL 인증서)

서버	최소 서버 버전
Tomcat	Java 버전 1.4.2 이상
Java 기반 서버 (Resin, Tomcat …)	버전 1.4.2 이상
Oracle WebLogic	버전 10.3.1 이상 (11g 이상)
Oracle iPlanet Web Server	버전 6.1 서비스 팩 3 이상
Oracle Wallet Manager	버전 11.2.0.1 이상
IBM Domino	9.0.1 Fix Pack 3
IBM HTTP Server	GSKit 7.0.4.14 이상 (IHS 6.1은 GSKit 7.0.4.28 이상일 때, gsk7capicmd 명령어를 이용하여 커맨드 라인에서만 SHA-2 지원 가능)
IBM Websphere Application Server	GSKit 8 이상

SHA-2 알고리즘 지원 환경 목록(SSL 인증서)

모바일 기기	최소 모바일 기기 버전
Android	버전 2.3 (진저브레드) 이상
Blackberry	버전 5.0 이상
iPhone iOS	버전 3.0 이상
Windows Phone	버전 7 이상

SHA-2 알고리즘 미지원 환경 목록(SSL 인증서)

OS
Citrix Secure Gateway
Citrix Access Gateway
Citrix Access Essentials version 3
Juniper SBR
Citrix Receiver models
BlackBerry 2.2 / BlackBerry 1.0 Tech Preview
Cisco ACE module software versions A2 and A3
★ SHA-2 지원되는 패치 938397 가 설치 되지 않은 Windows 2003

❖ SHA-2 인증서를 지원하지 않는 운영체제를 사용하시면…

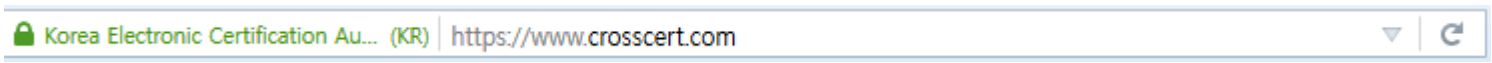
벤더 또는 유지보수 업체에게 문의하여 SHA-2가 지원되는 환경으로 변경하셔야 합니다.

❖ 웹 방화벽 등 SSL 인증서가 사용되는 별도의 장비는 호환성이 매우 상이하여 반드시 장비업체에 문의하여 확인하셔야 합니다.

EV 브라우저 녹색 창(Green Bar) 형태

Internet Explorer

Mozilla Firefox



Google Chrome

Safari

Opera

FAQ – 자주하시는 질문 (SSL 인증서)

Free

➔ SHA-1에서 SHA-2로 변경하시는 비용은 무료입니다.

Notice

➔ 2015년까지 SSL인증서는 1년형 인증서에 대해서 SHA-1 인증서 발급이 가능합니다.

✓ 1년형 인증서란 ? : 만료일 기준 2016년 12월 31일 이내의 SSL인증서

Process

➔ SHA-1에서 SHA-2로 변경하시는 과정은 갱신 과정과 동일하게 진행됩니다.

❖ Key 및 CSR 은 새로 만드셔야 합니다.

Support

➔ SHA-2 관련 문의 사항은 한국전자인증으로 문의 바랍니다.

Code Signing 인증서의 SHA-2 알고리즘 변경 알림

2016년 1월 1일 이후 Windows 7 이상에서 SHA-1 서명 차단

TimeStamp 옵션이 적용된 (2016년 1월 1일 이전에 SHA-1 서명된) 파일은 2020년 1월 1일에 서명 차단

2016년 1월 1일 이후 SHA-1 서명은 Windows 2008, Windows Vista에서만 가능

Microsoft (Internet Explorer), Mozilla (Firefox), Google (Chrome)

→ **2016년 1월 1일부터 지원 중단**

SHA-2 알고리즘 지원 환경 목록(Code Signing 인증서)

OS

OS \ Mode	Executables	Kernel Drivers	VBA Macros: Office 2003, 2007	VBA Macros: Office 2010	VBA Macros: Office 2013
Windows XP (SP1, SP2)	사용불가	사용불가	사용불가	사용불가	지원 안 함
Windows XP SP3	사용가능	사용불가	사용불가	사용가능	지원 안 함
Windows Vista	사용가능	사용불가	사용불가	사용가능	지원 안 함
Windows 7	사용가능	사용가능 (패치 필요)	사용불가	사용가능	사용가능
Windows 8	사용가능	사용가능	사용가능	사용가능	사용가능

Tools

Tools \ Version	Minimum Version Required
Visual Studio Tools for Office (VSTO)	10.0.50325+
Java	Java 1.4.2+

SHA-2 알고리즘 지원 환경 목록(Code Signing 인증서)

2016년 1월 1일 이후 변경 사항

	Before January 1st, 2016		On or after January 1st, 2016	
	SHA-1	SHA-2	SHA-1	SHA-2
Windows XP SP3	✓	✗	✓	✗
Windows Vista	✓	✗	✓	✗
Windows 7	✓	✓	✗	✓
Windows 8	✓	✓	✗	✓
Windows Server 2008	✓	✗	✓	✗
Windows Server 2008 R2	✓	✓	✗	✓
Windows Server 2012	✓	✓	✗	✓

Windows Code Signing Hash Algorithm (/fd 256 옵션 관련)

		SHA-1 Certificate		SHA-2 Certificate		EV Certificate (SHA-2 Only)	
		/fd sha1	/fd sha256	/fd sha1	/fd sha256	/fd sha1	/fd sha256
Windows XP	User Mode	✓	✗	✓	✗	✓	✗
	KernelMode	✓	✗	✗	✗	✗	✗
Windows Vista	UserMode	✓	✗	✓	✗	✓	✗
	KernelMode	✓	✗	✗	✗	✗	✗
Windows 7	UserMode	✓	✓	✓	✓	✓	✓
	KernelMode	✓	✓	✓	✓	✓	✓
Windows 8	UserMode	✓	✓	✓	✓	✓	✓
	KernelMode	✓	✓	✓	✓	✓	✓
Windows 10	UserMode	✓	✓	✓	✓	✓	✓
	Kernel Mode	✓	✓	✓	✓	✓	✓

✗	허용 안 함
✓	사용 가능
✓	**부분 허용** 2016년 1월1일 이전 서명(타임스탬프 옵션적용)
✓	**부분 허용** 윈도우 10에 대한 커널 모드 드라이버 액세스에는 EV 코드서명을 필요로 하는 Windows 하드웨어 개발자 센터 대시 보드 포털의 서명이 있어야 합니다. (2015년 7 월 29 일 이전에 서명된 파일(타임스탬프옵션 적용)의 경우에만 허용됨)
✓	**허용** 윈도우 10에 대한 커널 모드 드라이버 액세스에는 EV 코드서명을 필요로 하는 Windows 하드웨어 개발자 센터 대시 보드 포털의 서명이 있어야 합니다.

❖ Windows 10 Kernel mode 서명의 경우 2015년 7월 29이후에는 EV code 인승서만 사용 가능합니다.

FAQ – 자주하시는 질문 (Code Signing 인증서)

Windows7의 Office2010, Windows 7 and Windows Server 2008 R2

➔ Windows 7의 Office 2010은 SHA-2 지원을 위해 Hotfix KB 2598139 설치가 필요합니다.

➔ Windows 7와 Windows Server 2008 R2는 SHA-2 지원을 위해 Hotfix KB 3033929 설치가 필요합니다.

Time stamps

➔ 2016년 1월 1일부터 Windows 7 이상에서 TimeStamp 작업이 안 된 파일의 경우, 차단됩니다. (서명 날짜가 2016년 1월 1일 이전이어야 합니다.)

➔ 2016년 1월 1일부터는 Windows 7 이상에서는 SHA-1 으로 서명하면 차단됩니다.

Time stamps SHA-1

➔ Time stamps 옵션을 사용하여 SHA-1 인증서로 서명된 파일의 경우, 2020년 1월 1일 이후 차단됩니다.

➔ 2016년 1월 1일부터 SHA-1 인증서로 서명된 파일의 경우, Windows 2008, Windows Vista에서만 사용 가능합니다.

Support

➔ SHA-2 관련 문의 사항은 한국전자인증으로 문의 바랍니다.

Symantec.

한국전자인증

THE ULTIMATE TRUST ACROSS THE NET
Goverment Licensed Certification Authority

SSL 인증서 관련 보안 이슈

Nov 2015

Symantec.

한국전자인증

구글(Google) Chrome 브라우저 SHA-1 인증서 대응

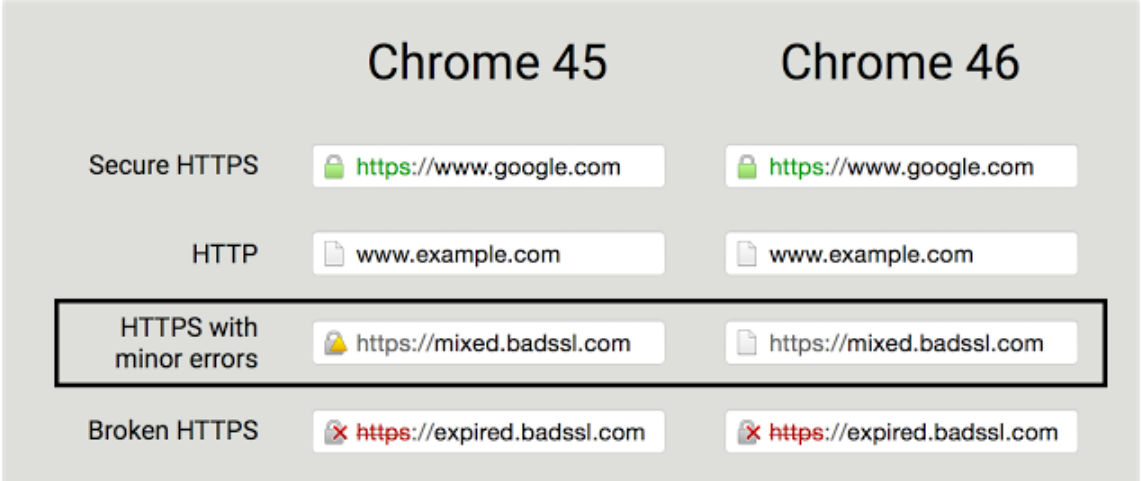
크롬 버전	출시(Release) 일자	SHA-1 인증서 만료일		
		2016.01.01 ~ 2016.05.31	2016.06.01 ~ 2016.12.31	2017.01.01 ~
39	2014.11.18	https://	https://	https://
40	2015.01.21	https://	https://	https://
41	2015.03.03	https://	https://	~~https~~://
42	2015.04.14			
43 ~	2015.05.19			

예1) 크롬 버전 39 사용 : 인증서 만료일이 2016.04.23 이라면 https://나타납니다.
예2) 크롬 버전 40 사용 : 인증서 만료일이 2016.10.10 이라면 https://나타납니다.
예3) 크롬 버전 41 사용 : 인증서 만료일이 2017.01.13 이라면 ~~https~~://나타납니다.

구글(Google) Chrome46 보안 표시 변경

Chrome 46이 출시되면서, “HTTPS with Minor Errors” 상태 아이콘이 변경되었습니다.

HTTPS를 사용하는 웹 페이지가 HTTP를 통해 이미지를 전송하는 등 혼합된 콘텐츠를 사용할 때 노란색 삼각형이 표시된 자물쇠 아이콘을 표시했었습니다. 하지만, 사용자들이 해당 사이트의 보안성이 높은지, 그렇지 않은지를 판단하는 과정에서 혼란을 줄 수 있다는 이유로 보안 표시가 변경되었습니다.

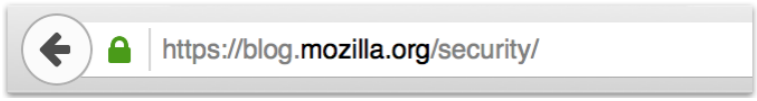


〈관련 포스트〉

https://googleonlinesecurity.blogspot.kr/2015/10/simplifying-page-security-icon-in-chrome.html

모질라(Mozilla) Firefox 42 보안 표시 변경

DV 주소 창 vs. EV 주소 창

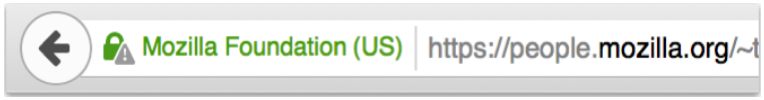
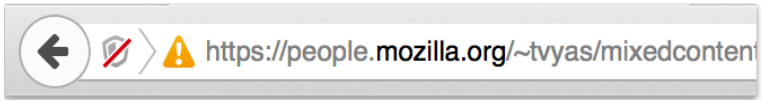
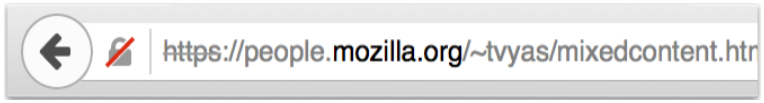
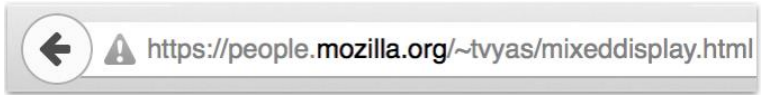
이전 버전	최신 버전
Sites with DV Certificates	
	
Sites with EV Certificates	
	

기존 Firefox 브라우저는 DV 인증서에는 **회색 자물쇠**를, EV 인증서에는 녹색 자물쇠를 표시하였으나, Firefox 42부터 DV 인증서를 녹색 자물쇠로 변경하였습니다. 녹색 아이콘을 사용함으로써 사용자들은 사이트 연결이 안전하다고 이해할 수 있습니다.

EV 인증서는 변동 사항이 없습니다.

모질라(Mozilla) Firefox 42 보안 표시 변경

혼합된 콘텐츠

이전 버전	최신 버전
Sites with mixed active content blocked	
	
Sites with mixed active content allowed	
	
Sites with mixed passive content loaded	
	

〈관련 포스트〉

https://blog.mozilla.org/security/2015/11/03/updated-firefox-security-indicators-2/

THE ULTIMATE TRUST ACROSS THE NET
Goverment Licensed Certification Authority

CROSSCERT

Symantec.

감사합니다.

Symantec.

한국전자인증