DVCS를 이용한 전자서명 유효성 연장 방법에 관한 연구

국상진*, 허승호*, 민철홍*, 원동호**
*(주)한국무역정보통신
**성균관대학교 정보통신공학부
e-mail:twister@ktnet.com

A Study on the method of Digital Signature Validation using DVCS

Sangjin Kook*, Seung ho Huh*,
Cheolhong Min*, Dong-Ho Won**
*IT-Reaserch, Korea Trade Network
**School of Information and Communication Eng.,
Sungkyunkwan University

요 약

전자서명의 안전성은 사용된 전자서명 알고리즘과 키 길이가 가장 중요한 요소이다. 안전한 알고리즘의 선택은 물론이고, 적당한 키 길이를 선택하여만 안전한 전자서명을 활용 할 수 있게 된다. 일반적으로 알고리즘과 키 길이에 따라서 키 사용기간은 결정이 되며, 이로 인하여 특정 기간을 주기로 인증서를 다시 발급 받아야 하는 문제점이 존재한다. 또한 사용하지 않는 키로 검증을 수행 할 경우 전자서명 된 내용을 신뢰 할 수 없음은 물론이다. 본고에서는 전자서명 된 데이터의 유효성을 연장하는 방법에 대하여 제안 한다.

1. 서론

전자서명서비스는 인증서 기반의 로그인과 같은 기본적인 신원확인 서비스에서 출발하여 점차 다양한 영역으로 확장 적용되고 있다. 서명과 검증을 활용한 신원확인과 거래안정성 확보는 대다수 전자상거래 서비스에서 기본적으로 활용할 만큼 일반화되었으나, 전자서명의 적용대상 영역이 확장되어가며, 이전에는 예측하지 못했던 문제점들도 발생하고 있다. 본 연구에서는 전자서명의 유효기간과 전자서명 적용 대상의 보증기간이 다를때 발생하는 문제점을 분석하고 TTP 기반의 대안 방안을 제안해 본다.

2. 전자서명 인증서와 유효기간

전자서명을 실제 서비스에 적용하고자 할 때 발생하는 문제점은 여러 가지가 있다. 컴퓨팅 환경과 네트워크가 기본적으로 구비되어 있어야 한다는 환경적 조건과, 사람이 눈으로 확인할 수는 없고 애플리케이션의 도움을 받아야 한다는 기기 의존성 등이 대표적인 예이다. 최근에는 온라인 서비스에 전자서명을 적용하고자 할 때, 전자서명 검증키를 포함하고 있는 인증서가 보유하고 있는 자체적 한계도 문제점으로 많이 지적되고 있다.

일반적으로 전자서명 인증서에는 전자서명 검증키 이외에도 전자서명 키의 소유자에 대한 정보와 인증서 생성 정보, 안전성을 위한 인증서 유효기간 등도 포함되어 있다. 전자서명 인증서의 유효기간은 인증서가 사용하고 있는 전자서명 알고리즘의 종류, 사용하고 있는 키 길이 사용 목적 등에 따라 결정되는데, 이는 암호학적 안전성을 고려하여 결정하게 된다. 인증서의 유효기간이 지났다면 이 인증서는 사용하지 말아야 하며, 사용할 수 없게 된다.

인증서 기반의 전자서명을 활용함에 있어서 인증서 유효기간의 존재는 안전성을 확보한다는 측면에서 필요하지만, 인증서 유효기간이 지났을 경우 전

자서명을 검증할 수 없다는 문제점도 야기 시킨다. 그렇다고 강력한 알고리즘의 적용과 긴 키 길이를 이용하는 방법을 사용하여도, 길어지는 연산시간과 메모리의 사용량 증가와 같은 문제점이 발생하기 때문에 인증서 유효기간을 무한히 크게 설정할 수도 없다.

3. TTP를 이용한 내용증명 방식

TTP(Trusted Third Party)는 신뢰된 제삼자를 지칭하는 말로써 기관의 기술적, 윤리적 신뢰성을 전제로 다양한 서비스를 제공하는 기관이다. 온라인 상에서 TTP는 전자서명을 대신하여 특정 데이터에 대한 존재 여부를 알려 주는 서비스를 제공하기도 한다. TSA(Time Stamp Authority)와 DVCS(Data Validation and Certification Server protocol) 서비스 등이 바로 그러한 서비스이다.

- TSA

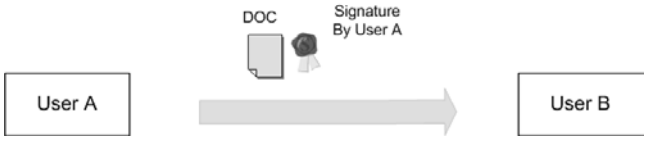
TSA는 특정한 시간에 특정한 정보가 존재하였음을, 신뢰된 시간 소스로부터 전달 받아 기록하여 주는 기관이다. TSA가 발급한 타임스탬프 토큰을 이용하여 이러한 사실을 증명 할 수 있게 된다.

- DVCS

DVCS는 TSA가 제공하는 정보의 존재에 대한 증명과 더불어 검증서비스를 제공한다. 이는 공개키 인증서 검증과 전자서명 데이터에 대한 검증을 포함하고 있다. DVCS의 일반적인 서비스는 다음과 같다.

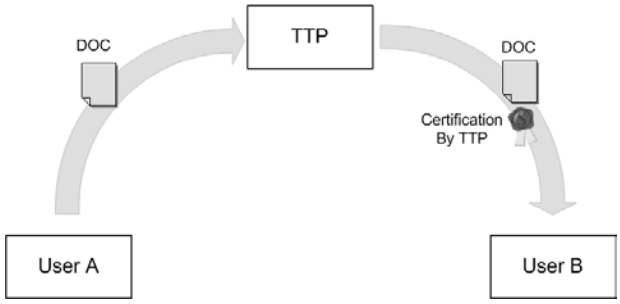
- CPD : Certification of Possession of Data
- CCPD : Certification of Claim of Possession of Data
- VSD : Validation of Digitally Signed Document
- VPKC : Validation of Public Key Certificates

DVCS의 Certification 서비스는 내용증명 서비스에 응용가능하며, 서비스의 결과로 생성된 DVC(Data Validation Certificate)는 증명서 혹은 보증서와 같은 역할을 수행 할 수 있다.



[그림 1] 일반적인 전자서명의 전달

[그림 1]은 일반적인 전자서명의 수행과 전달을 나타낸다. 이는 서명을 수행한 서명자(User A)가 전자서명을 받는 검증자(User B)에게 직접 전달하여, 자신의 전자서명으로 전달된 데이터에 대한 무결성을 제공 한다.



[그림 2] TTP를 이용한 전자서명의 전달

[그림 2]는 TTP를 이용하는 방식으로 내용증명 서비스에 해당된다. 서명자(User A)는 TTP에게 문서에 대한 증명을 요청하고 이를 검증자(User B)에게 전달함으로써 데이터의 존재 사실을 증명 할 수 있다. 이와 같은 내용증명 서비스는 신뢰를 제공하여야 하는 서비스에 적용가능하고, 검증자와 서명자 간에 서로 신원이 잘 파악되지 않거나, 보다 객관적인 증명이 필요 할 때 사용한다.

4. 장기서명 검증

PKI 기반 전자서명의 유효기간과 서비스 보증기간의 불일치 때문에 발생하는 문제점들을 해결하기 위해 여러 가지 방안들이 제안되고 있다.

IETF의 SMIME W/G에서 표준화 시킨 RFC3126(Electronic Signature Formats for long term electronic signatures)과 LTANS W/G에서 제안하고 있는 Merkle Tree를 응용한 방식인 ERS(Evidence Record Syntax)등이 대표적인 방안들이다. SURETY는 실제 상용 서비스를 제공하는 대표적인 사이트며, OpenEvidence 등의 프로젝트도 인증서 유효기간이 지난 이후에도 서명의 유효성 검증을 가능하도록 할 수 있는 방법들에 대한 연구를 계속하고 있다.

5. 제안하는 방법

TTP를 사용하는 경우에도 일반적인 전자서명 인증서를 사용한다면, 인증서 유효기간에 따른 문제

점이 그대로 나타난다. 다음에서 제안하고 있는 방식은 TTP의 역할을 하는 DVCS를 이용한 전자서명 유효성 연장에 관한 방안이다.

5.1 전제조건

TTP 기능을 수행하는 DVCS가 발급하는 DVC를 이용한 유효성 연장 방법은 다음과 같은 전제조건을 갖는다.

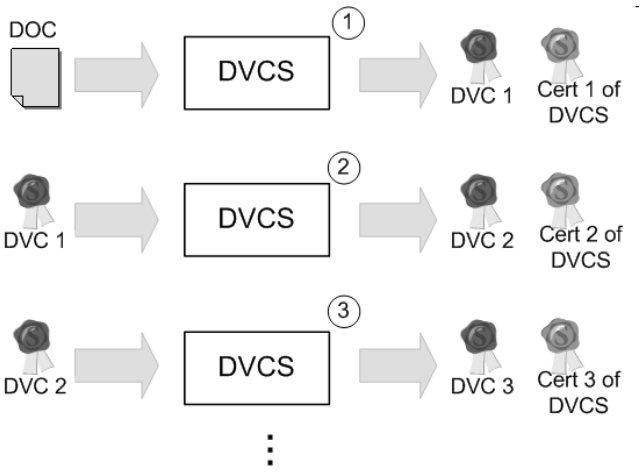
· DVCS는 CA로부터 DVCS가 서명할 전자서명인증서를 발급받고, 인증서는 적당한 유효기간을 갖는다.

· DVCS는 자기 자신의 인증서 만료 시점에 CA로부터 새로운 인증서를 발급 받아 사용한다.

· DVCS는 유효성 연장을 필요로 하는 모든 DVC에 대하여 갱신작업을 수행한다.

· DVCS는 자신이 발행한 모든 DVC를 쉽게 획득 할 수 있다. 자신이 발행한 모든 DVC에 대하여 갱신 가능 하도록 DVC를 보관한다.

5.2 DVCS를 이용한 DVC 갱신



[그림 3] DVC의 갱신 발급

① DVCS는 사용자로부터 요청받은 문서에 대하여 DVC1을 발급한다. (일반적인 DVCS의 DVC 발급 프로세스)

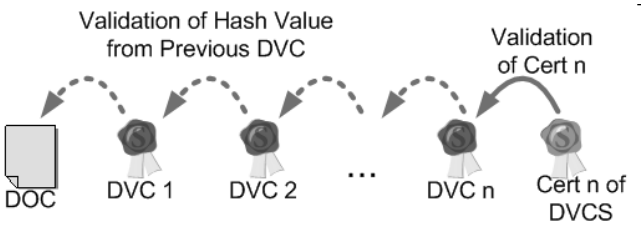
② DVCS의 인증서 만료에 따라 새로운 DVCS 인증서로 갱신하고, 기존에 발급했던 DVC1에 대하여 DVCSRequest를 이용하여 DVC2를 발급한다.

③ DVCS의 인증서 만료에 따라 새로운 DVCS 인증서로 갱신하고, 기존에 발급했던 DVC2에 대하여 DVCSRequest를 이용하여 DVC3를 발급한다.

④ 처음 요청 받은 문서의 종류와 정책에 의하여, DVCS 인증서 갱신이 일어날 때마다 DVC 갱신을 계속 수행한다.

5.3 DVC 검증

4.2에서 갱신 발급된 DVC들에 대한 검증 방법은 [그림 4]와 같이 수행 되어질 수 있다.



[그림 4] DVC 체인 검증 방법

① 검증자는 경로상의 모든 DVC, 요청문서(DOC), 가장 최근의 DVC를 서명한 DVCS의 인증서를 준비한다.

② DVCS의 인증서로 DVC를 서명 검증 수행한다.

③ n번째 DVC로부터 n-1번째 DVC의 정보를 확인한다. 이는 4.4에서 소개하는 구조를 이용한다.

④ 마지막 DVC 1을 이용하여 요청 문서와 비교한다.

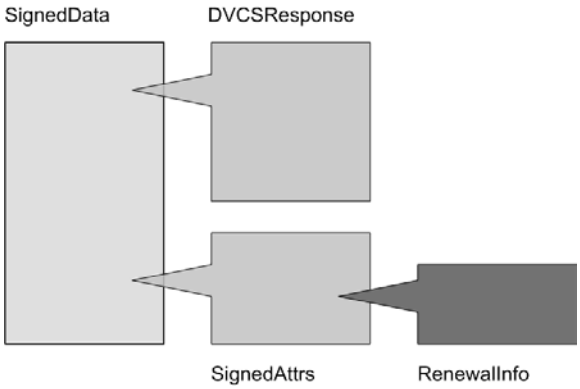
위의 방법이 모두 성공하였으면 DVC는 DVCS의 인증서 갱신 때마다 정상적으로 갱신을 하였으며, 갱신 하는 시점에 DVCS의 위협이 없었음을 확인 할 수 있다.

5.4 DVC 체인 구성 방법

DVC는 RSA의 메시지 표준인 PKCS#7 또는 CMS(Cryptographic Message Syntax)에서 정의 하고 있는 SignedData를 사용한다.

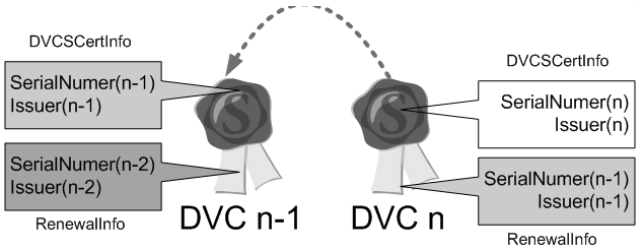
DVC 체인에 대한 구성정보는 [그림 5]의 RenewalInfo를 이용하여 나타낸다. 갱신하게 될 DVC는 그 자체가 DVCSRequest로 사용되기 때문에 체인 정보는 SignerInfo의 SignedAttrs를 이용하여 그 정보를 표현한다. RenewalInfo에는 갱신 전 DVC의 정보를 포함하게 되며, 다음과 같은 내용을 포함한다.

- 이전 DVC의 serialNumber
- 이전 DVC의 issuer



[그림 5] 체인 구성을 위한 정보 위치

다음의 [그림 6]은 RenewalInfo의 정보를 이용하여 DVC n-1과 DVC n과의 경로를 구성하는 방법이다. RenwalInfo는 근본적으로 먼저 발급된 DVC에 대한 정보를 포함한다.
SerialNumber는 DVCSCertInfo의 값을 사용하며, Issuer는 DVC를 발급한 DVCS의 DN을 사용한다.



[그림 6] DVC 체인의 비교대상

5.5 DVC의 구성

DVC가 사용하는 CMS의 ASN.1은 다음과 같으며, 제안하고 있는 RenewalInfo에 사용되는 Attribute는 다음과 같다.

```
SignerInfo ::= SEQUENCE {
  version              CMSVersion,
  sid                  SignerIdentifier,
  digestAlgorithm      DigestAlgorithmIdentifier,
  signedAttrs      [0] IMPLICIT SignedAttributes
                       OPTIONAL,
  signatureAlgorithm   SignatureAlgorithmIdentifier,
  signature            SignatureValue,
  unsignedAttrs    [1] IMPLICIT UnsignedAttributes
                       OPTIONAL }
Attribute ::= SEQUENCE {
  attrType    OBJECT IDENTIFIER,
  attrValues  SET OF AttributeValue }
```

[표 1] SignerInfo (RFC3852 CMS)

```
dvcs-rn ::= SEQUENCE {
  DVCIssuer GeneralNames    OPTIONAL,
  DVCSerialNumber SerialNumber OPTIONAL
}
SerialNumber ::= Integer
```

[표 2] Attribute 구조

6. 결론

전자서명과 전자서명 인증서에 관하여 이제 신문과 방송에까지 심심치 않게 등장하고 있다. 전자서명을 이용한 여러 가지 서비스들이 이제 자리를 잡아 가고 있고 보편적으로 전자서명이 필요하다고 사람들은 인식을 가지게 되었다.

전자서명의 여러 가지 장점에도 불구하고 아직도 불편함을 감수해야 하는 부분이 존재 하고 있다. 위에서 언급한 DVC 갱신 방법은 DVC를 발급하고 있는 DVCS가 자동적으로 DVC를 갱신함으로써 원본 문서 존재에 대한 보증을 긴 시간이 지난 이후에도 가능하게 한다. 또한 검증자는 DVC 체인을 구성함으로써 이를 검증 할 수 있다.

이러한 방식의 전자서명 유효성 연장방법은 현재 사용하고 있는 시스템에 쉽게 적용 가능하지만, 이는 DVCS에 의한 DVC 발급과 더불어 이를 보관하고, 서비스 해 줄 수 있는 방안이 함께 마련되어 적용되어야 한다.

참고문헌

[1] C. Adams, P. Sylvester, M. Zolotarev, R. Zuccherato "X.509 Internet Public Key Infrastructure Data Validation and Certification Server Protocols", RFC 3029, February 2001.

[2] Adams, C., Cain, P., Pinkas, D. and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001.

[3] Ralph C. Merkle, Protocols for Public Key Cryptosystems, IEEE Symposium on Security and Privacy, page 122-134, April, 1980.

[4] D. Brandner and Brian Hunter, "Evidence Record Syntax(ERS)", IETF Draft, 2004

[5] OpenEvidence, http://wwwopenevidence.org/

[6] SURETY, http://www.surety.com/