通信情報保護學會誌
第 10 券 第 4 號, 2000. 12

타임스탬프 서비스 동향 분석

홍 기 윤*

요 약

본 논문에서는 전자서명법 제20조에서 명문화된 시점확인서비스(타임스탬프)에 대한 동향을 분석하였다. 현재 타임스탬프 서비스는 IETF PKIX에서 1997년 처음 인터넷 드래프트가 발표된 이후 RFC로 표준화가 추진 중이며 ISO/IEC JTC1/SC27에서도 표준화가 추진 중이다. 공개키기반구조의 필수적 요소로서 전자서명 인증 서비스와 함께 구현이 필요한 타임스탬프 서비스에 대한 표준화 동향 및 타임스탬프 서비스 프로토콜에 대한 분석과 국외 서비스 업체의 서비스 제공 현황을 분석하여 타임스탬프 응용 서비스 개발에 활용할 수 있도록 작성하였다.

Ⅰ. 서 론

전자상거래는 기존 거래 방식에서 시간적·공간적 제약의 문제점을 해결해줌으로써 새로운 거래 문화로서 자리잡아 가고 있지만 많은 장점을 가지고 있음에도 불구하고, 거래정보의 노출, 거래 사실의 부인 등에 대한 보안 요구사항이 먼저 해결되어야만 전자적 거래의 활성화를 기대할 수 있을 것이다.

공개키기반구조 환경에서 전자서명을 통한 전자적 거래시 데이터 및 데이터의 생성 시간, 교환 등 이들 사이의 관계를 확립할 필요성이 여러 가지 상황에서 발생하게 되고 특히 디지털 데이터는 물리적으로 생성시점을 확인하는 것이 불가능하므로 전자적인 타임스탬프 서비스 과정을 통하여 생성 및 존재 증명이 필요하게 되었다.

분쟁시 거래 당사자들이 제시한 증거의 기준을 결정할 수 없기 때문에 부인방지 서비스에는 양측이 합의하는 제3의 신뢰기관이 항상 필요하고 타임스탬프 기관(TimeStamp Authority, TSA)은 디지털 데이터가 특정 시간에 존재하고 있었다는 내용을 증명해 주는 것으로 전자문서와 관련된 당사자간의 부인방지 서비스 (non-repudiation)를 제공하는 제3의 신뢰기관 역할을 수행할 수 있다.

본 논문에서는 공개키기반구조의 필수적 요소로서 전자서명에 대한 인증서 발행 서비스와 함께 구현이 필요한 타임스탬프 서비스에 대한 국제 표준화 동향과 선진 외국의 서비스 동향을 분석한다.

Ⅱ. 타임스탬프 서비스 프로토콜 표준화 동향

현재의 타임스탬프 서비스 프로토콜은 타임스탬프 서비스를 제공하는 업체나 연구 프로젝트를 수행중인 대학, 연구소 등에 따라 서로 차이를 보이고 있어 호환성에 문제가 있다. 이러한 호환성 문제를 해결하기 위하여 공개키기반구조 관련 표준화 활동에서 타임스탬프 서비스에 대한 표준화도 같이 추진되고 있다. 본 장에서는 ISO/IEC JTC1/SC27과 IETF P에서 추진되고 있는 타임스탬프 서비스 표준화 동향에 대해 분석해 본다.

1. ISO/IEC JTC1/SC27의 표준화 동향

ISO/IEC JTC1/SC27에서 추진되고 있는 타임스탬프 표준화는 1998년 10월에 스페인의 AEONR가 SC27 N2107 "Guidelines on the use and *management of time stamping services*"를 통해 타임스탬프 서비스와 관련된 새로운 연구 아이템을 제안하였고 1999년 3월 SC27 N2178 "Ti stamping services and protocols"이 NP work item Prorosal)로 제안되어 1999년 5월

* (주)케이사인 대표이사 (kyhong@ksign.com)

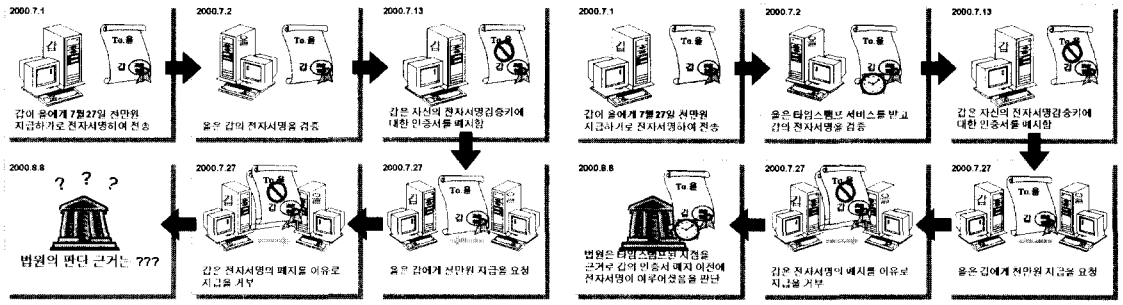

그림 1. 타임스탬프 서비스의 효용성

드래프트(WD)로 채택되었다. 3번의 갱신 작업 후 1999년 11월 15일에 제안된 SC27 N2439 표준안에서 3개의 파트로 나누어 Part 1 Frame- work, Part2 Mechanisms producing independent tokens, Part3 Mechanisms producing linked tokens으로 표준화를 추진하기로 하였으며 이에 따라 타임스탬프 서비스 표준화 프로젝트인 1.27.27 "Time stamping Services"는 3개의 세부 프로젝트로 조정되었다.

표 1. SC27 타임스탬프 서비스 표준(안) 문서

문서번호	제출 일시	문서타입
N2178	1999.3	Working Document
N2323	1999.5.	Working Draft 18014
N2357	1999.7	Working Draft 18014
N2439	1999.11	Working Draft 18014
N2595	2000.5	Working Draft 18014-1
N2596	2000.5	Working Draft 18014-2
N2597	2000.5	Working Draft 18014-3
N2715	2000.11	Committee Draft 18014-1
N2717	2000.11	Working Draft 18014-2
N2719	2000.11	Working Draft 18014-3

기존 문서의 내용으로 구성된 Part 1 Frame-work와 Part2 Mechanisms producing independent tokens, Part3 Mechanisms producing linked tokens인 타임스탬프 서비스 표준(안)의 문서 구성은 다음과 같다.

○ N2595 : Time stamping services - Part 1 Framework (WD18014-1)

1. Scope
2. Normative References
3. Definitions
4. General Discussion on Time-stamping
5. Communications between entities involved
6. Message Formats

Status Message and Failure Codes

Patent Information

○ N2596 : Time stamping services - Part 2 Mechanisms producing independent tokens (WD 18014-2)

1. Scope
2. Normative References
3. Definitions
4. General Discussion
5. Entities of the Time-Stamping Process
6. Data Structures
7. TSA signs with a public key
8. TSA signs with a secret key
9. TSA keeps recorded evidence

○ N2597 : Time stamping services - Part 3 Mechanisms producing linked tokens (WD 18014-3)

1. Scope
2. Normative References
3. Definitions
4. General Discussion
5. Building Blocks
6. The Time-stamping Process

표 2. SC27 타임스탬프 서비스 표준화 진행사항

프로젝트 번호	프로젝트명	프로젝트 에디터	추진일정	
1.27.27.01	Time staming services -Part1 Framework	Roland Müller	WD	1999. 5
			CD	2000.11
			FDIS	2001.11
			IS	2002. 5
1.27.27.02	Time staming services -Part2 Mechanisms producing independent tokens	Mike Matyas	WD	2000. 5
			CD	2001.11
			FDIS	2002.11
			IS	2003. 5
1.27.27.03	Time staming services -Part3 Mechanisms producing linked tokens	Wes Doonan	WD	2000. 5
			CD	2001.11
			FDIS	2002.11
			IS	2003. 5

7. Data Structures
Annex A. Bibliography

2000년 4월에 London회의에서는 타임스탬프 서비스 프로토콜 형식을 IETF PKIX 표준(안)으로 준용하는 방향으로 결정하였으며 타임스탬프 서비스 절차 중 TDA 부분을 표준 문서에서 삭제하기로 결정하였다. 프로젝트 에디터의 변경 등에 따라 표준화 진행이 1년 정도씩 늦추어지게 되었으며 10월 Tokyo회의 결과로 18014-1 Part 1 : Frame- work는 CD로 추진되었으며 Part 2, Part 3는 검토하여 2001년 2월 28일까지 의견을 수렴하기로 결정하였다.

2. IETF PKIX의 표준화 동향

공개키기반구조에 대한 연구를 수행 중인 IETF의 PKIX(Public-Key Infrastructure : X.509) 작업반에서는 Entrust사의 C. Adams, BBN사의 P. Cain, Bull사의 D. Pinkas, Entrust사의 R. Zuccherato가 제안한 타임스탬프 서비스 프로토콜 인터넷 드래프트 "Internet X.509 Public Key Infrastructure Time Stamp Protocol"의 표준화 추진이 진행되고 있다. IETF PKIX에서는 메일링 리스트를 통해 표준(안)에 대한 의견 교류가 활발히 이루어지고 있으며 표준(안)에 직접 반영이 되고 있어 ISO/IEC JTC1/SC27보다 표준화 추진이 빠르게 진행되고 있다.

인터넷 드래프트의 경우 IETF에 의해서 발표되어 의견 수렴이 이루어지는데 표준(안)은 6개월 동안 유효하며 6개월이 지나도 RFC로 채택되지 않으면 internet-draft 디렉토리에서 제거된다. 언제라도 인터넷 드래프트는 같은 명세서의 최근 버전으로 교체되며 다시 6개월의 유효기간을 갖게 되는데 타임스탬프 서비스 프로토콜에 관한 인터넷 드래프트도 1999년 5월부터 2000년 11월 현재까지 12차례의 갱신이 진행되고 있으며 RFC 채택을 추진중이다.

표 3. IETF PKIX 표준화 진행사항

제출 일시	파일명
1997. 11. 7.	draft-adams-time-stamp-00
1998. 3. 12.	draft-adams-time-stamp-01
1998. 6. 4.	draft-adams-time-stamp-02
1998. 9. 23.	draft-ietf-pkix-time-stamp-00
1999. 5.	draft-ietf-pkix-time-stamp-01
1999. 6.	draft-ietf-pkix-time-stamp-02
1999. 9.	draft-ietf-pkix-time-stamp-03
1999. 10.	draft-ietf-pkix-time-stamp-04
2000. 1.	draft-ietf-pkix-time-stamp-05
2000. 3.	draft-ietf-pkix-time-stamp-06
2000. 4.	draft-ietf-pkix-time-stamp-07
2000. 6.	draft-ietf-pkix-time-stamp-08
2000. 6.	draft-ietf-pkix-time-stamp-09
2000. 10.	draft-ietf-pkix-time-stamp-10
2000. 10.	draft-ietf-pkix-time-stamp-11
2000. 11.	draft-ietf-pkix-time-stamp-12

타임스탬프 서비스 기관의 요구사항, 타임스탬프 서비스 프로토콜의 형식, 메시지 전송 메커니즘, 보안 고려사항, TDA(Temporal Data Authority) 지원 내용 삭제, 서명된 토큰 자체의 외부 이동 상태, 해쉬 순서 지원 삭제, TST time 형식 변경 등 지속적인 갱신이 이루어진 인터넷 드래프트의 주요 변경 사항은 다음과 같다.

- 01 버전에서 02 버전의 변경 사항
  - 기존 TST(Time Stamping Token) 내부 상태 정보 필드의 위치 변경
  - 보안 고려사항에 대한 수정
  - precisionFactor 의 INTEGER 형식에서 BIT STRING으로 변경
  - TDA 개념에 대한 문서 수정
  - "Waiting" 상태 정보 사용에 대한 명시
  - Serial Number 사용에 대한 명시
  - CMP Encapsulation에 대한 명시
  - SEQUENCE OF MessageImprint에 대한 명시
  - extended key usage의 Criticality에 대한 명시
  - TSA name에 대한 명시
  - AIA(Authority Information Access) OID에 대한 명시

- 02 버전에서 04 버전의 변경 사항
  - 타임스탬프 시간의 GeneralizedTime 및 선택 필드인 accuracy로의 구성
  - Serial Number의 mandatory 사용 명시
  - TDA extension의 Generic extension으로의 변경
  - TSTInfo와 요청 메시지 필드의 변경

- 07 버전에서 08 버전의 변경 사항
  - Serial Number의 RFC2459 정의 준용
  - AIA를 son-of-RFC2459의 SIA(Subject Information Access)로의 변경
  - extensions 필드 형식 변경
  - certReq 필드의 사용
  - ordering 필드의 사용
  - TSTInfo의 tsa와 extensions 필드의 변경
  - accuracy의 단순화
  - 보안 고려사항의 새로운 아이템 추가

- 08 버전에서 09 버전의 변경사항
  - PKIStatus 정보에 대한 수정
  - multiple private signature key에 대한 변경
  - private key의 다른 목적의 사용 제한

- 09 버전에서 10 버전의 변경사항
  - Client의 policy 필드 체크 방법 변경
  - TSAPolicyId의 명시

- 10 버전에서 12 버전의 변경사항
  - 타임스탬프의 Access descriptor에 대한 명시

Roland Mueller가 ISO/IEC JTC1/SC27에서 추진중인 타임스탬프 서비스 표준(안)의 데이터 형식의 차이 등에 대한 조정 필요성을 제시하였고 인터넷 드래프트 제안자인 Denis Pinkas는 SC27과의 호환을 위하여 인터넷 드래프트에 반영하여 수정하였다. 메일링 리스트를 통한 의견들을 수렴한 12 버전의 인터넷 드래프트가 Proposed standard인 RFC로 추진하기 위하여 11월 21일 internet-draft 디렉토리에 등록되었다.

현재 버전의 문서 내용은 다음과 같다.

- Internet X.509 Public Key Infrastructure Time Stamp Protocol
  1. Introduction
  2. The TSA
     2.1. Requirements of the TSA
     2.2. TSA Transactions
     2.3. Identification of the TSA
     2.4. Request and Response Formats
  3. Transports
  4. Security Considerations
  5. Intellectual Property Rights
  6. References
  7. Authors' Address

  Appendix A. Signature Timestamp attribute using CMS
  Appendix B. Placing a Signature At a Particular Point in Time
  Appendix C. MIME Registrations
  Appendix D. ASN.1 Module using 1988 Syntax

Appendix E. Access descriptors for time-stamping

Ⅲ. 타임스탬프 서비스의 절차

타임스탬프 서비스의 절차는 초기 TDA의 선택적인 서비스 제공 과정이 삭제되어 사용자와 TSA(타임스탬프 서비스 기관)간의 서비스 제공 모델로 정립이 되었다. 이들 절차는 다음과 같다.

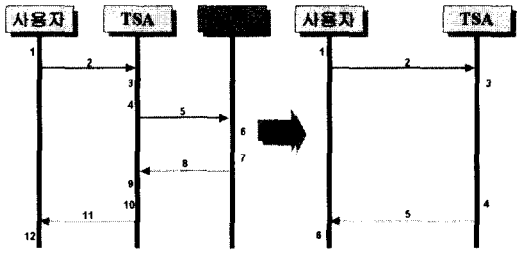

그림 2. 타임스탬프 서비스 절차

① 사용자는 타임스탬프 서비스 기관에 전송할 타임스탬프 요청 메시지를 작성한다. 메시지에는 다음과 같은 데이터들이 포함되어 있을 수 있다.
- 타임스탬프 발고자하는 데이터의 해쉬값
- 타임스탬프 서비스 기관의 정책 정보
- Nonce 값
- 타임스탬프 서비스 기관의 인증서 요청 정보

② 사용자는 타임스탬프 요청 메시지를 타임스탬프 서비스 기관에 전송한다.

③ 타임스탬프 서비스 기관은 요청 메시지의 완전성과 내용상의 정확성 여부를 확인한다.

④ 타임스탬프 서비스 기관은 요청 메시지에 대한 타임스탬프 응답 메시지를 작성한다. 요청 메시지의 에러나 서비스 제공이 불가능 시에는 에러에 대한 상태정보로만 구성된 응답 메시지를 작성하고 정확한 경우에는 타임스탬프 토큰을 타임스탬프 서비스 기관의 키로 전자서명하여 작성한다. 타임스탬프 토큰에는 다음과 같은 정보들로 구성된다.
- 타임스탬프 서비스 기관의 정책 정보
- 요청 메시지의 해쉬값
- 일련번호
- 타임스탬프 정보
- 요청 메시지의 nonce 값
- 타임스탬프 서비스 기관의 정보

⑤ 타임스탬프 서비스 기관은 응답 메시지를 사용자에게 전송한다.

⑥ 사용자는 응답 메시지의 완전성과 내용의 정확성 여부를 검사한다. 내용 검사는 다음과 같은 사항을 포함한다.
- 응답 메시지의 상태 정보 검증
- 타임스탬프 토큰의 전자서명에 대한 유효성 검사
- 타임스탬프 토큰 정보와 요청 정보와의 일치성 검사(해쉬값, Nonce 값, 보장되는 답변기한 내에 타임스탬프 토큰의 도착 여부)

1. 타임스탬프 서비스 기관 요구사항

타임스탬프 서비스 기관은 제 3의 신뢰기관으로서 다음과 같은 요구사항을 충족시켜야 한다.

- 신뢰할 수 있는 시간원을 사용해야 한다.
- 타임스탬프 토큰 안에는 신뢰할 수 있는 시간정보를 포함해야 한다.
- 타임스탬프 토큰에는 일련번호를 포함해야 한다.
- 신청자로부터 정당한 요청을 수신하면 타임스탬프 토큰을 발행해야 한다.
- 타임스탬프 토큰 생성에 사용된 security policy에 대한 식별자를 포함해야 한다.
- 데이터의 해쉬값에만 타임스탬프해야 한다.
- 일방향 충돌방지 해쉬함수의 OID를 검사하여 이 해쉬값의 길이가 해쉬알고리즘과 합치하는가, 함수의 강도나 성질이 적합한 것인지 확인해야 한다.
- 해쉬값에 대해 위 항목을 제외하고는 어떤 방법으로든 검사해서는 안된다.
- 신청자에 대한 어떠한 식별자도 타임스탬프 토큰에 포함시켜서는 안된다.
- 타임스탬프용 키를 사용하여 타임스탬프 토큰을 서명하여야 하고 그 키에 해당하는 인증서에 이러한 사실을 명시하여야 한다.
- Extension 필드를 사용한 신청자의 요청이 있을 시에는 지원가능한 타임스탬프 서비스 기관은 타임스탬프 토큰에 추가적인 정보를 포함시켜야 하고 지원하지 않는 기관은 에러처리를 해야 한다.

2. 보안 고려 사항

타임스탬프 서비스를 제공하기 위해서는 타임스탬프 토큰의 신뢰성 및 유효성을 보장하기 위한 사항을 고려해야 한다.

1) 타임스탬프 서비스 기관의 서명키가 노출된 경우가 아니면서 서비스 기관이 더 이상 신뢰할 수 없다고 판단된 경우에는 기관 인증서를 폐지한다. 이후, 해당 키로 서명된 토큰은 무효로 처리한다.
2) 타임스탬프 서비스 기관의 서명키가 손상된 경우에는 해당 인증서를 폐지한다. 이 경우 해당 키로 전자서명한 어떠한 토큰도 신뢰할 수 없다. 이를 위하여 키의 손상 가능성을 최소로 하기 위한 적절한 보안 및 조치를 취해야 하며 키가 손상된 경우에 서비스 기관이 생성한 모든 토큰의 진위성 여부를 식별할 수 있는 감사 기록을 제공할 수 있어야 한다.
3) 타임스탬프 서비스 기관의 서명키는 충분한 키 유효기간을 허용하는 길이를 갖추어야 한다. 서비스 기관이 전자서명한 모든 토큰의 신뢰성을 유지하기 위하여 다시 타임스탬프하거나 공증 서비스를 받을 수 있다. 타임스탬프 토큰을 Evidence Recording Authority에 보관시켜 신뢰성을 유지할 수도 있다.
4) 타임스탬프 서비스를 이용하는 application은 서비스 응답 시간을 고려해야 한다. man-in-the-middle-attack에 의해 서비스 지연을 야기할 수 있다. 그러므로 수용할 수 있는 기간 이상이 소요된 타임스탬프 토큰은 의심스러운 것으로 간주되어야 한다.
5) 다른 요청자가 동일한 데이터에 동일한 해쉬 알고리즘을 사용하여 타임스탬프 서비스를 요청하거나 동일한 요청자가 한 개의 데이터에 복수개의 타임스탬프를 요청하는 경우 타임스탬프 토큰 안에 identical message imprints를 포함시켜서 같은 데이터에 기반을 둔 타임스탬프 토큰임을 구분할 수 있도록 한다.
6) 부주의나 고의로 동일한 요청 메시지에 대한 처리는 nonce 값을 이용하여 동일한 요청인지를 확인하거나 local clock과 moving time window를 설정하여 해당 해쉬값이 포함된 요청이 time window 안에 존재하는지 확인하여 상황을 파악할 수도 있다.

Ⅳ. 타임스탬프 메시지 형식

타임스탬프 서비스는 요청 메시지와 전자서명된 타임스탬프 토큰을 포함하는 응답 메시지로 구성하여 제공된다.

1. 타임스탬프 요청 형식

현재의 타임스탬프 요청 형식은 다음과 같다.

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

- version : 현재 프로토콜의 버전
- messageImprint
  사용된 해쉬 알고리즘 ID와 해쉬값으로 구성

```
MessageImprint  ::= SEQUENCE  {
  hashAlgorithm       AlgorithmIdentifier,
  hashedMessage       OCTET STRING
}
```

- reqPolicy(선택)
  타임스탬프 토큰 생성에 적용되는 정책
  TSAPolicyId ::= OBJECT IDENTIFIER

- Nonce ("number n once"의 약자) (선택)
  요청 메시지에서 nonce값이 사용될 때 응답 메시지에도 동일한 nonce값이 포함되어야 하며 큰 랜덤 숫자를 사용한다(예. 64 비트 정수)

- certReq (선택)
  이 필드가 사용되고 true로 셋팅된 경우, 응답 메시지에 전자서명된 타임스탬프 토큰과 함께 타임스탬프 서비스 기관의인증서가 제공되어야 하며 이 필드가 사용되지 않거나 false로 셋팅

된 경우, 응답 메시지에 서비스 기관의 인증서가 포함되지 않는다

○ extensions (선택)
향후 추가적인 정보를 위한 필드로 신청자가 이 필드를 사용하였지만 타임스탬프 서비스 기관이 제공하지 못하는 경우 에러 정보를 제공해야 한다(unacceptedExtension)

2. 타임스탬프 응답 형식

타임스탬프 응답 형식은 다음과 같이 상태 정보와 타임스탬프 토큰으로 구성된다.

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

1) status

```
PKIStatusInfo ::= SEQUENCE {
  status            PKIStatus,
  statusString      PKIFreeText    OPTIONAL,
  failInfo          PKIFailureInfo OPTIONAL
}
```

상태 정보가 0과 1이면 응답 메시지에 타임스탬프 토큰을 포함하여야 하며 그 이외에는 타임스탬프 토큰을 포함시키면 안 된다.

```
PKIStatus ::= INTEGER {
  granted                    (0),
    /* 유효한 요청
  grantedWithMods            (1),
    /* 변경이 있는 시점확인서비스 토큰 응답
  rejection                  (2),
    /* 요청 거부
  waiting                    (3),
    /* 접수 확인 또는 지연확인 표시로 사용
  revocationWarning          (4),
    /* 폐지 시기에 대해 알리는 경고 메시지
  revocationNotification     (5)
    /* 폐지가 발생했음을 알리는 메시지
  }
```

상태 정보가 2이면 타임스탬프 서비스 요청이 요청 형식이 잘못되었거나 부적합한 해쉬 함수 사용 때문에 거부됨을 가르쳐 주며 상태 정보가 3인 경우 타임스탬프 신청을 접수했다는 것을 요청자에게 알리기 위한 목적으로 타임스탬프 서비스 기관이 일반적으로 사용할 수 있는 것으로 보장된 답변기간이 초과될 것으로 예상되어 이를 표시해야 할 경우 사용한다. 에러에 대한 경우 다음과 같은 데이터 구조를 통해 구체화되어야 한다.

```
PKIFailureInfo ::= BIT STRING {
  badAlg                (0),
    /* 인식되지 않거나 지원되지 않는 알고리즘 ID
  badRequest            (2)
    /* 허용되지 않거나 지원되지 않는 트랜잭션
  badDataFormat         (5),
    /* 구문 상 잘못된 데이터
  timeNotAvailable      (14),
    /* TSA의 시각소스를 사용할 수 없는 경우
  unacceptedPolicy      (15),
    /* 요청한 TSA의 정책을 TSA가 지원하지 않는 경우
  unacceptedExtension   (16),
    /* 요청한 확장 필드를 TSA가 지원하지 않는 경우
  addInfoNotAvailable   (17)
    /* 추가 정보 요청이 인식되지 않거나 사용할 수 없는 경우
  }
```

2) TimeStampToken

타임스탬프 토큰은 타임스탬프 서비스 기관의 서명키로 전자서명된 형식이다.

```
TimeStamptoken ::= ContentInfo
  -- ContentType is id-signedData ([CMS])
  -- Content is SignedData ([CMS])
```

```
TSTInfo ::= SEQUENCE {
  version           INTEGER { v1(1) },
  policy            TSAPolicyId,
  messageImprint    MessageImprint,
  serialNumber      INTEGER,
  genTime           GeneralizedTime,
  accuracy          Accuracy  OPTIONAL,
  ordering          BOOLEAN DEFAULT FALSE,
  nonce             INTEGER OPTIONAL,
  tsa               [0] GeneralName OPTIONAL,
  extensions        [1] Extensions  OPTIONAL
  }
```

○ policy
타임스탬프 토큰 생성 정책을 표시해 주는 것

으로 요청 메시지의 필드와 동일해야 하며 동일하지 않은 경우 에러 처리를 한다.

○ MessageImprint
요청 메시지와 동일한 값이다.

○ serialNumber
타임스탬프 토큰에 부여되는 유일한 값으로, 서비스의 중지시에도 유효한 값을 제공하는 인수이다.

○ genTime
타임스탬프 생성 시점을 가리킨다.
YYYYMMDDhhmmss[.s...]Z

○ accuracy

```
Accuracy ::= SEQUENCE {
 seconds   INTEGER    OPTIONAL,
 millis   [0] INTEGER (1..999) OPTIONAL,
 micros   [1] INTEGER (1..999) OPTIONAL
}
```

타임스탬프 시점의 정확성을 제공하는 추가 정보로 GeneralizedTime에 accuracy가 추가되면 TSA time의 upper limit이고 accuracy가 빼지면 TSA time의 lower limit가 된다.

○ ordering
필드가 사용되지 않거나 사용시 false로 설정된 경우 타임스탬프 서비스 기관에서 타임스탬프 생성 시점에 대해서 genTime 필드만이 가리키게 되고 이 필드가 사용되면서 true로 설정되면 같은 타임스탬프 서비스 기관에서 생성하는 타임스탬프 토큰은 accuracy에 대한 고려 없이 genTime을 기반으로 순서를 정하면 된다.

○ nonce
요청메시지와 동일한 값이 사용된다.

V. 타임스탬프 서비스 현황

타임스탬프 서비스 기술은 전세계적으로 상용화되어 초기 시장을 형성하는 단계이다. 현재 특허권/저작권 관련 분야에서 응용되고 있으며 인터넷과 전자상거래의 발전에 따라 응용 분야가 빠르게 발전해 나갈 것이다. 타임스탬프 서비스를 다음과 같은 분야에서 응용할 수 있다.

○ 행정 등록
시민들이 공공 행정 기관에 제출하는 문서를 승인하고 등록하는 과정에서 타임스탬프 서비스를 제공될 수 있다.

○ 공증 및 소유권 등록
전자서명 사용을 통한 공증시 문서의 내용이 검증되고 문서의 생성 및 수정된 시간에 대한 타임스탬프 서비스가 제공될 수 있다.

○ 저작권 및 지적 재산권
특허나 작품 등의 제출 시점에 대한 타임스탬프 서비스의 제공으로 신뢰할만한 증거를 제공될 수 있다.

○ 우편 서비스
발신 날짜, 시간 및 위치를 확인하는 검증 기능과 함께 소인을 제공하기 위해 사용될 수 있다.

○ 증권 거래
매매 주문 등 거래와 관련된 정보에 대해 타임스탬프 될 수 있다.

○ 사법 행정/조달
법 집행을 수행해야 하는 엄격한 조건 때문에 전자문서는 주어진 조건 내에서 유효성과 무결성을 확증하는 타임스탬프 서비스가 요구될 수 있다.

○ 공중 보건
원격 검진, 원격 진단, 또는 원격 분석을 통해 이루어지는 의료 사업이 증가함에 따라 각 환자의 내역 기록에 삽입될 진단 및 이미지의 무결성과 기밀성을 제공하기 위하여 타임스탬프가 사용될 수 있다.

○ 전자상거래
거래 당사자간의 적절한 보안 수준의 제공과 잠재적인 분쟁에 대처할 증거 제공을 위하여 타임스탬프 서비스가 사용될 수 있다.

○ 원격 회의 및 화상 회의
원격 회의에서 도달한 결론을 기록하여 추후 조작을 피하기 위해 참가자들 간에 교환된 문서와 오디오 및 비디오에 타임스탬프될 수 있다.

○ 방송
라디오, TV, 케이블, 위성방송 등의 분야에서 송출 시간에 따라 광고비 책정 등에 타임스탬프가 적용될 수 있다.

1. 국외 서비스 현황

대학과 연구소에서 연구 프로젝트로 무료 서비스를 제공하거나 e-Timestamp사, CRYPTOMAThIC사가 타임스탬프 서비스 및 타임스탬프 시스템 제품을 판매하고 있다.

1) e-TimeStamp사

e-TimeStamp사는 작업 내용이 특정 시점에 존재했다는 사실과 그 내용이 그 때 이후로 변하지 않았다는 사실에 대한 명백한 증거를 제공해 주는 타임스탬프 서비스 사업을 제공한다. 전자상거래 관련 기술을 개발해온 Rick Borgers를 중심으로 새로이 사업을 시작하였으며 인터넷을 사용하는 모든 국가에 대해서 타임스탬프 서비스를 제공한다.

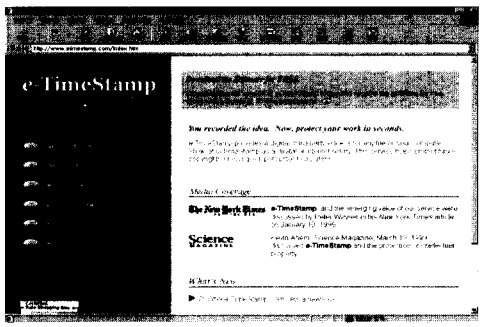

그림 3. e-TimeStamp사 홈페이지

특허품을 발명한 발명가, 작품을 새로이 만든 작가, 계약을 하는 기업가, 진료 기록을 작성하는 의사 등 자신의 기록에 대한 특정 시간의 존재 여부 증명이 필요한 모든 분야에 대해 e-TimeStamp를 이용하면 인터넷을 이용하기 때문에 비용이 적게 들며 암호화를 이용함으로써 더 안전한 서비스를 제공할 수 있다.

클라이언트 소프트웨어는 Sun MicroSystems Java, 개발자 환경으로는 IBM VisualAge for Java, 데이터 저장으로는 ObjectStore for Java from ObjectDesign, Installation software로는 Zero-g를 사용하여 개발하였으며 프로그램의 구성은 총 5개의 메인 메뉴로 구성되었다. 파일에 대한 지문을 생성하여 지문을 가지고 e-TimeStamp 서버와 통신하며, 서버로부터 받은 타임스탬프 토큰을 보관한다. 이 때, 파일 지문이란 특정 파일에 대해 해쉬함수를 적용했을 때, 생성되는 해쉬값으로서 어느 하나의 문서를 식별하는 데 사용되는 식별자의 역할을 한다. 시점확인 서버는 NIST(National Institute of Standards and Technology)의 시각 소스를 사용하여 초 단위까지만 서비스를 하므로 시점확인서비스 시간의 정밀도를 몇 초대로 넓게 잡고 있다.

2) CRYPTOMAThIC사

공개키기반구조 및 타임스탬프 시스템, 보안 툴을 제작하여 공급하는 업체로 타임스탬프 시스템인 Timelnk라는 제품을 판매하고 있다. PKIX 드래프트를 준용하고 있으며 "swisstime.ethz.ch"를 기본 신뢰시간 서버로 지정하고 있다. 해쉬 알고리즘은 SHA-1과 2048 비트 키를 지원한다. 현재 서버측의 타임스탬프 토큰의 저장과 감사로그 기록 기능이 제공되지 않는다.

Ⅵ. 결 론

이상으로 타임스탬프 서비스 동향에 대해 분석하였다. 타임스탬프 서비스 프로토콜의 표준화는 IETF PKIX의 시점확인서비스 프로토콜 인터넷 드래프트인 "Internet X.509 Public Key Infrastructure Time Stamp Protocol"이 RFC로 추진 될 것으로 예상되며 ISO/IEC JTC1/SC27의 표준(안)도 계획에 따라 의견을 수렴하여 2003년까지 표준화를 추진해 나갈 것이다.

타임스탬프 서비스 그 자체로서는 활용 가치가 크지 않으므로 전자거래를 제공하는 모든 환경에서안전 신뢰성을 제공하는 전자공증 서비스 등의 응용서비스 개발이 필요할 것이다.

참 고 문 헌

[1] Adams, Cain, Pinkas, Zuccherato, "Internet X.509 Public Key Infrastructure, Time Stamp Protocol(TSP)", draft-ietf-pkix-time-stamp-12, Internet-Draft, 2000.11

[2] FNMT, "PKITS Overview : Final Report", 1998. 12

[3] FNMT, "PKITS Deliverable D3 : Architecture of Time-Stamping Service and Scenarios of Use : Services and Features", 1998. 7

[4] IETF PKIX RFC2459, "Internet Public Key Infrastructure X.509 Certificate and CRL Profile",1999

[5] IETF PKIX RFC2510,"Internet Public Key Infrastructure Certificate Management Protocol", 1999. 3

[6] ISO/IEC JTC1/SC27 N2107, "Guidelines on the use and management of Time Stamping Services(GUMTSS)", 1998. 10

[7] ISO/IEC JTC1/SC27 N2595, "WD 18014-1 :Information technology - Security techniques - Time stamping services-Part 1:Framework", 2000. 5

[8] ISO/IEC JTC1/SC27 N2596, "WD 18014-2 :Information technology - Security techniques - Time stamping services-Part 2:Mechanisms producing independent tokens", 2000. 5

[9] ISO/IEC JTC1/SC27 N2597, "WD 1 :Information technology - Security tech- - Time stamping services-Part 3: Mecha producing linked tokens", 2000. 5

[10] http://www.e-timestamp.com

〈著者紹介〉

홍 기 융 (Ki-Yoong Hong)

1985년 2월 : 전남대학교 전자계산학과 졸업
1990년 2월 : 중앙대학교 전자계산학과 석사
1994년 4월 : 정보처리기술사
1996년 2월 : 아주대학교 컴퓨터공학과 박사
1985년 9월 - 1995년 10월 : 한국전자통신연구원 선임연구원
1992년 - 1993년 : 이태리 Alenia Spazio사 Senior Researcher
1995년 10월 - 1996년 4월 : 한국전산원 선임연구원
1996년 4월 - 2000년 2월 : 한국정보보호센터 인증관리팀장
1998년 - 현재 : 동국대학교 국제정보대학원 정보보호학과 겸임교수
2000년 6월 - 현재 : 인터넷보안기술포럼 PKI분과위원회 위원장
2000년 2월 - 현재 : (주)케이사인/(주)시큐브 대표이사
관심분야 : 컴퓨터 · 네트워크 보안, 공개키기반구조, 보안 커널, 침입탐지기술