한국산학기술학회논문지
Vol. 5, No. 1, pp. 16-20, 2004

# 국제 표준을 준수하는 웹 전자 공증 시스템의 개발

장 혜 진*

# Development of a Web-based Digital Notary System Conforming International Standards

**Hai Jin Chang***

**요 약** 본 논문은 보안적으로 안전하며, 타임스탬프 관련 국제 표준 규격을 만족하며, 사용자 접근성이 높은 웹 기반 시스템 형태를 갖는 전자 공증 시스템(digital notary system)을 개발하였다. 타임스탬프 관련 기술 및 응용 시스템들은 아직 대중화되어 있지 않지만 전자상거래, 디지털 저작권 관리, 인터넷 메일 등의 다양한 분야에서 잠재적으로 매우 중요한 의미를 갖는다. 개발된 전자 공증 시스템은 rfc3161을 준수하는 타임스탬프 요청(timestamp request) 및 타임스탬프 응답(timestamp response)을 사용한다. 또한 서버와 클라이언트 통신에 SSL(Secure Socket Layer)을 사용하여 통신 보안을 보장하며, 재사용 공격(replay attack)을 방지하기 위하여 논스(nonce)를 사용한다.

**Abstract** This paper developed a secure web-based digital notary system. The system conforms to international standards, and gives users very good accessibility to it. The technologies and the application systems for timestamp-related services are not yet popularized, but they are potentially meaningful to many kinds of areas such as e-commerces, digital right managements, and internet mail systems. The digital notary system uses the timestamp requests and responses which conforms to rfc 3161. The system supports secure communication between web-based notary server and its clients by using SSL(Secure Socket Layer), and use nonces for prevention of replay attacks.

**Key Words :** timestamp, timestamp authority, token, digital notary system, SSL

## 1. 서 론

어떤 문서나 데이터가 어떤 시점에 존재하였는가에 대한 엄밀한 판정이 필요한 경우가 많다. 전자 공증 시스템이란 고객의 임의의 전자 문서에 대하여 그 전자 문서가 어떤 특정 시점에 존재하였음을 신뢰할 수 있는 제3의 기관(trusted third party)을 통하여 증명하여 주는 시스템을 의미한다[1]. 전자 공증 시스템은 특허 분쟁이나 저작권 분쟁 뿐 아니라 전자 상거래에서 부인 방지(nonrepudiation) 등의 다양한 문제의 해결에도 도움이 될 수 있다. 예를 들어, 저작권 분쟁, 특허 분쟁, 그리고 전자 성거래 분쟁 등의 경우 분쟁의 내용에 대한 근거 자료나 문서가 언제부터 존재하였는가에 따라 분쟁의 승패가 결정된다.

종이 문서의 경우, 공증인의 서명을 받거나 변호사에게 복사본을 위탁하는 단순한 메커니즘을 사용하여 왔다. 하지만, 전자 문서의 경우 누구나 쉽게 내용을 수정하거나 문서 생성 시각을 수정하여 복사본을 만들 수 있으므로, 전자 문서나 데이터에 대하여 그 문서나 데이터가 어떤 시점에 존재하였음을 증명하는 전자 공증 서비스가 필요하다[2].

전자 공증 서비스는 타임스탬프 관련 서비스 중의 하나이다. 타임스탬프 관련 기술들은 전자 공증 서비스 이외에도 전자 경매, 전자 복권, 전자 주식 거래, 디지털 저작권 보호, 신뢰성을 보장하는 전자 메일 등의 다양한 분야에 사용될 수 있다.

본 논문에서 개발하는 전자 공증 시스템은 관련 국제 표준 규격들[3,6]을 준수하며, 웹 기반 방식으로 설계되고 구현되어 사용자 접근성이 높으며 다음과 같은 점에서 보안적으로 안전하다는 점을 특징으로 한다.

(1) 사용자는 데이터나 문서 자체가 아니라 그에 대한 축약(digest) 값만을 공증 서버로 전송하므로 사용자의 프라이버시(privacy)가 보장된다.

*상명대학교 컴퓨터 정보 통신학부
Tel: 041-550-5364
본 논문은 상명대학교의 연구지원을 받았음.

(2) 공증 서버는 재사용 공격(replay attack)에 대응하기 위하여 논스(nonce)를 사용한다.

(3) 클라이언트의 코드는 전자 서명된 형태를 가지므로 코드 배포자의 신원 파악 및 코드의 불법 훼손에 대응한다.

(4) 타임스탬프 요청에서 타임스탬프 토큰 발급까지의 과정의 시간 간격에 제약을 두지 않는 경우 보안 공격의 가능성이 커진다. 따라서 타임스탬프 요청의 송신에서 응답의 수신까지의 시간 간격을 제약할 수 있다.

(5) 공증 서버와 클라이언트는 HTTP 뿐 아니라 HTTPS를 사용하여 통신할 수 있다.

(6) 직접적으로 전자 공증 서비스를 제공하는 웹 서버는 방화벽 밖에 있으나 실제로 타임스탬프 토큰을 발행하는 TSA 서버는 방화벽 안에 별도로 존재한다. 또한 모든 데이터는 방화벽내의 DB 서버에 저장되므로 시스템의 해킹에 대응이 용이하다. 공증 웹 서버는 방화벽 밖에 있으므로 해킹을 당할 가능성이 크지만 해킹을 당해도 아무런 중요 데이터를 담고 있지 않으므로 즉시 복구될 수 있다.

본 논문의 제 2장에서는 전자 공증 시스템 및 타임스탬프 관련 기술 동향을 살펴본다. 제 3장에서는 개발된 공증 시스템의 구조와 특징을 살핀다. 제 4장은 결론이다.

## 2. 관련 기술 동향

전자 공증 시스템은 타임스탬프 기술의 중요한 응용분야의 하나이다. 현재 국제 표준화 기구인 ISO/IEC JTC 1/SC 27과 IETF 산하 PKIX에서 시점 확인 서비스에 대한 표준화 작업을 진행하고 있다. IETF의 표준안은 시점 확인 서비스의 기본 사항인 시점 확인 요청 및 시점 확인 응답에 대한 자료 구조와 프로토콜을 규정하고 있다. 시점 확인 시스템과 직접 관련된 IETF 표준안들은 RFC 3161[3], RFC 3126[4] 등이 있으며, 정확한 시각을 통신하기 위한 관련 표준안에는 RFC 1305 [5], RFC 2030 [6] 등이 있다.

JTC 1/SC 27에서는 IETF 표준을 수용하고 더 나아가 연결된 토큰(linked token)과 같은 새로운 기능이 포함된 시점 확인 시스템에 대한 기술 표준화 작업을 진행하고 있다. 관련 표준 문서들에는 ISO/IEC 18014의 1부, 2부, 3부 [7,8,9]가 있다.

전자 공증 시스템은 PKI(Public Key Infrastructure) 기술에 근거하는 보안 기술들을 사용한다. 전자 공증 시스템에는 축약(digest), 전자 서명(digital signature), 전자 인증서(public key certificate), SSL(Secure Socket Layer), 논스(nonce) 등의 보안 기술들이 적용된다.

타임스탬프 관련 시스템 기술들에 대한 표준화 작업은 진행 중에 있다. 보안적으로 보다 안전하고 신뢰도가 높은 타임스탬프 체계를 위한 기술들이 지속적으로 연구되고 있다. 응용적 측면에서, 전자 공증 시스템과 같은 타임스탬프 응용 분야는 아직 대중화되고 있지 못하다. 그 이유는 타임스탬프 관련 시스템에 공신력을 부여하는 법적 제도적 장치들이 부족한 탓으로 짐작된다. 현재, 국내의 전자 인증서 발행 기관들은 타임스탬프 용 인증서 발행 능력은 가지고 있으나 관련 서비스를 구체적으로 제공하고 있지는 않다. 본 논문의 시스템은 다음과 같이 국제 표준 규격을 준수한다.

- 타임스탬프 토큰 발행 요청은 rfc3161에서 규정하는 규격을 따르며, 타임스탬프 토큰 발행 요청에는 공증 대상 문서 자체가 아닌 그 문서에 대한 축약값 만이 포함된다. 이는 타임스탬프 관련 표준에서 개인의 프라이버시 보호를 위해 요구하는 사항이다.
- 타임스탬프 토큰은 전자 서명된 형태를 갖는다. 그 전자 서명 형태는 rfc3369에서 규정하는 "SignedData"라는 자료 구조 포맷을 따르고 있다. 전자 서명에 사용되는 축약 알고리즘들 및 공개키 암호 알고리즘들은 모두 표준 알고리즘들을 사용한다.
- 시각 원천과 TSA 서버는 정확한 시각 정보를 통신하기 위하여 표준 규격인 SNTP 프로토콜을 사용하여 통신한다. 시각 원천은 한국표준기술연구원의 원자시계를 사용한다. 한국표준기술연구원은 한국 표준 지역 시각을 정하는 권한을 갖고 있다.

본 논문은 국제 표준 규격을 철저히 준수하며, 표준 규격이 규정하지 않는 세부적 구현 사항들을 자체적으로 결정하여 접근성이 높고 안전한 웹 기반의 전자 공증 시스템을 개발하였다는 데에 의의가 있을 것이다.

## 3. 웹 기반 전자 공증 시스템 개발

### 3.1 전체 구조

개발된 시스템은 시각 원천(time source), TSA(timestamp authority) 서버, 공증 웹 서버, DB 서버, 그리고 사용자들의 PC의 웹 브라우저 상에서 동작하는 타임스탬프 클라이언트(timestamp client) 등으로 구성된다. 다음은 개발된 웹 기반 전자 공증 시스템의 구조도이다.

시스템의 개발 환경은 다음과 같다 : DB 서버로는 오라클 9i가 사용되었다. 관리자 클라이언트와 TS 클라이언트는 마이크로소프트의 Win32 환경을 사용한다고 가정하였으며 마이크로소프트사의 비주얼 베이직 6.0을 주 개발 언어로 사용하였다. ActiveX 콤포넌트 제작에 비주얼 C/C++를 사용하였다. TSA 웹서버는 운영체계

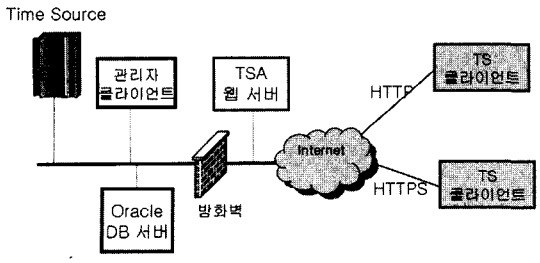


**그림 1.** 웹 기반 공증 시스템 구조

로 Linux를 사용하고, 웹서버는 Apache 1.3.28을 사용하였다. 클라이언트와 서버 모두에서 보안 관련 라이브러리로 OpenSSL[11]이 사용되었다. 위 웹 기반 공증 시스템은 신뢰성 있는 시각 원천(time source)으로 한국 표준 과학 연구소의 원자 시계를 사용한다. 공증 서버의 시각은 SNTP(Simple Network Time Protocol) 프로토콜을 사용하여 원자 시계의 시각과 동기화된다. 사용자는 웹 브라우저로 공증 웹 서버에 접속한다. 공증 웹 서버는 웹 브라우저 상에서 동작하는 타임스탬프 클라이언트의 타임스탬프 요청(timestamp request)을 받아, 그 요청을 TSA 서버로 전달한다. 그러면 TSA 서버는 타임스탬프 클라이언트의 타임스탬프 발급 요청에 대하여 타임스탬프 토큰을 발급한다. DB 서버는 TSA 서버가 발급한 타임스탬프 토큰 및 감사 로그(log)를 저장한다.

### 3.2 타임스탬프 요청 및 응답 토큰의 규격

타임스탬프 서비스에서 타임스탬프 클라이언트와 TSA 서버 간에 사용되는 메시지의 유형에는 타임스탬프 요청 메시지와 타임스탬프 응답 메시지가 있다. 본 시스템은 타임스탬프 요청 및 응답 메시지 등의 규격을 rfc 3161에 준하여 구현하였다. 타임스탬프 요청에는 버전, 공증 대상 문서에 대한 축약, 요청 정책 등이 포함된다. 타임스탬프 요청 자체에는 요청자의 프라이버시 보호를 위하여 공증 대상 문서 자체나 요청자의 신상 정보가 포함되지 않아야 한다. 타임스탬프 요청 메시지에는 재사용 공격(reply attack)에 대비하기 위한 논스(nonce)가 선택적으로 포함될 수 있다. 타임스탬프 응답은 상태 정보 필드와 타임스탬프 토큰 필드로 구성된다. 정상적으로 타임스탬프 응답이 생성된 경우, 상태 정보 필드의 값은 0이며 타임스탬프 토큰 필드에는 타임스탬프 토큰이 들어있게 된다. 제 3.5절에 타임스탬프 토큰의 구성 요소들이 설명된다.

### 3.3 타임스탬프 토큰의 요청 및 타임스탬프 응답 발급

본 시스템에서는 타임스탬프 클라이언트가 TSA 서버에게 직접 타임스탬프 요청을 보내지 않고, 공증 웹 서버를 경유하여 TSA에게 타임스탬프 요청을 보내도록 구현되었다. 이런 구현 방법은 사용자에게 편리하고 직관적인 웹 기반의 공증 서비스를 제공할 수 있으며, 웹 서버가 해킹 등으로 훼손되더라도 방화벽 안에 있는 TSA 서버는 안전할 수 있다는 장점을 갖는다. 본 시스템에서 타임스탬프 클라이언트가 TSA 서버에게 타임스탬프를 요청하여 타임스탬프 응답을 받는 절차는 다음 그림 2와 같이 수행된다. 그림 2에서 세로축은 위에서 아래로의 시간의 흐름을 나타낸다.

(1) 타임스탬프 클라이언트는 타임스탬프를 찍을 대상 자료에 대한 축약값을 계산한다. (계산 결과를 h라고 하자)

(2) 타임스탬프 클라이언트는 다음과 같은 데이터가 포함된 타임스탬프 토큰 요청 메시지를 생성하여 공증 웹 서버로 보낸다. 여기서 타임스탬프 발행 정책(policy)과 논스(nonce)는 선택 사항이다.

- 축약값 h
- 사용된 축약 알고리즘
- 타임스탬프 발행 정책
- 논스

(3) 공증 웹 서버는 타임스탬프 요청을 수신하여, TSA 서버로 전달한다.

(4) TSA 서버는 수신된 타임스탬프 요청이 올바른 요청인가 확인한다.

(5) TSA 서버는 확인 결과에 따라 결과에 맞는 타임스탬프 응답 메시지를 생성하여 공증 웹 서버에게 전송한다.

(6) 공증 웹 서버는 TSA 서버로부터 수신한 타임스탬프 응답을 TSA 클라이언트에게 전송한다.

(7) TS 클라이언트는 공증 웹 서버로부터 수신한 타임스탬프 응답 메시지를 검증하고 이후의 사용을 위해 저장한다.

타임스탬프 응답은 상태 정보와 타임스탬프 토큰을 포함한다. 위 단계 (5)에서, 확인 결과가 올바른 것으로 확인되는 경우 타임스탬프 토큰을 포함하는 응답 메시

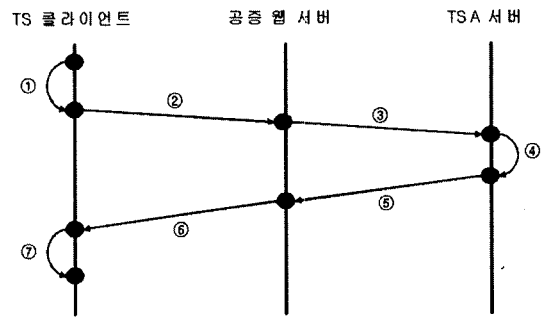


**그림 2.** 타임스탬프 요청 및 발급 절차

지가 생성된다. 확인 결과가 올바른 것이 아닌 경우, 오류를 포함하는 응답 메시지가 생성된다. 예를 들어, 타임스탬프 클라이언트가 요구하는 발행 정책이나 축약 알고리즘 등이 TSA 서버에 의해 지원되는 값이 아니면 오류를 포함하는 응답 메시지가 생성되어 공증 웹 서버로 전송된다. 오류를 포함하는 응답 메시지에는 타임스탬프 토큰이 포함되지 않는다.

### 3.4 타임스탬프 토큰의 검증

타임스탬프의 검증 기능은 타임스탬프 클라이언트가 제공한다. 타임스탬프 검증에는 타임스탬프 토큰의 TSA 서버의 전자서명 검증 및 토큰에 포함된 타임스탬프 검증 대상 문서의 축약에 대한 검증이 포함된다. 타임스탬프 토큰의 검증 절차는 다음과 같다.

(1) 타임스탬프 토큰 자체의 유효성을 검증한다. 즉, 토큰에 포함된 TSA 서버의 전자 서명을 확인한다. 전자 서명 검증에 실패하면 검증 실패 메시지를 반환한다.

(2) 타임스탬프 대상 문서의 축약을 계산한다. 이때 그 문서에 대한 토큰을 요청할 당시 사용한 축약 알고리즘과 같은 알고리즘을 사용하여야 한다.

(3) 문서에 대한 계산된 축약값과 토큰에 들어있는 축약값을 비교한다. 두 축약값이 같으면 검증 성공 메시지를 반환한다. 아니면 검증 실패를 반환한다.

타임스탬프의 검증 결과로 검증 성공 메시지를 반환받을 수 있다는 것은 타임스탬프 대상 문서가 타임스탬프 토큰에 적힌 시점에 존재하였다는 증거로 사용된다.

### 3.5 타임스탬프 클라이언트의 설치 및 수행

타임스탬프 클라이언트는 마이크로소프트사의 ActiveX 배포 기술을 사용하여 사용자가 웹 브라우저로 공증 웹 서버에 접속하였을 때 자동으로 사용자 PC로 다운로드되어 설치되도록 구현되었다. 타임스탬프 클라이언트가 웹 기반 방식으로 동작하는 것은 사용자 접근의 편의성을 높게 하므로 바람직하다. 다음 그림 3은 구현된 공증 시스템에서의 타임스탬프 클라이언트의 설정에 관련된 사용자 인터페이스이다.

다음 그림은 발급된 타임스탬프 토큰에 대한 정보를 보여주는 타임스탬프 토큰 뷰어의 화면 모습이다. 타임스탬프 토큰에는 토큰 일련 번호, 시점 확인 시각, 시점 확인 서버 식별 정보, 시점 확인 정책 식별자, 사용된 축약 알고리즘 종류, 축약값, 논스(nonce) 값 등의 정보가 포함된다. 타임스탬프 토큰은 전자 서명된 자료이다. 서명된 타임스탬프 토큰의 구조에 대한 규격은 RFC 3369[10]에서 규정된다.

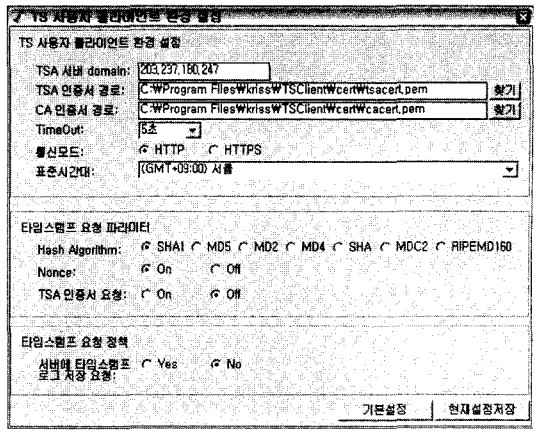


**그림 3.** 타임스탬프 클라이언트의 설정

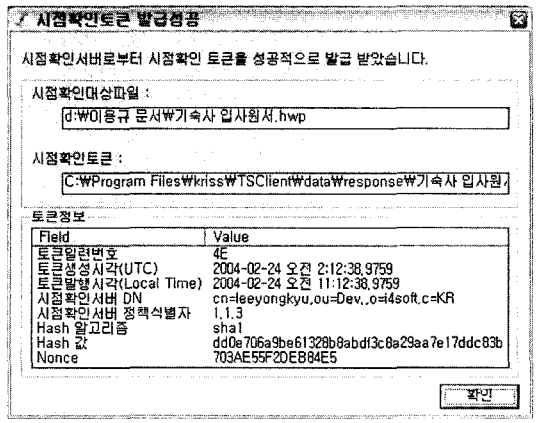


**그림 4.** 타임스탬프 토큰 뷰어

### 3.6 보안적 고려

RFC 3161은 시점 확인 시스템에 관련된 보안을 위하여 다양한 보안 관련 조건들을 규정하고 있다. 본 시스템은 다음에 기술되는 조건들을 만족하도록 구현되었다.

(1) 타임스탬프 대상 문서 또는 데이터에 대한 프라이버시를 보호하기 위하여 시점 확인 대상 문서 자체가 아닌 문서의 축약에 대한 정보만이 타임스탬프 발급 기관으로 전달되어야 하며, 타임스탬프 요청이나 응답에는 타임스탬프를 요청한 사용자에 대한 정보를 저장하지 않도록 규정하고 있다.

(2) 재전송 공격(replay attack)에 대응하기 위해 논스(nonce)를 사용할 수 있다.

(3) 타임스탬프 토큰에 대한 위조나 변조를 방지하기 위하여 타임스탬프 토큰은 TSA 서버의 전자 서명이 추가된다.

(4) 중간자 공격(man-in-the-middle attack)등으로부터 보다 안전하기 위하여, 타임스탬프 요청 직후부터 타임

스탬프 응답이 도착할 때까지 지정된 시간 이상이 지나면 타임스탬프 발급이 실패된 것으로 간주할 수 있다.

본 전자 공증 시스템은 보안을 위하여 서론에서 언급한 조건들 (1)에서 (6)을 구현하였다. 조건 (1), (2), (3), (4)는 표준 규격 문서 차원에서 요구하고 있는 조건들이다. 조건 (5), (6)은 구현적 차원에서 웹 기반 시스템이라는 점이 반영된 조건들이다. 구현된 시스템은 시각 소스(time source)와 SNTP 프로토콜[6]을 통해 시각을 동기화한다.

## 4. 결론 및 향후 연구

본 논문은 국제 표준 규격을 준수하며 보안적으로 안전하며 사용자 접근성이 좋은 웹 기반 방식 전자 공증 시스템을 개발하였다. 타임스탬프 관련 표준 규격들은 타임스탬프 토큰의 자료 구조와 같은 근본적인 규격만을 규정하고 있으므로 표준을 준수하는 시스템들 간에도 구현적인 측면에서는 세부적으로 많은 차이가 나타날 수 있다.

본 논문은 국제 표준을 준수하면서, 보안적으로 안전하고, 사용자 접근성이 좋은 실용적인 타임스탬프 응용 시스템의 설계 및 구현 사례를 제공하였다는 의미를 갖는다.

전자 공증 시스템과 같은 타임스탬프 시스템 응용 기술들에 대한 수요는 잠재적으로 매우 크다. 인터넷을 통한 전자 상거래가 대중적으로 보급되고 있으며, 전자 문서 및 데이터들이 폭발적으로 증가하고 있기 때문이다. 향후 연구로, 보안적으로 더욱 안전한 타임스탬프 관련 규격 및 시스템들에 대한 연구가 필요하다. 또한 새로운 타임스탬프 응용 분야들을 발굴하기 위한 연구 및 타임스탬프 관련된 응용 기술 및 실용적 시스템의 개발에 대한 연구가 좀더 필요하다고 판단된다. 예를 들어, 전자 서명과 시점 확인 기술의 결합 분야는 덜 개척된 응용 분야라고 여겨진다.

## 참고문헌


[1] Bruce Schneier, Timestamping Services, Applied Cryptography 2nd Ed., pp 75-79, Willy, 1996.

[2] Cryptomathic, TimeStamping Authority Technical White paper 1.0, February 2003.

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

[4] D. Pinkas, J. Ross, N. Pope, Electronic Signature Formats for long term electronic signatures, RFC 3126, September 2001.

[5] D.L. Mills, Network Time Protocol (Version 3) - Specification, Implementation and Analysis, RFC 1305, March 1992.

[6] D.L. Mills, Simple Network Time Protocol (SNTP) Version 4 - for IPv4, IPv6 and OSI, RFC 2030, October 1996.

[7] ISO/IEC 18014-1 : 2002. Information technology - Security techniques - Time-stamping services - Part 1 : Framework, October 2002.

[8] ISO/IEC 18014-2 : 2002 Information technology - Security techniques - Time-stamping services - Part 2 : Mechanism producing independent tokens, December 2002.

[9] ISO/IEC 18014 : 2003. Information technology - Security techniques - Time-stamping services - Part 3 : Mechanism producing linked tokens (DRAFT STANDARD)

[10] R. Housley, Crypographic Message Syntax, RFC 3369, August 2002.

[11] Mark J. Cox, et al., Welcome to the OpenSSL project, http://www.openssl.org