情 報 保 護 學 會 誌
第 11 券 第 6 號, 2001. 12

Time Stamping Service 기술 표준화 동향

임 영 숙*, 강 경 희*

요 약

Time stamping service는 데이터가 특정 시점에 존재하였다는 증거를 신뢰할 수 있는 제3의 기관(Trusted Third Party)이 제공해주는 서비스로서 e-Business가 활성화되면서 그 필요성이 부각되고 있는 서비스이다. Time stamping service 관련 기술은 ISO/IEC JTC1 SC27 WG2에서 표준화 작업이 진행되고 있으며 IETF PKIX WG에서는 RFC 3161로 표준문서가 나와있다. 본 고에서는 현재 표준 작업이 진행되고 있는 ISO/IEC JTC1 SC27의 time stamping service 기술을 중심으로 서비스 개요와 지난 2001. 10.16(화)~19(금) 서울에서 개최된 23차 SC27 기술 표준 회의에서 논의된 주요 쟁점 사항을 정리한다.

Ⅰ. 서 론

인터넷 사용 인구가 급증하면서 인터넷을 통한 e-Business가 팽창일로에 있다. 인터넷을 안전하고 믿을 수 있는 정보 통로로 만들기 위하여 많은 정보 보호 기술 및 장치들이 제시되고 있으며 특히 공개키 기반(PKI, Public Key Infrastructure)의 전자 서명 보안 기술은 서명 생성자에 대한 신원 증명이나 전자 데이터의 무결성 증명 등이 가능한 보안 기술로서 국내에서도 이미 전자서명법 시행에 따라 확산되고 있는 중이다.

그러나 전자 서명 기술 독자적으로는 완벽한 보안 장치가 될 수 없으며 특히 부인 방지를 위해서는 전자 서명 생성 시점과 같은 별도의 증빙 데이터가 요구된다. 또한 중요 연구 결과 자료나 창작물, 설계서, 계약서와 같은 데이터들은 그 내용이 변조되지 않았으며 특히 어느 시점에 존재했는가에 대한 정보가 매우 중요하다.

Time stamping service(이하 시점확인서비스)는 데이터가 특정 시점에 존재하였다는 증거를 신뢰할 수 있는 제3의 기관(Trusted Third Party)이 제공해주는 서비스로서 현재 ISO/IEC JTC1 SC27 WG2와 IETF PKIX 작업반에서 국제 표준화 작업이 진행되고 있으며 미국, 캐나다 등에서 서비스가 제공되고 있다.

본 고에서는 ISO/IEC JTC 1/SC 27 WG2에서 논의하고 있는 TSS 표준 기술에 대한 전반적인 사항을 논의하고, 지난 2001. 10.16(화)~19(금) 서울에서 개최된 23차 SC27 기술 표준 회의에서 논의된 주요 쟁점 사항에 대해 기술하고자 함으로써 관련 기술의 구현 및 표준 연구에 기여하고자 한다.

Ⅱ. Time Stamping Service 개요

1. 서비스 전제 사항

시점확인 서비스는 전자 데이터와 특정 시점을 암호학적으로 연결시켜서 데이터의 존재 시각과 데이터에 대한 변조 여부를 확인할 수 있는 시점 토큰(time stamping token)을 생성하는 서비스로서 전자 데이터의 생성, 유통, 저장/관리 과정에서 데이터의 존재 시점이나 그 내용이 변조되지 않았음을 어떻게 객관적으로 입증할 것인가 하는 것에 대한 솔루션으로 대두된 기술이다.

이와 같은 시점 확인 서비스는 다음과 같은 항목을 기본 전제 조건으로 요구하고 있다.

① 임의의 데이터가 특정 시점에 존재하였음을 객관적으로 증명하기 위해서, 위조 불가능(non-forgeable)한 방법을 사용하여 해당 데이터와 Time Stamping Authority(이하 TSA)가

* 한국통신 멀티미디어연구소 ({ylim, puppycat}@kt.co.kr)

제공하는 시간 값을 결합시켜야 한다.
② 데이터 전송 시, 해당 데이터가 노출되지 않아야 한다.

실제적인 서비스 적용 단계에서 상술된 전제 사항은 원시 데이터의 해쉬 값을 사용함으로써 데이터가 드러나는 것을 방지하여 궁극적으로 데이터의 무결성(integrity)을 확보하게 되며, 도출된 해쉬 값과 TSA가 제공하는 시간 값을 다양한 암호 기법을 통해 결합함으로써 데이터에 대한 무결성과 서버 인증(authenticity)을 보장할 수 있게 된다.

2. Service Entity 유형

시점 확인 서비스와 관련된 주체(entity) 유형은 크게 서비스를 제공하는 TSA와 서비스를 사용하는 사용자로 분류할 수 있다. 각 주체별 정의/기능을 기술하면 다음과 같다.

◎ TSA

TSA는 특정시점에서의 데이터 존재를 증명할 수 있는 시간정보를 제공하는 주체로서 신뢰할 수 있는 제 3의 기관(trusted third party)이 수행한다. TSA는 제공하는 시간정보에 대한 정확성을 보장해야 한다.

◎ 서비스 사용자

데이터를 소유하고 있으며 시점 확인 서비스를 요청하는 시점 확인 요청자(time-stamping requester)와 데이터를 소유하고 있으며 데이터에 대한 존재시점과 내용의 무결성을 검증하고자 하는 시점 검증자(time-stamping verifier)로 세분된다.

3. 시점 토큰

시점 토큰(time-stamp token)은 특정 시점에 데이터가 존재하였다는 증거를 제공해 주는 토큰으로, 이러한 증거는 시점 확인 요청자가 제출한 데이터의 해쉬 값과 데이터의 인증 기법이 결합되어 생성된다. 시점 토큰 생성과 관련하여 SC27에서는 다음과 같은 사항을 정의하고 있다

또한 다음과 같은 상황에서는 기 생성된 시점 토큰을 갱신할 것을 권장하고 있으나, 구체적인 갱신 메커니즘은 기술하지 않고 있다.

① TSA의 전자서명 키가 만료될 경우
② TSA가 교체되는 경우
③ 시점 확인 요청자가 사용한 해쉬 함수에 문제가 있는 경우

항 목	내 용	비 고
토큰 유형	Independent token	IETF에서도 정의됨
	Linked token	-
인증 기법	Digital signature mechanisms	IETF에서도 정의됨
	Message Authentication Mechanisms	-
	Archiving Mechanisms	-

4. Entity간의 통신

시점 확인 서비스는 크게 시점확인 요청자가 TSA에게 시점 확인 서비스를 요청하여 TSA가 시점 토큰을 생성하고, 생성된 토큰을 서비스 요청자에게 전달해 주는 시점 확인 서비스와 시점 토큰이 정확한지를 검증하는 시점 검증 서비스로 구분된다.

4.1 시점 확인 서비스 절차

이 서비스는 다음과 같은 일련의 단계를 수행한다.

1. 시점 확인 요청자는 다음과 같은 데이터를 포함한 요청 메시지를 TSA에게 전송한다.
   - 해쉬값(hash value)
   - 사용된 hash algorithm
   - nonce
2. TSA는 수신된 시점확인 요청 메시지를 검사한다.
3. TSA는 다음과 같은 데이터가 포함된 시점 토큰을 생성한다.
   - 요청자가 보낸 데이터(해쉬값, 해쉬 알고리즘, nonce 등)
   - 시각 정보
   - 요청자가 보낸 데이터와 시각 정보를 암호학적으로 연결한 정보
4. TSA는 요청자에게 시점 토큰을 전송한다.
5. 요청자는 수신한 시점 토큰을 검증한다.

4.2 시점 검증 서비스 절차

시점 검증 서비스는 기 발행된 시점 토큰의 유효성을 검증함으로써 해당 데이터의 존재 시점과 토큰 발행 시점이후 데이터의 내용이 변조되지 않았음을 증명해주는 서비스이다. 시점 검증 절차는 시점 토큰의 인증 기법에 따라 TSA와는 독립적으로 이루어지거나 혹은 TSA에게 시점 토큰 검증 의뢰를 하고 그 결과를 받음으로써 이루어진다.

시점 토큰 검증 절차는 기본적으로 검사하고자 하는 시점 토큰에 포함된 정보를 사용한다. 그러나 linked token의 경우 검증하고자 하는 토큰 외에 TSA가 부수적으로 생성하는 토큰을 함께 사용하여 수행한다.

5. 메시지 구조

5.1 시점 확인 서비스의 메시지 구조

서비스 사용자와 TSA간의 교환되는 메시지로는 서비스 요청자가 TSA에게 전송하는 시점 확인 요청 메시지와, TSA가 그 결과로서 서비스 요청자에게 전송하는 서비스 응답 메시지가 있다.

```
TimeStampReq ::= SEQUENCE  {
  version            INTEGER  { v1(1) },
  messageImprint   MessageImprint,
  reqPolicy          TSAPolicyId  OPTIONAL,
  nonce              INTEGER    OPTIONAL,
  certReq            BOOLEAN    DEFAULT FALSE,
  extensions     [0] IMPLICIT Extensions  OPTIONAL
}
```

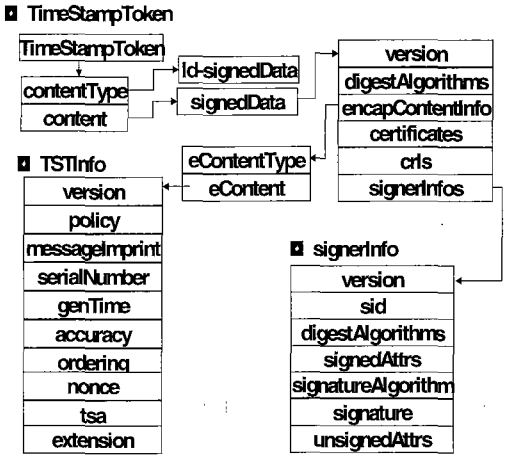
```
TimeStampRes ::= SEQUENCE  {
  status                PKIStatusInfo,
  timeStampToken    TimeStampToken OPTIONAL
}
```

5.2 시점 토큰

시점 확인 서비스의 결과는 시점 토큰의 수신으로 볼 수 있으며, 수신된 시점 토큰은 서비스 응답 수신 시점 또는 미래의 어느 시점에서 해당 데이터의 존재시점과 무결성 증명을 위하여 토큰 검증 절차를 거치게 된다. 토큰 검증은 시점 토큰이 TSA가 생성한 시점 토큰임을 증명하는 인증 과정을 포함하게 되는데, 토큰 생성/인증 기법에 따라 다음 3가지 유형으로 나뉘어 진다.

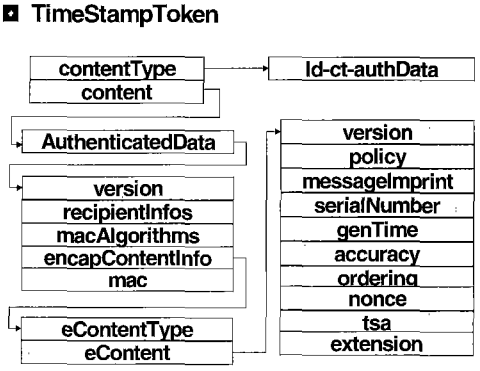
◎ 전자서명기법의 시점 토큰

시점 토큰의 인증을 위하여 전자서명 기술을 이용하는 기법이다. 이 기법으로 생성된 시점 토큰은 토큰 검증 작업이 TSA와 독립적으로 수행될 수 있다.



◎ MAC 기법의 시점 토큰

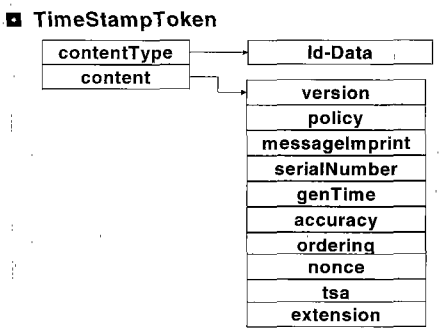
시점 토큰의 인증을 위하여 MAC(Message Authentication Code)를 이용하는 기법이다. 이 기법을 사용하여 생성된 토큰의 검증은 TSA가 수행하여야 한다.



◎ Archiving 기법의 시점 토큰

시점 토큰 내에 별도의 인증 정보를 포함하지 않는다. 따라서 이 기법을 사용하는 경우 서비스 응답

메시지 수신시 별도의 보안 채널이 필요하게된다. 시점 확인 서비스 이용 시점이후 시점 토큰을 검증해야 할 경우에는 토큰을 발행한 TSA만이 검증 작업을 수행할 수 있다.



5.3 시점 검증 서비스의 메시지 구조

시점 검증 서비스는 시점 토큰의 유효성 검사를 TSA에게 의뢰하는 서비스이다. 시점 검증자는 TSA에게 시점 검증 요청 메시지를 보내고 그에 대한 응답으로 검증 결과 메시지를 수신한다.

```
ValidateRequest ::= SEQUENCE {
    version          INTEGER {v1(0)},
    tst              TimeStampToken,
    requestID[0]     OCTET STRING OPTIONAL
}
```

```
ValidateReply ::= SEQUENCE {
    version          INTEGER {v1(0)},
    status           PKIStatusInfo,
    tst              TimeStampToken,
    requestID[0]     OCTET STRING OPTIONAL
}
```

Ⅲ. Time Stamping Service 표준화 동향

1. 표준 현황

시점 서비스는 2개의 국제 표준화기구에서 기술 표준화 작업이 진행되고 있다.

ISO/IEC JTC 1/SC 27 WG2에서는 time stamping service 기술 분야를 〔표1〕과 같이 세 부분으로 나누어 표준화 작업을 수행하고 있다.

〔표 1〕 JTC1 SC27 TSS 표준화 현황

문서 번호	표준상태	문서명
SC27 N2910	Final CD	ISO/IEC 18014-1 Time stamping services - Part 1 Framework
SC27 N2912	First CD	ISO/IEC 18014-2 Time stamping services - Part 2 Mechanisms producing independent tokens
SC27 N2914	Third WD	ISO/IEC 18014-3 Time stamping services - Part 3 Mechanisms producing linked tokens

상기 표를 통해서 파악할 수 있는 것처럼 Part1에서는 TSS에 관련된 일반적인 사항과 서비스에 대한 기본 골격에 대하여 서술하고 있다. Part2와 Part 3에서는 Part 1에서 정의된 기본 서비스 골격을 바탕으로 각각 독립 시점 토큰 생성 기술 및 연계 토큰 생성 기술에 대하여 서술하고 있다.

IETF PKIX WG2에서는 SC27보다 먼저 표준 작업을 시작하였으며 2001년 8월 RFC 3161로 표준 작업을 사실상 마무리한 상태이다.

〔표 2〕 IETF PKIX의 TSS 표준 현황

문서 번호	표준상태	문서명
RFC 3161	RFC	Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)

2. 서울 회의의 주요 쟁점 사항

제 23차 SC 27/WG 2 회의는 서울 ASSEM Tower에서 acting Convener R. Müller(독일)에 의해 문서번호 N2970 rev1(=WG2/ N468rev1) "Draft agenda for 23rd SC27/WG2 meeting in Seoul Republic of Korea, 2001-10-16/19"에 따라 진행되었으며, 회의의 결의 사항들은 10월 19일에 작성된 SC27 N3071 "Resolutions of the 23rd SC27/WG2 meeting in Seoul, Korea 2001-10-16/19"에 정리되었다.

서울 회의 이전에 개최된 제22차 Oslo 회의의 주요 쟁점은 동 학회지 제11권 3호(2001년 6월)에 나와있음으로 이를 참고하시기 바란다.

서울 회의는 9.11 테러 여파로 회의 참석인원이 적었다. 이번 회의에서는 그동안 논의된 기술 사항들이 Part 3 연계토큰 생성기법의 linking에 대한 검토 외에는 대체적으로 정리가 되었다. 특히 ASN.1 표기는 TSS 전 표준 문서에 대하여 정리하여 표준에 반영하였다.

이하 각 표준 과제별로 중요 논의 사항을 정리한다.

27.01 Time Stamping Services - Part 1 : Framework

〈 검토기술자료 〉

N2977 SoV on ISO/IEC FCD 18014-1(SC27 N2910), 2001-10-04

N2910 ISO/IEC FCD 18014-1, 2001-05-29

Time stamping Service part1 (first CD 18014-1)을 final DIS로의 승격에 대한 안건과 표준 문서에 기술된 ASN.1 표기를 전체적으로 재정리하기로 하였다. 주요 논의사항을 정리한다.

- final DIS ballot 하기로 함.
- 현재 time stamping service 표준 문서는 IETF 문서로부터 ANS.1 표기를 차용해서 표기하고 있음. 이번 서울회의에서 WG2에서 작업하는 표준은 ISO/IEC 표준이란 주장과 전체적으로 time stamping 메시지구조에 대한 ASN.1 표기가 불충분하다는 미국 안을 수용하고 Part1에 사용된 ASN.1 notation을 재정비하여 표준에 싣기로 하였다.
- 시점토큰 검증의 validation, verification 용어의 혼용을 verification으로 정확히 사용하기로 함
- 문서내의 절, 부록의 번호를 본문과 별도의 체계로 가져가기로 함.
- 그 외 각국의 기고문을 검토하고 기술 사항을 논의함.

27.02 Time Stamping Services - Part 2 : Mechanisms producing independent tokens

〈 검토기술자료 〉

N2964 SoV on ISO/IEC CD 18014-2(SC27 N2912), 2001-09-24

N2912 ISO/IEC CD 18014-2, 2001-06-07

Time stamping Service part2 (first CD)를 final CD로의 승격에 대한 안건과 표준 문서에 기술된 ASN.1 표기를 전체적으로 재정리하기로 하였다. 주요 논의사항을 정리한다.

- final CD ballot 하기로 함
- 현재 time stamping service 표준 문서는 IETF 문서로부터 ANS.1 표기를 차용해서 표기하고 있음.
  Part1 회의에서 이미 논의한 바처럼 ASN.1 표기를 관련 표준의 최신 버전에 맞게 수정하여 싣기로 함.
- validation, verification 용어의 차이에 대하여 논의. validation 은 time stamp request에 대한 response를 검증하는 것이고, verification 은 나중에 time stamp token을 검증하는 절차를 지칭하는 것으로 결론.
- validation, verification 모두 TSA의 인증서가 토큰 발행 시에 유효함(했)음을 검사하여야 함.
- 한국은 general comment 1, technical comments 3개, editorial comments 7제안.
- Technical comments 및 editorial comments는 accept됨.
- general comment는 time stamp token의 reissuing에 대한 comment였음. Token reissue는 part2, part3 방식 모두에 적용되는 상황이어서 part2 가 아닌 part1에 대한 comment로 변경해서 논의. 그러나 reissue가 필요한 상황은 너무나 다양하기 때문에 표준에서 전부 다루는 것은 힘들고 이는 구현상의 문제다라는 editor 주장이 받아들여져서 표준에서는 제외됨.
- 그 외 각국의 용어 추가 및 수정, 기술적 comment들을 검토하였으며, 대부분 accept됨.

27.03 Time Stamping Services - Part 3 : Mechanisms producing linked tokens

〈 검토기술자료 〉

N2982 U.S National body proposal for a co-Editor for project 1.27.27.03, 2001-09-14

N2979 SoC on ISO/IEC 18014-3(SC27 N2914), 2001-10-04

N2914 ISO/IEC 3rd WD 18014-3, 2001-08-08

서울회의에서는 미국 대표 Dimitri Andivahis 씨가 part 3의 editor로 추인되었다. SC27 회의는 Editor 주관으로 진행되며 표준에 반영 여부가 editor에 의해 좌우되는 경우도 많은데, Mr. Andivahis는 시점 확인 서비스를 제공하는 미국 Surety사 직원으로 그 회사의 기술이 표준으로 반영될 것으로 예견된다.

기술 논의 사항으로는 Time stamping Service part3 (third WD)를 first CD로의 승격에 대한 안건과 지난 Oslo 회의에서 의결사항이었던 linking과 aggregation에 대하여 논의하였으나 주 기고국인 에스토니아 대표의 불참으로 다음 회의에서 논의될 예정이다.

주요 논의사항을 정리한다.

- Co-Editor 추인
- Part3를 first CD ballot 하기로 함.
- aggregation, linking 기법에 논의함. 그러나 기고국인 Estonia가 불참함으로써 이에 대한 논의가 충분히 이루어지지 않음.
- 표준 본문에 time stamp request, validation, verification에 대한 설명을 싣기로 함.
- Linking, aggregation, publishing에 대하여 구현 측면을 고려하여 더욱 정확하게 설명하기로 함. 또한 각 operation의 신뢰도의 level에 대한 정보를 부록에 데이터 등을 포함해서 보충 설명하기로 함.
- 그 외 각국의 comments 검토함.

Ⅳ. 결 론

본 고에서는 ISO/IEC JTC1 SC27에서 현재 표준 진행중인 시점 확인 서비스를 중심으로 서비스 전반에 대한 사항을 기술하였다.

시점 확인 서비스와 관련된 기술은 IETF에서는 올해(2001년) 8월에 RFC(RFC 3161 Time Service Protocol)가 되었으며, JTC1 SC27에서는 지난 서울 회의에서 part1, 2, 3에 대하여 각각 final DIS, final CD, first CD로 상정하기로 함으로써 part3를 제외한 part1,2는 기술적으로는 사실상 표준이라 할 수 있다.

그러나 Part3는 세부적인 메커니즘 부분에서는 앞으로도 많은 연구가 지속되어야 할 것으로 판단되며, 이외에도 서비스 구현이나 운용 측면에서 시점 토큰의 재발행(renewal)은 재발행 요청/응답 및 TSA에서 어떤 방식으로 서비스를 제공할 것인가에 대한 보다 세부적인 프로토콜 제시를 위한 연구가 진행되어야 할 것이다.

더불어 IETF와 달리 ISO에서는 독립 토큰 생성 기법에서 MAC, archiving 이라는 두 가지 유형의 토큰 생성/인증 기법을 추가로 제시하고 있는데, 현실적으로 이러한 기법 적용이 타당한 것인지에 대한 논의가 필요하며, 마지막으로 linked token에 대한 보다 세부적인 메커니즘 제시하는 데에 향후 연구가 집중되어져야 할 것으로 판단된다.

참 고 문 헌

[1] ISO/IEC JTC 1/SC 27 N2910, Information technology - Security techniques - Time stamping services - Part 1: Framework, 2001-05-29

[2] ISO/IEC JTC 1/SC 27 N2912, Information technology - Security techniques - Time stamping services - Part 2: Mechanisms producing independent tokens, 2001-06-07

[3] ISO/IEC JTC 1/SC 27 N2914, Information technology - Security techniques - Time stamping services - Part 3: Mechanisms producing linked tokens, 2001-08-08

[4] ISO/IEC JTC 1/SC 27 N2715, Information technology - Security techniques - Time stamping services - Part 1: Framework, 2001-03-08

[5] ISO/IEC JTC 1/SC 27 N2717, Information technology - Security techniques - Time stamping services - Part 2: Mechanisms producing independent tokens, 2001-01-26

[6] ISO/IEC JTC 1/SC 27 N2719, Information technology - Security techniques - Time stamping services - Part 3: Mechanisms producing linked tokens, 2001-01-19

[7] ISO/IEC JTC 1/SC 27 N2977 Summary of voting on ISO/IEC FCD 18014-1 (SC27 N2910), 2001-10-04

[8] ISO/IEC JTC 1/SC 27 N2964 Summary of voting on ISO/IEC CD 18014-2 (SC27

N2912), 2001-09-24
[9] ISO/IEC JTC 1/SC 27 N2979 Summary of comments on ISO/IEC 18014-3 (SC27 N2914), 2001-10-04
[10] ISO/IEC JTC 1/SC 27 N3071 Resolutions of the 23rd SC 27/WG 2 meeting in Seoul, Korea 2001-10-16/19.

〈著者紹介〉

임 영 숙 (Young Sook Lim)

1987년 2월 : 연세대학교 전산과학과
1989년 2월 : 한국과학기술원 전산과 석사
1989년 3월~1998년 7월 : 한국통신 통신망연구소
1998년 7월~현재 : 한국통신 멀티미디어연구소
관심분야 : PKI 기반의 정보보안 및 응용서비스, 차세대 통신망의 정보보안

강 경 희 (Kang Kyung Hee)

1991년 2월 : 한국외국어대학교 경영정보학과
1993년 2월 : 한국외국어대학교 경영정보학과 석사
1993년 3월~현재 : 한국통신 멀티미디어 연구소
관심분야 : PKI기반의 응용서비스 개발