

빠른 가이드: 루트 KSK 롤오버를 위한 시스템 준비

🔑 루트 KSK 롤오버란?

ICANN(국제 인터넷 주소 관리 기구)은 일반적으로 루트 영역 KSK(키 서명 키)라고 알려진 DNSSEC(도메인 이름 시스템 보안 확장) 프로토콜에서 사용되는 암호 키의 "최상위" 쌍을 롤하거나 변경할 계획입니다. KSK의 변경은 2010년에 처음 생성된 이후로 이번이 처음입니다. 이것은 중요한 보안 단계로 간주되며 인터넷 사용자가 정기적으로 암호를 변경하는 일을 신중하게 생각하는 것과 같습니다.

키를 변경하려면 새로운 암호 키 쌍을 생성하고 새로운 공용 요소를 DNSSEC 검증 확인자에게 배포해야 합니다. DNSSEC를 사용하는 모든 인터넷 쿼리가 대상 검증을 위해 루트 영역 KSK에 의존하기 때문에 이번 변경은 매우 중요합니다. 새 키가 생성되었으므로 ISP와 같은 운영자는 사용자가 웹 사이트를 방문하려고 할 때 새 KSK에 대해 유효성을 검사할 수 있도록 시스템을 새 키로 업데이트 해야 합니다.

📄 준비해야 하는 이유

현재 전 세계 인터넷 사용자의 약 4분의 1은 KSK 롤오버의 영향을 받을 수 있는 DNSSEC 검증 확인자를 통해 인터넷에 액세스합니다. KSK 배포 후 검증 확인자에게 새로운 키가 없으면 해당 확인자에 의지하는 최종 사용자는 오류가 발생하여 인터넷에 액세스할 수 없게 됩니다.

DNSSEC를 사용하지 않는 시스템의 경우 이번 롤오버로 인해 영향을 받지 않습니다. 하지만 DNSSEC는 도메인 이름 하이재킹을 예방하는 중요한 요소임을 기억하십시오.

ICANN은 운영자 또는 관심이 있는 누구나 자동화된 업데이트 프로세스를 시스템이 제대로 처리할 수 있는지 확인할 수 있도록 테스트 베드를 제공하고 있습니다. 다음을 방문하여 시스템이 준비되었는지 확인하십시오. <https://go.icann.org/KSKtest>.



DNSSEC 검증을 활성화한 경우 새로운 KSK로 시스템을 업데이트해야 사용자에게 문제없는 인터넷 액세스를 제공할 수 있습니다.

해야 할 일

시스템은 2017년 7월 11일에 게시된 새로운 루트 영역 KSK를 사용하여 롤오버에 앞서 언제든지 업데이트될 수 있고 일부는 이미 자동 업데이트가 진행 중일 수 있습니다. 해야 할 일은 다음과 같습니다.



소프트웨어가 DNSSEC 신뢰 앵커(RFC 5011) 자동 업데이트를 지원하는 경우

KSK는 적절한 시기에 자동으로 업데이트되어야 합니다. 특별한 조치가 필요하지 않습니다.

롤오버 중에 오프라인인 기기는 롤오버가 끝난 후 온라인이 될 경우 수동으로 업데이트해야 합니다.

ICANN은 2017년 3월부터 운영자 또는 관심이 있는 누구나 자동화된 업데이트 프로세스를 시스템이 제대로 처리하는지 확인할 수 있도록 테스트 베드를 제공하고 있습니다. 자세한 내용은 <https://icann.org/kskroll>에서 확인 할 수 있습니다.



소프트웨어가 DNSSEC 신뢰 앵커(RFC 5011)의 자동 업데이트를 지원하지 않거나 자동 업데이트를 사용하도록 구성되지 않은 경우

소프트웨어의 신뢰 앵커파일을 수동으로 업데이트해야 합니다. 새 루트 영역 KSK는 이제 다음에서 제공됩니다.

<https://go.icann.org/2DOB7zn>.



KSK 롤오버는 언제 실시될니까?

KSK 롤오버는 한 번에 끝나는 것이 아닌 장기적인 절차입니다. 다음 날짜는 최종 사용자가 프로세스 중에 인터넷 서비스 중단을 겪을 수 있는 주요 이정표입니다.

2018년 10월 11일

서명을 위한 새 KSK 첫 사용 예정 날짜

2019년 1월 11일

이전 KSK 폐기 예정 날짜



예정된 변경 사항 대비를 돕기 위한 리소스를 포함하여 롤오버에 대한 자세한 정보는 <https://icann.org/kskroll>에서 찾을 수 있습니다.



제목에 "KSK Rollover"라고 적어서 globalsupport@icann.org에 이메일로 문의하거나 Twitter에서 #KeyRoll 해시태그를 사용하여 대화에 참여할 수 있습니다.