전자서명 장기검증을 위한 인증역사서비스

이병천
중부대학교 정보보호학과
e-mail: sultan@joongbu.ac.kr

Certification History Service for Long-term Signature Verification

Byoungcheon Lee
Dept. of Information Security, Joongbu University

요 약

전자서명의 장기검증이란 서명에 사용된 인증서의 유효기간이 지난 오랜 후에 서명을 검증하고자 하는 문제이다. RFC3126에서는 전자서명의 장기검증을 가능하게 하기 위해 타임스탬프기관(TSA)에 대한 신뢰를 바탕으로 전자서명에 타임스탬프(TS)를 부가하여 장기검증포맷으로 변환하여 저장하는 방법을 제시하고 있는데 TSA의 인증서도 유효기간을 가지기 때문에 시간이 지날수록 새로운 TS를 계속 부가해야 한다는 단점이 있다.

한편 과거에 사용했던 인증서 및 CRL등의 인증체계 자체를 보존하고 인증해주기 위한 메커니즘은 인증체계의 연속성을 보장하기 위해 매우 중요하다고 볼 수 있는데, 현재의 공개키기반구조(PKI) 메커니즘에는 특별히 정의되어 있지 않다. 인증체계의 장기검증을 위해 RFC3126[1]의 방법론을 적용하는 것은 여러 가지 측면에서 효율적인 방법이 아니다. 이 논문에서는 인증체계의 과거역사를 보존하고 보증해주기 위한 새로운 방법을 제시하는데, 인증기관이 자신의 인증서를 갱신하는 경우 자신이 운영했던 과거의 인증역사에 대해 봉인을 하고 책임있는 사후서비스를 하도록 하며, 현재의 인증서에 과거역사에 대한 명시적인 인증을 포함하도록 하는 것이다. 이러한 방법은 기존의 인증체계와 함께 이용될 수 있고 인증체계의 연속성을 보장하는데 큰 역할을 하게 되며 전자서명 장기검증에도 유용하게 이용될 수 있음을 보인다.

▸ Keyword : 전자서명(digital signature), 장기검증(long-term verification), 인증역사(certification history)

I. 서 론

전자서명은 서명자가 자신의 개인키를 이용하여 전자문서에 서명을 하는 것을 말하며 검증자는 서명자의 공개키를 이용하여 서명의 유효성을 검증하게 된다. 공개키 인증서는 서명자가 해당 공개키를 소유하고 있음을 인증하기 위해 인증기관(Certification Authority, CA)이 발행하는 유효기간을 가지는 문서이다. 유효기간 내에 사용자의 공개키를 취소해야 할 사정이 있는 경우 인증기관은 인증서취소목록(Certificate Revocation List, CRL)[2]에 사용자의 인증서를 포함하여 발행함으로써 인증서의 유효성을 취소할 수 있다. 검증자는 전자서명의 검증시 CRL을 통해 사용자 인증서가 취소되지 않았는지를 함께 검증해야 한다.

전자서명 장기검증이란 서명에 사용된 인증서의 유효기간이 지난 오랜 후에 해당 서명이 과거 특정 시점에 생성된 사실을 검증하고자 하는 것이다. 그런데 오랜 시간이 지난 이후에는 서명 검증에 여러 가지 문제가 있을 수 있으며 장기검증을 가능하게 하는 적절한 대책이 필요하다. 전자서명의 장기검증 기능을 제공하기 위하여 RFC3126[1]에서는 시점확인기관(Timestamping authority, TSA)이 제공하는 타임스탬프(TS)를 덧붙여서 장기검증 포맷으로 변환하여 보관함으로서 해당 전자서명이 특정시점에 존재했었

다는 것을 증명한다. 그런데 이 방법은 TSA의 인증서가 갱신되는 경우 새로운 TS를 부가하여 보존하도록 함으로써 시간이 지남에 따라 TS의 개수가 계속 증가하는 단점이 있다. 또한 이 방법은 각 문서별 장기검증 대책으로서 과거의 인증체계 자체를 미래시점에서 보증해주는 서비스는 아니다.

현재의 공개키기반구조는 현재 시점의 인증체계를 구축하는 방안에 대해서는 잘 정의되어 있지만 시간축으로 과거의 인증체계를 현재 시점에서 어떻게 인증할 것인지, 현재의 인증체계를 미래시점에서도 유효성을 인증하도록 하기 위해선 어떻게 해야 하는지, 인증기관이 발행하는 인증정보를 오랜 기간 어떻게 보존, 서비스할 것인지는 분명하게 정의하지 않고 있다. 과거의 인증체계를 검증하기 위하여 문서별 장기검증 대책인 RFC3126의 방법을 적용하는 것은 여러 가지 측면에서 효율적인 방법이 아니다.

이 논문에서는 인증체계의 과거역사를 보존하고 보증해주기 위한 새로운 방법을 제시하는데, 인증기관이 자신의 인증서를 갱신하는 경우 자신이 운영했던 과거의 인증역사에 대해 봉인을 하고 책임있는 사후서비스를 하도록 하며, 현재의 인증서에 과거역사에 대한 명시적인 인증을 포함하도록 하는 것이다. 이러한 방법은 기존의 인증체계와 함께 이용될 수 있고 인증체계의 연속성을 보장하는데 큰 역할을 하게 되며 전자서명 장기검증에도 유용하게 이용될 수 있음을 보인다.

II. RFC3126의 장기검증 기법 분석

1. 서명된 전자문서의 장기검증

전자서명 장기검증이란 서명에 사용된 인증서의 유효기간이 지난 오랜 후에 해당 서명이 과거 특정 시점에 생성된 사실을 검증하고자 하는 것인데, 인증서의 유효기간이 지난 이후에는 서명 검증에 여러 가지 문제가 있을 수 있다. 전자서명의 장기검증 기능을 제공하기 위하여 RFC3126에서는 시점확인기관(TSA)이 제공하는 타임스탬프(TS)를 덧붙여서 장기검증 포맷으로 변환하여 보관하는 방법을 제시하고 있다. 즉

1) 사용자가 생성한 전자서명에는 시점정보가 포함되어 있지 않으므로 신뢰할 수 있는 시점정보를 추가해야 한다. RFC3126에서는 시점확인기관(Timestamping authority)이 제공하는 타임스탬프(TS)를 덧붙여서 보관함으로서 해당 전자서명이 특정시점에 존재했었다는 것을 증명한다. (ES-T 포맷)
2) 서명의 검증을 위해서는 인증서, CRL, 인증경로 등의 종합적인 인증정보가 제공되어야 한다. RFC3126에서는 장기검증의 필요에 따라 이러한 인증정보에 대한 레퍼런스, 또는 인증정보 자체를 원래의 서명문에 덧붙여서 보관할 수 있도록 하고 있다. (ES-C, ES-X 포맷)
3) 서명에 사용되었던 알고리즘이 취약해지거나 키가 누출되는 등의 문제가 발생하는 경우, 또는 TSA의 인증서가 갱신되는 경우에는, 강도가 높은 알고리즘, 늘어난 키길이를 사용하여 TSA의 인증서를 갱신하고 새로운 TS를 덧붙여 보관하도록 한다 (ES-A 포맷). 시간이 지나면서 TSA의 인증서가 갱신되면 전자서명에는 여러개의 TS가 부가되어 보관될 수 있다.

RFC3126에서는 TSA의 인증서를 단순 갱신하는 경우에도 ES-A 포맷에서 새로운 TS를 부가해야 하는 것으로 기술하고 있는데 이런 경우 장기보관 문서에는 시간에 따라 TS의 개수가 계속 증가하게 되어 TS의 생성, 보관, 검증에 많은 비효율성을 야기하게 된다. 그러므로 ES-A 포맷에서 TS의 추가는 알고리즘이 취약해지거나 키가 누출되는 등의 심각한 문제가 발생한 경우에만 이루어지도록 수정할 필요가 있다. 그런데 이러한 방법은 다음과 같은 문제점이 있다.

1) 이러한 대책은 각 문서별 장기검증 대책일 뿐이며 과거의 인증체계 자체에 대한 인증을 제공하는 대책은 아니다. 서명 생성시에 사용된 인증서와 CRL 등의 인증체계가 현 시점에서 유효하다고 인정할 수 있는지 검증할 수 있는 체계가 필요하다.
2) 서명검증에 필요한 인증서, CRL 등의 인증정보를 각 문서에 덧붙여서 보관하도록 하는 것은 검증시 도움이 될지는 모르지만 인증정보들은 모든 문서에 덧붙여지기 때문에 보관해야할 문서가 늘어날수록 불필요한 자원의 낭비를 가져오게 된다. 인증정보가 원활하게 보관, 서비스된다면 이러한 낭비를 막을 수 있다.
3) 이렇게 TSA의 TS에 절대적으로 의존하는 모델에서는 적절한 TS를 부가하지 않은 정보는 미래시점에서 유효성을 인정하지 않게 될 것인데 이것은 인증기관의 권위에 위배되는 것이다. TS가 꼭 필요한 응용이 아니라면 과거 시점의 인증기관의 권위는 TS의 존재와 상관없이 인정되어야 할 것이다.
4) 과거시점에 존재했던 정보에 대해 미래시점에서 추가적인 인증을 해주어야만 유효성을 인정하겠다는 것은 우리의 일반적인 역사상식에 맞지 않는 개념이라고 생각된다. 과거에 존재했던 정보라면 큰 위조의 위험성이 없는 경우 그 자체로 유효성이 인정되어야 한다.

2. 인증체계의 장기검증

인증체계를 운영하는데 사용되는 인증서, CRL 등도 인증기관이 발행하는 전자서명으로 이루어지기 때문에 과거의 인증서, CRL등이 위조되지 않은 유효한 정보라는 것을 현재시점에서 검증하기 위해서는 이들에 대한 장기검증 대책이 필요하다. 현재의 공개키기반구조에서는 이러한 과거의 인증체계를 어떻게 보존하고 사후서비스 하는지, 현재의 시점에서 과거의 인증체계 정보의 유효성을 어떻게 보장하는지에 대해 정의하지 않고 있다. 과거 시점에서 사용했던 알고리즘의 취약성이 발견되었거나 인증기관의 비밀키가 노출된 경우, 성공적인 공격자는 사후에 과거의 인증서나 CRL을 위조할 수 있으며 이러한 일이 발생한다면 인증체계의 안전한 운영에 큰 위협이 될 것이다. 또한 일반적으로는 인증기관이 인증서나 CRL을 위조하는 등의 불법적인 행위를 하지 않을 것이라는 신뢰성을 가정하고 있지만, 오랜 기간 인증기관을 운영하게 되면 운영자가 바뀌거나 인증정책이 변화하는 등 이러한 신뢰성 가정이 적용되기 어려울 수도 있다. 예를 들어 인증기관이 미래시점에서 과거시점의 사용자 인증서를 불법적으로 발급하고 결과적으로 위조된 서명을 생성할 수 있도록 방조하는 것이 가능하다면 큰 문제가 될 것이다. 인증기관이 과거 시점의 키를 가지고 사용자 인증서를 과거시점으로 발급하는 것을 막을 수 있는 대책이 필요하다. 그러므로 이러한 신뢰가정에 의존하지 않고도 인증기관의 불법행위를 방지할 수 있는 근본적인 기술대책을 고려할 필요가 있다.

첫 번째 생각할 수 있는 기술적인 대책으로서는 전자문서에 대한 장기검증 대책인 RFC3126의 방법론을 인증서, CRL 등의 장기검증에 그대로 적용하는 것을 고려해 볼 수 있다. 즉, TSA에 대한 신뢰를 바탕으로 인증서, CRL 등에 TSA의 TS를 부가하여 장기검증 포맷으로 변환하여 저장함으로써 유효기간을 늘리는 방법이다. 그런데 이러한 방법은 인증서, CRL 등을 하나의 전자문서로 보고 개개의 전자문서별로 장기검증 대책을 제공하는 것으로 매우 비효율적인 방법이다.

지나간 과거의 인증서, CRL, 인증경로정보 등의 인증체계 자체에 대한 정보는 공개되는 정보이며 추후에 위조될 수 없도록 안전하게 보관되고 서비스되어야 한다. 현재의 인증체계 하에서 안전하게 보관되고 먼 훗날까지 원활하게 서비스된다면 각 문서의 장기검증에도 유용하고 효율적으로 사용될 수 있을 것이다.

III. 인증역사 서비스의 제안

1. 인증역사서비스의 정의

현재의 공개키기반구조에서는 현시점에서의 인증체계를 구축하고 서비스를 제공하는 것에 초점이 맞추어져 있고 역사적 관점에서의 인증서비스의 연속성에 대해서는 큰 고려를 하지 않고 있다. 물론 인증서비스의 연속성은 인증기관의 정책에 따라 얼마든지 다양한 방법으로 제공될 수 있겠지만 인증역사서비스(Certification history service)의 필요성과 요구사항을 분명히 정의하고 표준화된 방법으로 제공하는 것이 상호 호환을 위해 매우 중요할 것으로 생각된다.

이 논문에서는 인증서비스의 연속성을 제공하기 위해 인증기관이 기본적으로 제공해야 하는 서비스로서 인증역사서비스를 정의하고자 한다. 이 서비스는 다음과 같은 기능을 가져야 한다.

1) 유효기간이 지나서 인증기관의 인증서가 갱신되는 경우 이전의 인증서로는 더 이상 추가적인 서명행위가 이루어지지 않도록 봉인이 이루어져야 한다. 이를 위해 이전의 인증서로 발행했던 모든 사용자 인증서와 CRL들에 대해 해쉬값을 계산하고 이에 대해 새로운 인증서로 서명하여 공개한다.
2) 이전의 인증서로 발행된 모든 사용자인증서와 CRL등은 서명검증에 필요하므로 DB에 안전하게 보관되고 사용자의 요청에 따라 적절히 제공될 수 있는 정보시스템을 갖추어야 한다.
3) 인증기관의 현재시점의 인증서에는 과거인증서에 대한 명시적 유효성 인정이 제공되어야 한다. 이를 이용하여 현재시점의 인증기관 인증서에 대한 신뢰를 바탕으로 과거시점의 인증기관 인증서를 신뢰할 수 있게 되고 과거시점의 사용자 인증서까지 유효성을 검증할 수 있게 된다. 이를 위해 인증기관이 사용했던 모든 인증서들에 대해 리스트를 만들고 현재의 인증서로 서명하여 인증역사문서를 만들고 공개한다.

2. 인증역사서비스의 구현방법

인증기관은 인증역사서비스를 제공하기 위해서 다음과 같은 기능을 가져야 한다.

1) 인증기관 자신의 과거 인증서, 발행했던 CRL, 발급했던 사용자 인증서들에 대해 언제든지 검색해 볼 수 있도록 온라인 정보시스템을 갖추어야 한다.
2) 위와 같은 정보를 포함하는 인증역사문서를 만들고 현재의 인증서로 서명하여 온라인으로 공개한

다.

3) 인증기관의 현재의 인증서에는 위의 인증역사문서에 대한 링크가 제공되어야 한다. 이러한 링크는 인증서의 확장영역에 포함시킬 수 있다.

만일 일반 사용자가 과거의 인증서로 서명된 문서를 검증하려고 한다면 그 인증서의 유효성을 검증하기 위해서 인증기관이 발행한 인증역사문서를 참조하면 된다.

3. 인증역사서비스의 효과

인증기관이 서비스했던 과거의 인증역사에 대해 인증기관이 스스로 서명한 명시적인 문서가 제공된다면 전자서명의 장기검증 과정이 매우 단순화될 수 있다. TSA의 TS에 의존하는 복잡한 검증이 문서별 대책이라면 이것은 전체 인증역사에 대한 대책이며 인증기관으로서 필수적으로 제공해야 하는 서비스이다. 그러므로 사용자들이 문서별로 특별한 조치를 취하지 않더라도 과거의 서명된 문서들을 언제든지 간단히 검증할 수 있게 된다.

한편 과거 인증기관의 키가 누출되었거나 과거 사용되었던 암호시스템의 취약성이 발견되는 등의 경우에는 문서 위조의 위험성이 있으므로 RFC3126에 기반한 문서별 장기검증 대책이 여전히 유효하며 제안된 인증역사서비스와 동시에 사용되어야 할 것이다.

V. 결 론

이 논문에서는 전자서명의 장기검증 효율화 대책으로서 인증기관이 스스로 인증역사문서를 서명하여 발행함으로써 과거의 인증역사를 한번에 보증하도록 하는 새로운 방식을 제안하였다. 이런 서비스는 인증서비스의 연속성을 보장하기 위해 인증기관들이 제공해야 하는 가장 기본적인 서비스라고 생각된다.

참고문헌

[1] RFC 3126, Electronic Signature Formats for Long Term Electronic Signatures, http://www.ietf.org/rfc/rfc3126

[2] RFC 3280, Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile, http://www.ietf.org/rfc/rfc3280