정보학연구 제4권 제2호 2001년 6월(pp.1-23)
The Journal of Information Technology, Vol.4, No.2


# 볼레로 시스템상의 메시지 송수신에 관한 고찰

전순환*

요 약

정보통신기술의 발달에 따른 전자상거래의 도입으로 국제무역거래에도 무역서류의 전자화가 필요하게 되었다. BOLERO 프로젝트는 MANDATE 프로젝트의 성과를 기초로 하여, 전자식 선화증권의 실용 가능성에 관련한 예비실험(Pilot Test)을 실행한 것으로서, 이 프로젝트를 발전시켜 1999년 9월부터 상용서비스를 개시한 것이 볼레로넷 서비스이다. 따라서, 본고는 볼레로넷이 서비스를 제공하기 위하여 사용하는 시스템과 그 시스템상의 메시지의 안전한 송수신을 살펴봄으로써 무역업자들이 이 서비스를 사용할 수 있는지 여부를 고찰하고자 하는 것이다.

## Ⅰ. 서론

정보기술의 진전에 의해 상거래의 대부분이 전자화되고 있음에도 불구하고 국제간에서의 무역실무의 전자화에 대해서는 이제까지 거의 전무한 상태이었다. 그 이유는 무역에 관계하는 서류는 수출입업자, 은행, 선박회사 등 다수의 관계자간에서 유통하고 이들 서류에는 선화증권과 같은 유가증권도 포함되고 있고, 세계각국의 법률도 관련되어 있기 때문이었다. 무역절차를 전자화함에 있어서는 국제적인 운용능력, 안전성, 신뢰성, 법제도의 확립이 필요하고, 이제까지 검토는 행해져 왔지만 전자화가 실현되지 못한 것이 현실이다. 하지만 전형적인 무역거래에 있어서는 20여개 이상의 관계자가 관련되어 있고, 40종류의 서류가 유통하고 약 200항목의 명세가 서류에 기재되고, 그 항목의 60-70%는 반복해서 기입되고 있다(APEC의 조사)고 하는 현상이 있고, 이들 사무처리비용은 현재 전무역거래액의 약 7%(UN의 조사)에 이르고 있기 때문에 무역절차의 전자화에 대해서의 조기실현이 전세계적으로 요구되어 왔다.[1)]

유럽에서는 단일 시장의 도입에 따라 인력·상품·자본·서비스·정보 등의 자유로운 이동이 실현되고 전지역에 걸쳐 사업 경영의 통합이 이루어지고 있는 반면, 사업 관리면에서는 복잡해지는 현상이 증폭되어 지고 있다고 지적되고 있다. 이에 EU가맹국들 사이에서 사업관리를 보다 효율적으로 하기 위한 EDI 및 관련 기술이 급속도로 보급되고 있다.

이와 같은 상황하에 EC위원회에서는, EU 가맹국간에 최대한으로 EDI를 도입하고, 그

* 중부대학교 경상학부 조교수

1) http://www.bsbs.co.jp/press/data/t000125.html

도입에 따라 변경되어야 하는 거래관행에 관한 법률적인 제문제를 검토하기 위해 자금을 제공하여, MANDATE 프로젝트, BOLERO 프로젝트 및 EDIBOL 프로젝트라고 하는 세 가지의 프로젝트가 실시되었다. 첫째, MANDATE 프로젝트는 「유통성서류 및 무역거래의 전자관리」(Managing Negotiable Documents and Administrating Trade Electronically)의 약칭으로, 「EDI에 의한 유통성 서류의 전자적 대체물」을 확립하기 위한 법률적·상업적·기술적 방법의 조사연구를 실시하였다[2]. 둘째, BOLERO 프로젝트는 MANDATE 프로젝트의 성과를 기초로 하여, 전자식 선화증권의 실용 가능성에 관련한 예비실험(Pilot Test)을 실행하였다[3]. 셋째, EDIBOL 프로젝트에서는 전자적 환경 하에서 이루어지는 선화증권의 양도에 관련한 법적인 제문제를 검토하고, EDI의 진전을 방해하는 법적인 장애를 제거하는 해결책의 조사연구가 이루어졌다.[4]

볼레로넷은 1994년 6월 영국을 중심으로 홍콩, 네덜란드, 스웨덴, 미국 등의 해상운송회사와 은행, 통신회사 등이 참여하여 컨소시엄형태로 시작된 "볼레로 프로젝트(Bolero Project; Bill of Landing for Europe, Bill of Landing Electronic Registry Organization)"의 결과이다. 무역거래에서의 볼레로(Bolero)는 "Bill Of Landing for EuROpe(유럽을 위한 선화증권)" 또는 "Bill Of Lading Electronic Registry Organization(선화증권 전자등록기구)"의 약어다. 볼레로 시스템은 기존 무역절차를 인정하는 대신 선화증권 등의 모든 무역서류를 전자문서화 함으로써 무역업자, 은행, 보험사, 선박회사, 세관, 항만당국 등의 모든 무역관련 당사자들이 무역관련 서류나 자료를 인터넷을 통하여 디지털 전송방식으로 교환할 수 있도록 하고, 이에 따른 안정성 및 신뢰성을 검증해 전자무역거래를 뒷받침해주는 국제전자무역시스템이다. 현재는 선화증권 뿐만 아니라 모든 무역서류를 전자적으로 유통시킬 수 있도록 네트워크를 제공하고 전자서명의 인증기관역할을 담당하는 것으로 발전되어 있다.

따라서, 본고에서는 볼레로넷이 서비스를 제공하기 위하여 사용하는 시스템에 관하여 살펴보고 그 시스템상에서 메시지의 흐름을 파악함으로써 볼레로 서비스를 안전하게 사용할 수 있는지 여부를 고찰하고자 하는 것이다.

# II. 볼레로넷 서비스와 시스템의 고찰

## 2.1. 볼레로넷 서비스의 개요

### 1) 볼레로넷 서비스의 운영회사

볼레로 프로젝트는 유통성 선화증권의 EDI화를 추진한 최초의 국제규칙인 "전자선화증권에 관한 CMI규칙(CMI Rules for Electronic Bills of Lading; 1990)"에 기초하여 유통성 선화증권의 EDI화 실험을 실시한 것이다. BOLERO 프로젝트에서는 당초, 기술적 및

2) Marinade Ltd., MANDATE - final report for the TEDIS programme, Final version 1.3-04/4/95.
3) The BOLERO Consortium, BOLERO Final Report for submission to the European Commission, Issue 1.0, September 1955.
4) 朝岡良平, 電子商去來時代における貿易慣習, 早稻田商學 第376号, 1998, pp.576-577.

법적 가능성 연구(feasibility study)를 4개월간 행한 후 시스템 설계, 개발 및 사용자거래(user trading)를 1994년부터 순차적으로 행하여 국제적 Pilot Test를 1995년 7월부터 9월까지 실시하는 것으로 하였다. 이 프로젝트는 Dloitte & Touche Europe Services를 중심으로 한 컨소시엄 멤버에 의해 추진되고, 예비실험(Pilot Test)은 영국, 스웨덴, 네덜란드, 미국 및 홍콩의 수출입업자, 운송업자, 은행의 28조직에 의해 실시되었다.[5] 이 테스트에서는 전기통신 및 메시지 전송의 국제표준(X. 400, X. 500 및 UN/EDIFACT 표준), 신뢰 제3자(TTPs)와 관련하여 이용하는 보안 기술 및 전자서명(digital signature)이 사용되었다.[6]

즉, 이 프로젝트는 1994년부터 1995년에 걸쳐 실증실험을 행하고 그 성공을 답습한 후, 1998년 4월에는 SWIFT(세계은행간금융전산망; Society for Worldwide Interbank Financial Telecommunication)와 TT클럽(Through Transport Club)[7]이 각각 50%(각각 1,000만 달러)의 지분을 출자하여 볼레로 운영회사(Bolero Operation Ltd.)를 설립하였다. 그 후, 동사는 명칭을 볼레로 인터네셔널사(Bolero International Ltd.)[8]로 개칭하고, 무역서류의 무서류화(paperless)를 실현하기 위한 기반으로서 1999년 9월 27일부터 Bolero.net[9]을 개시하고, 인터넷을 경유하더라도 전자서류를 안전하고 확실하게 송수신할 수 있는 메시징 서비스와 유가증권인 선화증권을 전자화하고 그 소유권이전을 관리하는 권리등록(Title Registry) 서비스를 개시했다. 즉, 볼레로넷(bolero.net)은 SWIFT와 TT클럽이 주축이 돼 컴소시엄 형태로 구성된 전자결제업체이며 국제적인 무역절차전자화 서비스의 제공회사인 Bolero International Ltd.의 서비스명이다. 볼레로넷은 1999년 1월부터 3월까지 기존 종이문서 체제와 병행하면서 실제로 시범서비스를 운영한 후 동년 9월부터 상용서비스를 개시함으로써 모든 무역서류의 전자화를 추진하고 있다. 볼레로넷 서비스의 상용화로 수출입업체는 무역서류를 들고 은행이나 보험·해운회사 등에 가지 않고 사무실에서 인터넷으로 서류전송부터 최종결제까지 처리할 수 있는 시대가 도래한 것이다.

### 2) 볼레로넷 서비스의 목적

"BOLERO 프로젝트(Bolero Project; Bill of Lading for Europe, Bill of Lading Electronic Registry Organization)"는 무역거

5) 안병수, 전자식 선적서류의 실무적용 실험의 결과고찰, 무역상무연구, 1998, 2, pp.566-568.

6) J. Livermore & K. Euarjai, Electronic Bill of Lading: A Progress Report, Journal of Maritime Law and Commerce vol.28, No.1, January, 1997, p.58.

7) SWIFT(본부: 벨기에)는 전세계의 금융기관이 참가하는 협동조합조직으로서, 73년 15개국 239개 은행이 창립해 현재 189개국 7000여개의 금융기관이 이용하고 있으며, 현재 국제자금결제의 90% 이상을 장악하고 있다. TT클럽(본부: 버뮤다)은 해운회사, 복합운송업자(NVOCC) 등의 손해배상책임보험 상호조합으로서, 세계 80여개국의 운송업자, 운송주선인, 항만당국 등이 회원으로 참여하고 있으며 컨테이너 선단의 2/3, 1725개의 항만시설, 5890사의 운송업자에 대한 보험을 담당하고 있다. 이들 두 기관들에 가입된 1만2천5백 여개의 회원사들은 다시 국제무역을 하는 전세계 거의 모든 회사와 거래를 할 수 있게 된다.

8) 볼레로 인터네셔널사(Bolero International)는 당분간 볼레로 시스템의 소유자이거나 관리자, 또는 그 권리의 계승자를 말한다; bolero.net, Bolero RuleBook, Part 1.1(14).

9) bolero.net은 볼레로인터네셔널사의 거래명칭이다. 볼레로넷은 네트워크를 통해서 전자화된 무역절차서비스를 제공하는 것으로서, 영국 런던의 본사 외에 뉴욕, 도쿄, 프랑크프루트, 파리, 홍콩, 싱가포르, 파리에 지사를 두고 있다. 이는 볼레로 프로젝트에 대하여 95년 7월부터 3개월간의 법적, 기술적 타당성 검토를 위한 테스트를 거친 후 전세계 18개 무역권에 대한 법률분석을 완료하고 시범서비스 기간을 거쳐 1999년 9월 27일 상용서비스를 개시하였다. 우리나라의 삼성전자와 한빛은행을 포함한 전세계 50여개 업체가 회원사로 참여하고 있다.

래에 필요한 종이서류를 전자메시지로 전환하여 안전하게 교환할 수 있는 기반을 제공하는 것을 목표로 하고 있다.[10] 즉, Bolero 프로젝트는 무역거래에 관한 절차의 전자화를 추진하는 것, 구체적으로는 ① 양도성 유가증권인 선화증권 등의 선적서류를 전자화하는 것, ② 그 전자데이터를 중앙등록기관에서 일괄해서 등록하고, 인증제도에 의해서 데이터의 유일성을 확보하고 보존하는 것, ③ 중앙등록기관에 의한 전자서명의 발행, 또는 인증제도를 통한 전자적 양도 등에 의한 유가증권의 유통성을 확보하는 것을 목적으로 추진된 실험프로젝트를 기원으로 한다.[11]

이와 같이 볼레로 프로젝트의 초기 설립목적은 선화증권(B/L)을 전자화하는 하는 것이었으나, 선화증권의 전자화만으로는 전자결제에 큰 기여를 할 수 없다고 판단하여 볼레로넷은 선화증권 뿐만 아니라 모든 무역서류를 전자적으로 처리할 수 있도록 프로젝트의 범위를 넓혔다. 그 목적을 구체적으로 살펴보면 다음과 같다.[12]

첫째, 볼레로 프로젝트는 무역거래에 필요한 종이서류를 전자메시지로 전환하여 안전하게 교환할 수 있는 기반을 제공하는 것을 목표로 하고 있다. 이는 범세계적으로 전자거래에 대한 법적 환경이 정비되는 한편, 전자 메시지의 안전성을 높일 수 있는 암호화 기법도 발전을 거듭함에 따라 이를 바탕으로 무역거래 전반에 관련된 선적서류 전체를 전자화하여 이를 상업적으로 유통시키려는 시도이다.[13]

둘째, 선화증권 및 기타 선적서류의 전자화를 실현하기 위하여 TTP(Trusted Third party; 신뢰 제3자)와 전자서명(Electronic Signature)을 이용한 Pilot Test의 스킴을 구축하고 실시하는 것이다.[14]

셋째, 필요하다고 생각되고 있는 보안(Security)요건을 충족하기 위하여 TTP시스템과 전자서명에 관한 하부구조가 유효하게 기능하는지 여부를 확인하는 것이다.[15]

넷째, 법적 및 상업적으로 입수가능한 전자적 서비스의 Pilot 시스템을 개발하는 것 등이다. 즉, 현단계에서는 EDI에 의한 국제상거래를 규제하는 법률은 존재하지 않는다. BOLERO Polit Test에서는 사용자가 안심하고 계약을 체결할 수 있도록 다음과 같은 방법을 채택하였다. 사용자에 의한 협회로서 클럽(Club)을 결성하고, 클럽내의 모든 메시지의 거래가 안전하게 행해지는 것을 목적으로서, BOLERO거래에 있어서 강제력을 가지는 "BOLERO Rule Book"에 참가자 전원이 따른다고 하는 전제조건하에서 실제의 거래가 행해졌다. 따라서 Pilot test는 클럽내에서의 상거래만을 대상으로 하는 것이다. 폐쇄적 구조중에서의 상거래에 대해서는 규제할 수 있고, Security의 확보도 가능하다. 그러나 이것이 open system으로서 기능하기 위해서는 국제적으로 적용하는 법규의 제정을 가질지도 모를 것이다.[16]

다섯째, 국제표준화를 목표로 하고 있는 볼레로 넷은 전세계 기업들이 문서를 통한 거래에서 낭비하는 연간 4천 2백억 달러의

10) J. Livermore & K. Euarjai, op. cit., p.58.
11) "bolero.net, 營業開始", 『金融』, 1999.11, p.81.
12) 森岡 峰子, 船荷證券のEDI化, 國際商務論の諸問題, 同文館, 1998, pp.151-153.
13) 안병수, BOLERO프로젝트와 TRADE CARD 시스템: http://210.95.204.2/haksup/조대행/조대행1-8.htm.
14) 森岡 峰子, 前揭書, pp.151-153.
15) 森岡 峰子, 上揭書, pp.151-153.
16) 森岡 峰子, 上揭書, pp.151-153.

비용을 줄이는데 목적이 있다.[17]

## 2.2. 볼레로 시스템의 개념과 구성요소

볼레로 시스템은 볼레로규약집과 그 사용을 적용하는 운영규칙 뿐만 아니라, 메시지와 서류를 통신하고 비즈니스 거래를 촉진하기 위하여 볼레로 인터네셔널이 제공하는 디지털 정보시스템과 비즈니스 과정 및 방법이다. 볼레로시스템은 볼레로 인터네셔널과의 합의에 의해 시험적인 거래 및/또는 구속력이 없는 거래에 명백히 제한되어 사용되는 시스템, 소프트웨어, 또는 설비를 포함하지 않는다.[18]

볼레로 시스템의 기술적 구조는 다음의 5개의 기본적인 요소로 구성되어 있다.[19]

이러한 기본적인 요소 중에서, 중앙메시징플랫폼, 권리등록기, 사용자 데이터베이스 및 사용자 지원자원은 볼레로 시스템이 모든 사용자에게 제공하는 서비스이며, 사용자 시스템은 제3자 밴더(third-party vendors) 및 서비스 사무국이 제공한다.

### 1) 중앙메시징플랫폼

중앙메시징플랫폼(Core Messaging Platform; CMP)은 볼레로사용자, 볼레로 인터네셔널 및 볼레로 협회간에 볼레로 사용자에게 그리고 볼레로 사용자로부터 특정 전자메시지를 송신하기 위한 시스템이다. 또한 이것은 일단 송신된 메시지의 수신확인과 추적(tracking)을 제공한다.[20] 또한, 중앙메시징플랫폼은 권리등록기(Title Registry)로 정보를 송신한다. 메시지는 송신자의 선택으로 "서류(Documents)"라고 부르는 추가된 정보의 단위 또는 "첨부서류(attachments)"를 포함할 수 있다.

즉, CMP(Core Messaging Platform)로 불리우는 볼레로넷(bolero.net)의 메시징서비스는 인터넷을 이용하면서, 공개키방식(비대칭키방식)에 의한 전자인증절차와 암호화기술에 의해서 전자화된 서류를 안전하고 확실하게 송수신할 수 있는 통신서비스이다. 또한, 사용자는 모니터링 기능에 의해서 송수신한 메시지(전자서류)의 상태(status)를 파악할 수 있다.[21]

### 2) 권리등록기

권리등록기(Title Registry)는 볼레로 인터네셔널사(Bolero International)에 의해 운영되고, ① 볼레로 선화증권의 소지권(Holdership)과 이전에 관한 기능을 이행하기 위한 수단, ② 현재의 볼레로 선화증권의 상태에 대한 기록, ③ 그러한 볼레로 선화증권과의 거래의 감사추적을 제공하는 응용프로그램을 의미한다. 즉, 볼레로 권리등록기는 볼레로 선화증권에 관한 정보의 중앙전자데이터베이스로서, 전통적인 종이 선화증권에 대한 전자적 대체를 달성함으로써 그러한 주요무역서류의 통신속도 및 효용성을 향상시키는 시스템을 제공한다.

다시 말하면, 권리등록기(Title Registry)는 볼레로 선화증권의 일생에 걸쳐서 변경될 수

17) http://www.goshop.co.kr/news/092703.htm
18) bolero.net, Bolero RuleBook, Part 1.1(16).
19) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 1.2.
20) 보다 엄밀하게, 중앙메시징플랫폼은 일단 송신된 메시지를 기록하고 저장하기 위한 데이터베이스와 연결된 운송메시지에 대한 특별한 우편 서버이다. 그것은 RIDs를 점검하기 위하여 사용자 데이터베이스와 밀접하게 작동한다.
21) http://www.bsbs.co.jp/bolero/main.html

있는 것처럼, 볼레로 선화증권에 관하여 사용자의 권리와 의무에 관한 메시지에 있어서 특별한 지시로 작성된 정보의 데이터베이스이다. 권리등록기의 일반적인 목적은 전통적인 종이 선화증권의 기능을 전자적으로 구현하는 것이다.

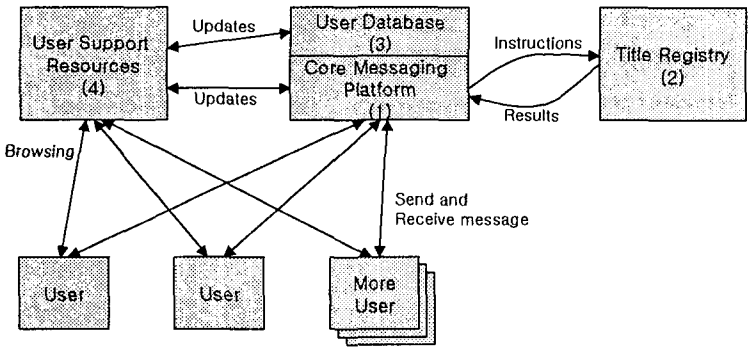
### 3) 사용자 데이터베이스

사용자 데이터베이스(User Database)는 정당하게 인증된 사용자의 신원을 확인하고, 볼레로 시스템에 대한 접속을 제한하고 사용자로부터 메시지의 진정성을 결정하고, 사용자와 교섭하고, 서비스를 위하여 사용자에게 계산서를 보내고, 기타 유사한 목적을 위하여 사용되는 볼레로 참여자에 대한 정보를 보존한다. 단일의 데이터베이스로 언급되어 있더라도, 사용자 데이터베이스는 실제로 일부분은 볼레로 인터네셔널에 의해서, 일부분은 볼레로 협회에 의해서 통제되고 사용되는 상호관련이 있는 일련의 정보의 수집이다.

사용자 시스템은 중앙메시징플랫폼에 인터페이스하기 위하여 볼레로 명세서에 따라야 한다. 볼레로 인터네셔널은 현재 사용자 시스템을 평가하거나 그 안정성 또는 운영에 관한 의견을 나타내지 않지만, 볼레로 인터네셔널은 장차 사용자 시스템을 공인할 수 있다.

### 4) 사용자 지원자원

사용자 지원자원(User Support Resources)은 ① 사용자가 그 메시지를 모니터(monitor)할 수 있도록 중앙메시징플랫폼에 견해를 제공하는 인터페이스, ② 사용자의 관리자가 그 거래(account) 유지할 수 있도록 하는 사용자 데이터베이스내의 인터페이스, ③ 볼레로 사용자에 대한 종합적인 온라인 정보의 수집, 볼레로 시스템의 사용에 관한 지원, 고시 및 경보, 이와 유사한 정보, 그리고 ④ 전화 또는 전자우편에 의한 활발한 지원을 위한 지원창구(help desk)로 구성되어 있다. 더구나 지원자원은 장차 추가될 수 있다. 온라인 사용자 지원자원은 월드와이드웹 브라우저를 통해 사용될 수 있다. 메시지는 중앙메시징플랫폼으로 송신될 수 없고 권리등록기는 사용자 지원자원을 통하여 변경될 수 없다: 이것은 단순히 월드와이드웹을 통하여 온라인 정보에 대한 대화식의 접속을 제공한다.




(그림 2-1) 볼레로시스템 구성요소간 정보 및 거래과정

#### 5) 사용자 시스템

사용자 시스템(User Systems)은 볼레로 시스템을 사용하기 위한 사용자의 로컬 컴퓨터 설비(local computer facilities)로서, 중앙 메시징플랫폼에 연결된 네트워크와 통신링크, 그 통신링크에 연결된 탁상용 컴퓨터(desktop computer) 하드웨어, 중앙메시징플랫폼을 통하여 메시지를 생성하여 송수신하고 사용자 지원수단을 브라우징(browsing)하기 위한 소프트웨어를 포함하고 있다.

# Ⅲ. 볼레로 시스템상의 메시지

## 3.1. 볼레로 시스템의 메시지 구성요소

전형적인 볼레로 메시지의 주요 구성요소는 다음과 같다.[22]

#### 1) 메시지 헤더

메시지 헤더(Message headers)는 전체적으로 메시지의 맨 처음에 나타나는 텍스트(text)의 라인(lines)을 말한다. 메시지 헤더는 메시지의 경로를 설정하고(헤더에 또는 헤더로부터), 메시지가 도착시에 경로가 정해지는 장소를 보여주고, 메시지를 처리하는 방법을 나타내며, 전체적으로 메시지의 수준에 유사한 목적을 제공한다. 메시지 헤더는 표준에 의해서 규정되어 있으며, 볼레로 시스템에 특유한 것이 아니다.

22) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.1.

#### 2) 메시지 파트 헤더

메시지의 본문은 MIME(Multipurpose Internet Mail Extensions)[23]에 대한 명세서에 따라 파트(parts)로 구분된다. 각 파트는 그 컨텐트 유형과 전자우편 경로를 통하여 그것을 통과시키는데 사용된 암호화와 그 컨테트 유형을 적어두는 헤더에 의해서 결정된다. 메시지 파트 헤더(Message part headres)는 MIME 표준에 의해서 규정되어 있으며, 볼레로 시스템에 특유한 것은 아니다.

#### 3) 볼레로 헤더

또한 각 볼레로 메시지는 볼레로 헤더(Bolero Header)를 포함하고 있는데, 볼레로 헤더는 볼레로 시스템내에서 그 유형과 기능을 표시하고, 볼레로 시스템의 로그, 권리등록기, 기타 기록장치에 데이터를 전달하는 메시지의 일부분이다. 볼레로 헤더는 볼레로 시스템에 특유한 것이다. 이것은 볼레로가 규정하고 있는 XML(Extensible Markup Language)과 DTD(document type definitions)에 따라 태그된 데이터를 포함하고 있다.

#### 4) 도큐멘트 파트

볼레로 헤드 뒤에, 메시지는 하나 이상의 추가적인 파트(parts)를 가질 수 있으며, 각각은 메시지 파트 헤더(message part header)가 소개한 서류(Document)를 구성하고 있다. 메시지의 토큐멘트 파트(Document parts)는 때로는 "첨부물(attachments)", "첨부된 서류(attached document)" 또는 그러한 종류의 다른 것으로 정의되고 있다. 토큐멘트 파트

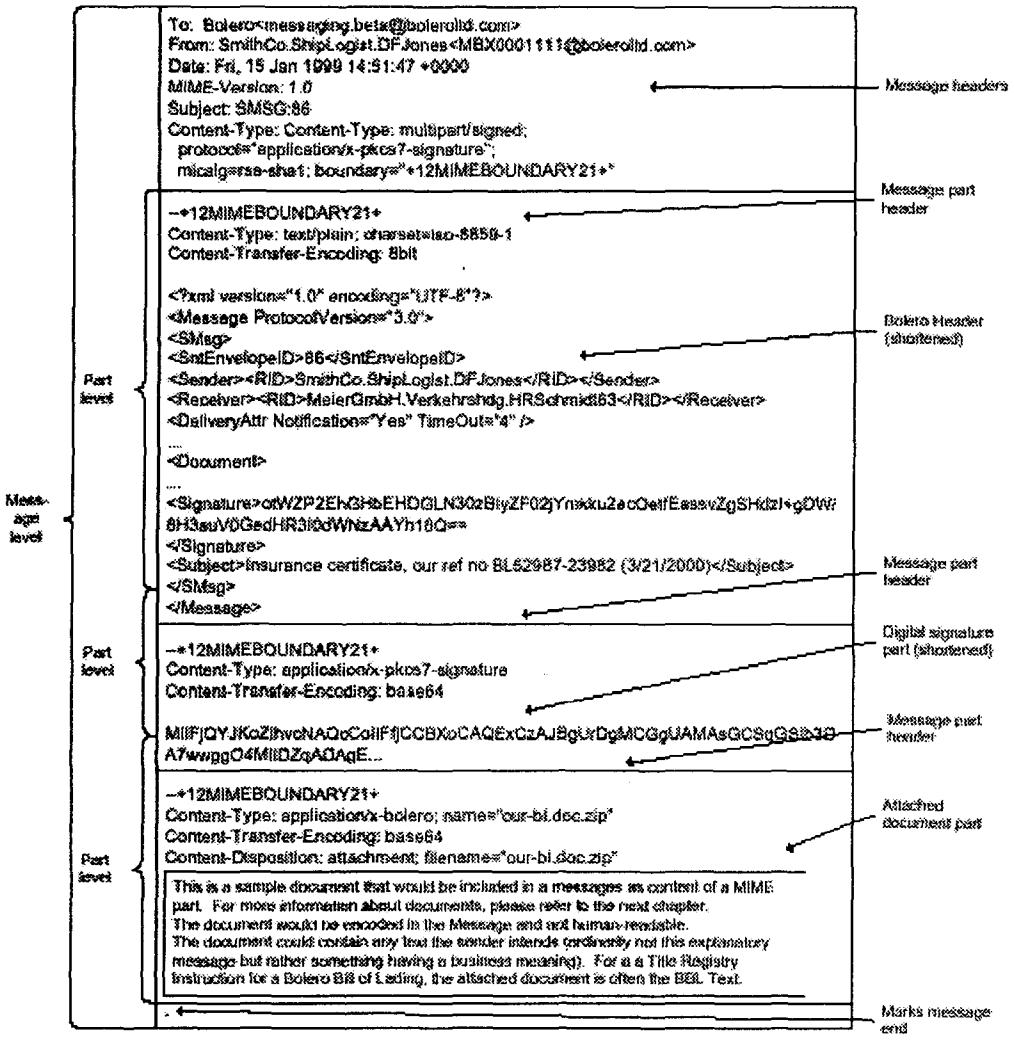
23) SMTP(Simple Mail Transport Protocol)를 사용하는 인터넷 메일을 위하여 메시지 헤더를 규정하고 있는 주요 표준은 IETF(Internet Engineering Task Force)의 RFC 822이다.

는 선택이지만, 볼레로 시스템에서 송신된 대부분의 메시지에 공통적이다. 도큐멘트 파트의 형태는 볼레로 시스템에 특유하지 않으며, MIME 표준에 의해 규정된다.

### 5) 메시지 마침표

하나의 점(dot)을 구성하고 있는 라인(line)은 인터넷 전자우편 표준(즉, IETF의 RFC 822)에 따라 전체적으로 메시지의 끝에 표시된다.

메시지 헤더(Message headers), 메시지 파트 헤더(Message part headers) 및 볼레로 헤더(Bolero header)는 장면(scenes) 뒤에서 메시지를 이동시키고 보존시키는데 주로 사



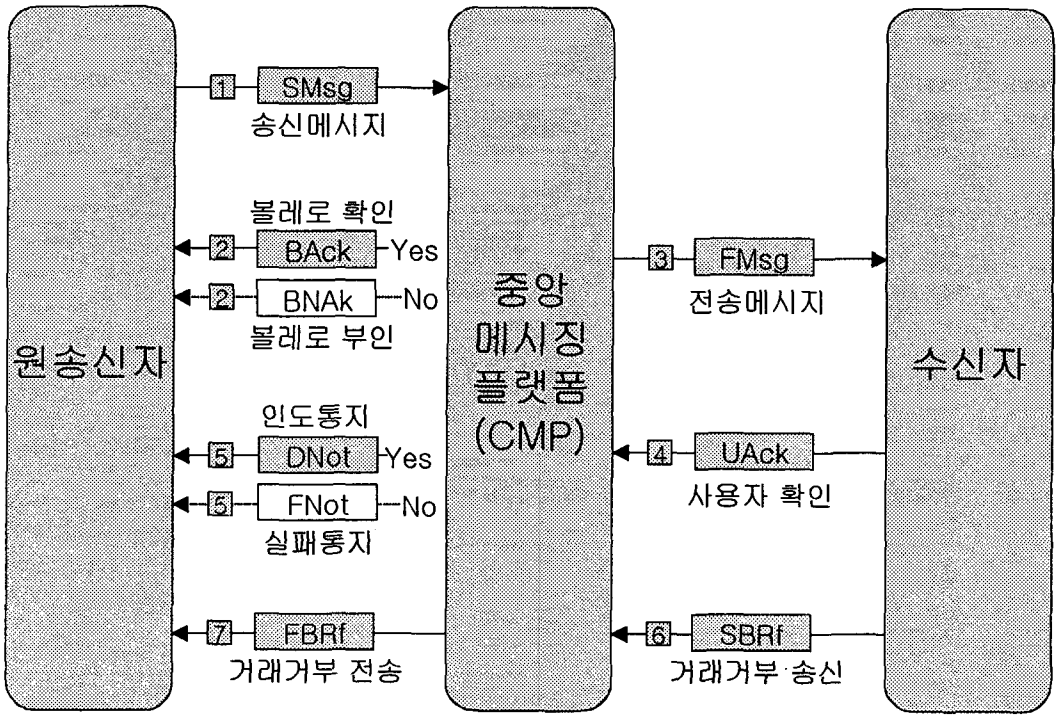

(그림 3-1) 볼레로 메시지의 구성요소

용되는 기계장치이다. 메시지 헤더(볼레로 헤더를 포함)내의 내용이 볼레로 시스템에서 전자적으로 서명되어야 하고 암호화될 수 있더라도, 그 메시지 헤더는 전자적으로 서명되거나 암호화되지 않는다. 메시지를 기술적인 형태로 구성하는 것은 사용자 시스템을 위한 작업이다. 볼레로 시스템은 그것을 위한 기능을 제공하지는 않지만, 그것은 메시지가 정해된 형태로 존재하도록 요구하고 있다. 또한, 사용자 시스템은 가공되지 않은 형태로 수신된 메시지를 나타내지 않는다. 사용자 시스템은 메시지 헤더의 모든 것을 나태내지 않을 수 있다. 대조적으로 메시지내의 볼레로 헤더와 도큐멘트는 볼레로 시스템을 통하여 비즈니스를 수행하는데 광범위하게 사용된다.

## 3.2. 볼레로 시스템상의 메시지의 흐름

볼레로 시스템의 중앙메시징플랫폼과 함께 사용자의 활동은 본질적으로 다음을 구성하고 있다.[24]

첫째, 메시지의 송신이다. 하나의 사용자가 다른 사용자 또는 거기에서 기능을 수행하도록 하는 지시를 가지는 권리등록기와 같은 볼레로 시스템 자원(예를 들면 권리등록기)에 메시지를 송신하는 것이다(예를 들면, 볼레로 선화증권의 생성). 메시지는 볼레로 헤더와 아마 하나 이상의 동봉된 서류, 그 메




(그림 3-2) 모든 볼레로 헤더의 흐름

24) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.2.

시지를 루팅(routing)하고 처리하는데 사용된 헤더로 구성되어 있다.

둘째, 메시지의 수신확인이다. 볼레로 시스템을 통하여 송신된 메시지의 수신을 확인하는 것이다. 사용자가 상대방 사용자(fellow user)로부터 작성하는 메시지를 수신할 때, 운영규칙 제2조는 들어오는 메시지가 수신되었다는 것을 볼레로 시스템에 통지하도록 수신하는 사용자에게 요구하고 있다. 확인(acknowledgement)은 확인된 메시지에서 제시된 특정 의무에 대한 동의가 아니다. 그것은 단순히 메시지가 정당하고 진정한 형태로 도착되었다는 사실의 통지에 불과하다. 수신자가 메시지에 응하여 추가적인 행동을 취하지 않는 경우에도, 그 수신자는 메시지의 수신을 확인한다.

셋째, 비즈니스의 수행거부이다. 수신되고 확인된 메시지에 의하여 비즈니스의 수행을 거부하는 것이다. 이 메시지 유형의 주요한 응용은 볼레로 선화증권에서의 역할에 대한 최근의 지정을 거절하는 것이다.

중앙메시징플랫폼의 메시지는 메시징서비스의 높은 보증을 제공하는데 필요한 각종 기능을 제공하고 있다. 그러한 기능은 메시지에 사용되는 볼레로 헤더의 각종 유형에 합치한다. 볼레로 헤더는 다음의 그림에서 설명되는 숫자를 가지고 다음의 표에 요약되어 있다.

〈표 3-1〉 볼레로 메시지의 유형

| 메시지 유형 | 내 용 |
|---|---|
| ① SMsg: 송신메시지 (Sent Message) | 메시지의 내용이 무엇인지를 제공함. |
| ② BAck: 볼레로 확인 (Bolero acknowledge) | SMsg가 검증할 수 있는 디지털서명이 첨부되고 요구된 기술적 형태로 중앙메시징 플랫폼에 의해 수신되었음. |
| ② BNak: 볼레로 부인 (Bolero Negative acknowledgement) | SMsg메시지가 볼레로 시스템에 의해 수신되었으나 특정기술요건을 충족시키기 못함. |
| ③ FMsg: 전송메시지 (Forwarded Message) | 원SMsg메시지가 포함된 모든 것. 볼레로의 전자서명(원송신자의 전자서명이라기보다는 오히려), 약간 다른 형태로 된 볼레로 헤더를 가짐. FMsg 볼레로 헤더는 원송신자가 누구인가를 나타냄. |
| ④ UAck: 사용자 확인 (User acknowledgement) | FMsg 메시지의 형태로 볼레로에 의해 전송된 것으로서, SMsg가 검증할 수 있는 전자서명이 첨부되고 기술적으로 정확한 형태로 수신자에 의해 수신되었음. |
| ⑤ DNot: 인도통지 (delivery notification) | FMsg 메시지의 형태로 전송된 것으로서, SMsg가 수신자로부터 UAck에서 표시된 것처럼, 정당하게 수신되었음. |
| ⑤ FNot: 실패통지 (fatal notification) | FMsg 메시지의 형태로 전송된 것으로서, SMsg가 지정된 기간내에 UAck의 수신에 의해서 정당하게 확인되었음. |
| ⑥ SBRf: 거래거부 송신 (sent business refusal) | 수신자가 수신되고 확인된 FMsg를 무시하고자 함. |
| ⑦ FBRf: 거래거부 전송 (Forwarded business refusal) | 수신자가 중앙메시징플랫폼에 송신된 SBRf에 따라 수신되고 확인된 FMsg를 무시하고자 함. |

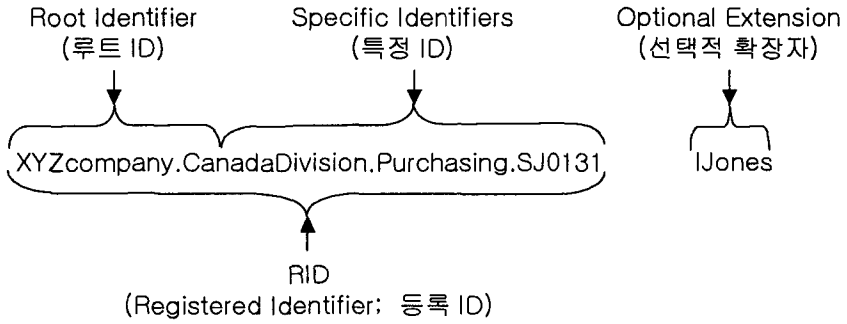
# Ⅳ. 사용자의 신원확인과 메시지 인증

## 4.1. 볼레로 시스템상의 사용자의 신원확인

### 1) RID의 개념

RID(등록된 ID)는 루트 ID(Root identifiers)와 특정 ID(specific identifier)를 포함하고 있는 하위계정(sub-account)에 대한 완성된 ID를 말하는 것으로서, 두 개의 주요 부분과 선택적인 확장자(optional extension)로 구성되어 있다. 두 개의 주요 부분은 각 RID에서 요구되는 루트 ID와 특정 ID이다.

사용자는 회사를 대표하는 개개인의 피고용인 또는 기타 사람이라기 보다는 오히려 회사이다. 따라서, 각 루트 ID는 회사를 의미한다. 사용자 회사는 많은 루트 ID를 가질 수 있지만, 루트 ID는 항상 하나의 사용자만을 의미한다. 볼레로는 각 사용자가 등록될 때 그 사용자에게 루트 ID를 할당한다. 사용자가 합병 등과 같은 근본적인 조직변경을 당하지 않는 한 루트 ID의 변경은 드물다. 루트 ID는 때로는 간결하고, 때로는 비즈니스 또는 법률상의 목적을 위하여 요구되는 명백한 회사를 의미하지는 않는다. 루트 ID가 회사의 공식적이고 법적인 명칭과 유사하다고 하더라도, 루트 ID는 통상적으로 그 회사의 공식적이고 법적인 명칭과 동일하지는 않다. 더구나, 장래의 사용자는 그 루트 ID를




(그림 4-1) RDI와 확장자의 실례

루트 ID(Root identifiers)는 볼레로 시스템 내에서 알려진 사용자의 명칭[25]이다. 모든 무엇으로 할 것인지를 결정하는데 있어서는 약간의 재량권을 가지고 있으며, 사용자는 자신의 실제의 비즈니스 명칭과 관계없는 루트 ID를 선택할 권리가 있다. 볼레로 인증서

25) 루트 ID는 명칭이기 때문에 볼레로 시스템에 기록될 수 있는 사용자의 전자우편을 포함한 주소 및 기타 부속물과는 다르다. 특히, 엄밀히 말하자면, 전자우편 주소는 사용자의 신원을 확인하지 않는다. 오히려, 그것은 전자우편이 수신될 수 있는 기계장치의 기억장소(location)를 확인한다. 거리주소, 전화번호 및 기타 지역코드처럼, 전자우편 주소는 회사를 확인하는데 도움이 되는 부속물이 될 수 있지만, 회사 그 자체는 아니다. 그러한 일체의 부속물은 그 회사의 실체에 실질적으로 영향을 미치지 않고서도 변경할 수 있다. 다른 모든 사용자와 구별되는 것처럼, 법인의 실체는 루트 ID가 무엇을 의미하고 있는 것인가 하는 것이다.

는 공식적 또는 법적인 명칭이 아니라 그 루트 ID로만 가입자(subscriber)의 신원을 확인하며, RID를 구성하기 위한 하나 이상의 특정 ID에 의해서는 선택적으로 그 가입자의 신원을 확인한다. 사용자의 정당한 법적인 명칭을 확인하기 위하여 사용자는 RID등록을 조회하여야 한다.[26]

특정 ID(specific identifier)는 사용자의 내부관리목적을 위하여 사용자 내부의 부, 과 및 개인을 보다 상세하기 표시하는데 사용될 수 있는 하나 또는 그 이상의 것으로서, 선택(공통이 아닌)이 가능하다.

사용자는 루트 ID에 회사의 부, 과 또는 개인을 의미하고 있는 더 구체적인 ID(specific identifier)를 추가할 수 있다. 특정 ID를 수반하고 있는 것과 함께 루트 ID는 RID라고 명명된다. 또한, 사용자는 사용자가 희망하고 있는 것은 무엇이든지 주목하는 "확장자(extension)"를 RID에 추가할 수 있다.[27] 특정 ID와 확장자는 모두 선택이며, 사용자에 의해서 결정된다. 특정 ID와 확장자는 전적으로 사용자의 편의를 위한 것이며, 사용자간의 법적 의미는 없다. 이것들은 사용자가 그 조직내에서 내부적으로 볼레로 능력의 분배를 조직하는 것을 가능하게 할 수 있다. 그러나 특정 ID 또는 확장자가 루트 ID에 추가된 것에 관계없이, 기타 사용자는 메시지에 대한 책임이 있는 신원이 확인된 사용자를 고려할 수 있다.[28]

RIDs는 메시지 또는 서류를 송신한 자의 신원을 확인하는 편리한 비공식적인 수단(informal means)이다. 그러나 전자서명의 검증은 메시지를 가진 송신자의 신원을 확인하기 위한 안전한 수단이다. RID없이 메시지를 송신하는 것은 기술적으로 불가능할 뿐만 아니라 운영규칙 제3조와 제4조[29]의 위반이다. 대부분은, 볼레로 시스템은 운영규칙 제3조와 제4조를 시행하고 있다. 그것은 중앙멤시징플랫폼을 통하여 메시지를 처리하는데 있어서 완전한 RID를 저장하고 통과시킨다. 정식으로 요구된 RID가 메시지의 볼레로 헤더(Bolero header)에 있는 정확한 장소에서 발견되지 않는 경우, 또는 RID(또는 그 내부의 루트 ID)가 해제되거나, 또는 취소, 제명 또는 정지된 사용자를 나타내는 경우에는 볼레로 시스템은 부인(negative acknowledgement)을 반송(return)한다. 또한, 중앙메시징

26) 두 루트 ID간의 관계는 볼레로 시스템에서 아직 정의되어 있지 않다. 따라서 RID 등록은 관련이 있더라도, 한 사용자가 법인으로서 다른 사용자와 어떻게 관련되어 있는지를 나타내지는 않고 있다. 관련된 기업들의 루트 ID는 서로 유사하거나 또는 유사하지 않을 수도 있다. 그리고 한 회사는 모회사이고 다른 회사는 자회사라거나, 또는 그 회사들이 심지어 지분을 공유한 법인조직의 일부라고 하는 RID에 기초한 가정은 발견되지 않는다: bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.3.1.

27) 확장자 필드(field)의 사용은 특정 ID가 얼마나 명확한 것인지에 달려있다. RID가 개개의 수준으로 아래로 확장되는 특정 ID를 포함하고 있는 경우에는 RID 확장자는 아마 추가할 가치를 거의 확인하지 않을 것이다. 덜 정밀한 특정 ID에 대하여, 사용자는 그 지역사용자(local user)에게 중요한, 그리고 정말로 그 지역사용자에게만 중요한 피고용인의 머리글자 또는 기타 정보를 기입하는 것이 유익하다는 것을 알 수 있다. 볼레로 시스템과 기타 사용자의 시스템은 확장자를 점검하지 않고 기계적인 방법으로 확장자를 단순히 통과할 뿐이다. 확장자는 사용자가 원하는 것은 무엇이든지 가능하기 때문에, 기타 사용자는 통상적으로 확장자에 중요한 의미를 부여할 수 없다.

28) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.3.1.

29) 운영규칙 제3조에서는 "중앙메시징플랫폼에 송신된 모든 메시지에 있어서, 사용자는 메시지 송신자의 신원을 확인하는 RID로서 그 루트 ID(그리고 또한 선택적으로 특정 ID와 확장자)를 명시하여야 한다"고 규정하고 있으며, 운영규칙 제4조에서는 "어떤 사용자가 등록되지 않거나 또는 볼레로 인터네셔널사가 그 사용자에 대하여 루트 ID를 할당하지 않은 경우에는 사용자는 중앙메시징플랫폼으로 송신된 메시지에 루트 ID를 포함시키려고 해서는 안된다.

플랫폼은 RID를 보유하고 있는 메시지가 그 RID와 결합된 비밀키(Private key)에 의해서 전자적으로 서명되는지 여부를 결정하는 것을 점검한다.[30]

## 4.2. 볼레로 시스템상의 인증서와 전자서명

RID와 루트 ID는 비밀이 아니다. 사용자는 사용자 지원자원에서 다른 사용자의 루트 ID를 찾아볼 수 있으며, 사용자는 종종 송신하는 메시지를 위한 준비된 주소록으로서 공통적인 RIDs의 목록을 보유하고 있다. 모든 사용자가 상호간의 루트 ID를 가지고 있기 때문에, 루트 ID는 메시지를 인증하는 안전한 수단이 아니다. 따라서, 일반적으로 사용자는 메시지가 진정으로 신원이 확인된 사용자에 의해서 서명되거나 또는 그와 관련된다는 것을 루트 ID에 의해서만 확실하게 추론할 수 있다. 전자서명이 유효한 인증서의 참조에 의해서 정당하게 검증될 수 있는 경우에는, 오히려 그 추론은 사용자의 전자서명으로부터 도출되어야 한다. 여기에서는 볼레로 시스템상의 전자서명과 그 사용에 적용되는 원칙을 소개하고자 한다.[31]

### 1) 전자서명의 생성과 검증

전자서명은 정해진 데이터의 단위와 정해진 비밀키(Private Key)에 유일한 대수(large number)를 산출하는 복잡한 수학적인 계산의 결과로 생긴다. 서명된 데이터와 서명하는 비밀키에 유일한[32] 그 대수는 전자서명이다.

비밀키는 전자서명이 처리되어야 하는 또 하나의 대수이다. 비밀키는 그러한 대수들을 기억하는 것이 실제적으로 불가능한 대수이다. 대신에, 비밀키는 컴퓨터 파일로 스마트카드[33] 또는 기타 저장매체에 저장된다. 비밀키를 수용하고 있는 스마트카드 또는 기타 저장장치는 서명을 위한 비밀키를 사용하기 위하여 사용자가 인증한 자에게 소유되어 독점적으로 유지되어야 한다. 인증받지 못한 자가 다른 사람의 비밀키를 획득하는 경우, 인증받지 못한 자는 마치 자신이 정당한 비밀키 소지인인 것처럼, 전자적으로 서명할 수 있을 것이다. 다른 사람의 비밀키를 이용하여 전자적으로 서명함으로써, 서명인은 사실상 전자문서를 위조하고, 정당한 비밀키 소지인의 역할을 한다. 사용자가 비밀키로 생성한 모든 전자서명에 책임이 있기 때문에[34], 사용자는 비밀키를 안전하게 유지하도록 권고되며, 비밀키 보안을 유지하도록 설계된 보안정책을 가지도록 권고된다.

전자서명이 생성된 후, 그 전자서명은 검증(Verification)이라고 하는 또 하나의 수학적인 과정에 의해서 서명된 데이터에 대한 그 서명인의 서명으로 검증될 수 있다. 전자서명을 검증하기 위하여, 컴퓨터는 기능을

30) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.3.1.

31) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.3.2.

32) 숫자가 어떤 다른 것(일반적으로 다른 큰 숫자, 그리고 서명되는 데이터는 전자서명목적을 위한 숫자로 축소된다)에 유일하다는 이 절의 설명은 두 숫자간의 일대일의 수학적인 합치가 있다는 것을 의미한다. 그러나, 그러한 사실의 정확성은 컴퓨터의 사용가능성의 한계에 의해 구속된다. 컴퓨터의 처리과정은 안전한 전자서명보안을 유지하기 위하여 시간이 경과하는 것처럼 훨씬 더 막대한 숫자를 필요로 한다.

33) 스마트카드(Smart cards)는 신용카드크기의 데이터저장장치이다. 그러나 신용카드와는 달리, 스마트카드는 카드상의 데이터를 안전하게 돕도록 구성될 수 있는 운영회로를 가지고 있다.

34) bolero.net, Bolero Rulebook, Part 2.2.4(1).

수행하고, 서명되어야 하는 데이터와 인증서를 제공한다. 중앙메시징플랫폼은 자신이 수신하고 전송하는 모든 메시지상의 전자서명을 검증하고, 메시지가 볼레로 시스템으로부터 들어온다는 것을 사용자가 확신하는 경우에는 모든 사용자는 중앙메시징플랫폼이 볼레로 시스템으로부터 수신하는 모든 메시지상의 볼레로 전자서명을 검증하여야 한다.

인증서(certificate)와 전자서명은 비밀키의 소지인의 신원을 확인하는 전자적 기록을 의미한다. 소지인은 명칭에 의해서 신원이 확인되며, 비밀키는 이에 합치하는 공개키를 포함함으로써 표시된다. 비밀키는 비밀이기 때문에 인증서에 포함되지 않으며 인증서는 널리 배포된 전자기록(digital record)이다. 또 하나의 대수인 전자서명은 그 비밀키에 유일하며, 따라서, 공개키는 그 비밀키를 표시하고 확인하는데 사용될 수 있다. 한 쌍의 공개키와 비밀키는 수학적으로 관련되어 있지만, 공개키를 가지고 비밀키를 복원하는 것은 컴퓨터의 조작으로 불가능하다.

전자서명검증이 긍정적인 결과(positive result)를 산출하는 경우, 전자서명은 수학적인 사실, 즉, ① 데이터의 단위가 전자적으로 서명된 이후에는 그 전자적으로 서명된 데이터의 단위는 변경되지 않았다는 사실, ② 전자서명은 인증서에 포함된 공개키에 합치하는 비밀키로 생성되었다고 하는 사실로서 설명할 수 있다. 그 인증서는 특정 사용자로서 그 비밀키의 소지인(전자서명인)의 신원을 확인한다. 그래서 그 검증인은 전자서명이 그 특정 사용자에 의해서 생성되었다는 것을 인증서에 기초하여 추론할 수 있다.

볼레로 규약집에서 "서명된(signed)"의 정의에 의하여, 전자서명이 볼레로 인터네셔널 사가 발행한 인증서에 포함된 공개키를 사용하여 검증될 수 있는 경우에는 그 전자서명은 법적으로 그 사용자에 기인하며, 전자서명이 생성되었을 때 유효하다. 이와 같이, 전자서명이 인증기관에 의해서 발행된 인증서에 포함된 공개키를 이용하여 검증될 수 있는 경우에는 전자서명은 특정 사용자의 것으로 보며, 그 전자서명이 생성되었을 때 유효하다.

요약하면, 전자서명은 메시지를 특정 비밀키와 관련시킨다. 그 전자서명의 검증은 비밀키가 이를 생성하는데 사용되었다는 것을 나타내고, 인증서는 사용자가 그 비밀키를 보관하고 있다는 것을 나타낸다. 정당한 검증에 비추어, 메시지는 그 서명인에게 기인될 수 있다. 따라서, 볼레로 규약집은 자신들의 전자서명에 대하여 서로에게 책임있는 사용자를 가지고 있으며, 법적 형식요건(서면, 서명, 원본 등)이 서명된 메시지에 의하여 충족된다는 것을 규정하고 있다.[35]

### 2) CMP상의 전자서명의 실행

볼레로 시스템내에서 전자서명과 인증서의 적용과 관련하여 볼 때, 각 메시지는 등록된 볼레로 사용자에게 인증된 비밀키를 이용하여 전자적으로 서명되어야 한다. 그렇지 않은 경우에는 볼레로 시스템은 그 메시지를 폐기한다. 각 사용자의 메시지상의 전자서명은 볼레로 시스템내의 데이터베이스에 보관된 인증서에 의해서 검증된다. 그 메시지는 볼레로 인터네셔널의 전자서명으로 송신된다. 수신자의 사용자 시스템은 볼레로 인터네셔널의 전자서명을 검증하여야 하는데, 그

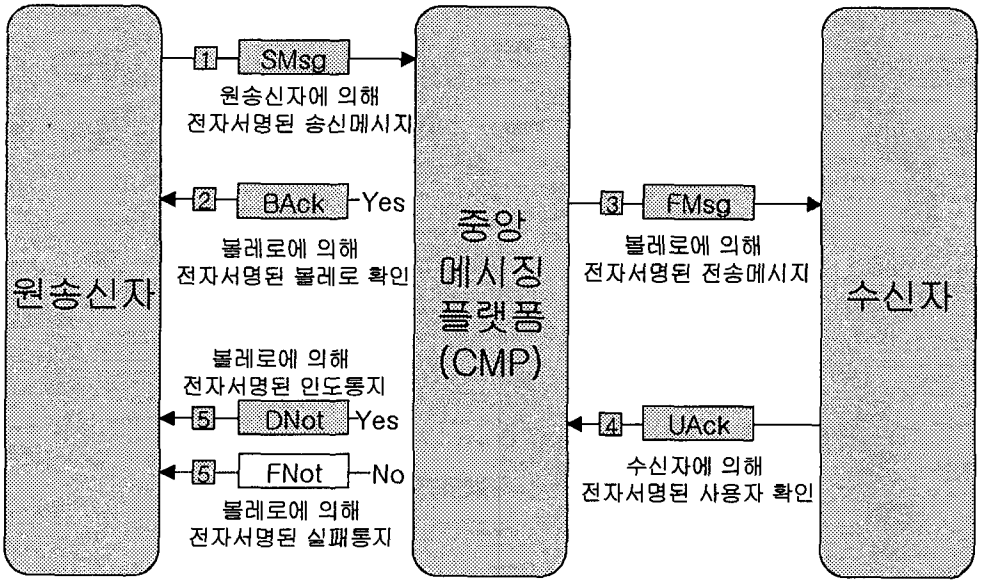
35) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.3.2.1.

것은 볼레로 인터네셔널이 원메시지상의 전자서명을 검증했다는 사실을 증명할 것이다. 볼레로 시스템을 통하여 송신된 모든 서류와 권리등록지시는 전자적으로 서명되고 검증된 메시지에 동봉된다. 볼레로 시스템상의 각 메시지, 서류 및 권리등록지시의 인증은 증명될 수 있고 안전하다.[36]

하나의 사용자가 다른 사용자에게 메시지를 송신하는 과정은 다단계의 연속이다. 송신자는 메시지를 전자적으로 서명한다. 중앙메시징플랫폼이 하나의 사용자로부터 다른 사용자에게 메시지(확인을 포함)를 중계할 경우, 이 플랫폼은 원송신자로부터 중계된 메시지를 전자적으로 서명한다. 그 전송된 메시지상의 전자서명이 운영서비스계약에서 규정된 것처럼, 원메시지상의 원송신자의 서명의 검증을 입증한다. 다음의 그림은 이러한 일련의 서명 및 메시징의 과정이다.[37]

첫째, 송신메시지(Sent Message; SMsg)를 전자서명하여 송신한다. 즉, 작성하는 사용자는 특정 수신자에게 전송하기 위한 볼레로 시스템에 메시지를 전자서명하여 송신한다.

둘째, 볼레로 시스템은 볼레로 확인(BAck; Bolero Acknowledgement) 또는 볼레로 부인(BNak: Bolero Negative Acknowledgement)를 전송한다. 즉, 볼레로 시스템은 SMsg상의 송신자의 전자서명을 검증하고, 그 진정성과 형식을 점검한 후, 볼레로 시스템이 원송신자의 전자서명을 정당하게 검증하고 그 내용(content)을 정확하게 인지한 경우에는




(그림 4-2) CMP를 이용한 서명된 메시지의 흐름

36) Welcome to Digital Signature in the Bolero System: http://www.bolero.net/downloads/digisigs.pdf

37) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.3.2.2.

원송신자에게 BAck를 송신한다. BAck 메시지는 볼레로 시스템의 운영자인 볼레로에 의해 서명된다. 볼레로 시스템이 전자서명을 정당하게 검증하지 못하거나 또는 형식상 오류(errors)를 인지한 경우에는 그 시스템은 SMsg 메시지를 폐기한다.

셋째, 볼레로 시스템은 전송메시지(FMsg; Forwarded Message)를 전송한다. 원송신자로부터 SMsg가 검증된 전자서명을 가지고 있거나 또는 기술적 형식상 정당한 경우에는 중앙메시징플랫폼은 최종 수신자에게 FMsg의 형태로서 SMsg를 송신한다. FMsg 메시지는 볼레로 인터네셔널사의 명의로 중앙메시징플랫폼에 의해서 전자적으로 서명된다. 그 전자서명은 FMsg가 볼레로로부터 송신되었다는 것을 나타내며, 중앙메시징플랫폼이 원 SMsg 메시지상의 송신자의 전자서명을 정당하게 검증하였다는 것을 추가적으로 입증한다. 요청하는 대로, 볼레로 인터네셔널사는 운영서비스계약에 따라 그 검증의 증거를 제공할 것이다.

넷째, 수신자는 사용자확인(UAck)을 송신한다. FMsg 메시지를 수령하자마자, 수신자의 사용자 시스템은 FMsg상의 볼레로 전자서명을 검증하고자 한다. 그 전자서명이 검증되고, 그 메시지의 기술적 형식이 정확한 경우에는, 그 수신자의 사용자 시스템은 중앙메시징플랫폼에 UAck를 송신함으로써 응답한다. UAck 메시지가 중앙메시징플랫폼에 송신되기 전에 그 메시지는 FMsg 메시지의 수신자에 의해서 전자적으로 서명된다.

다섯째, 중앙메시징플랫폼은 인도통지(DNot; Delivery Notification) 또는 실패통지(FNot; Failure Notification)를 송신한다. 중앙메시징플랫폼이 UAck 메시지를 수신한 경우, 그 플랫폼은 원SMsg의 송신자에게 DNot 메시지를 중계한다. 중앙메시징플랫폼이 명시된 기간내에 UAck 메시지를 수신하지 못한 경우에는 그 플랫폼은 원송신자에게 FNot 메시지를 중계한다. 경우에 따라서 DNot 또는 FNot은 볼레로 인터네셔널사의 전자서명을 보유하고 있으며, 그 전자서명이 UAck상의 수신자의 전자서명에 대한 정당한 검증을 입증한다.

여섯째, 송신하는 사용자는 SBRf를 송신하고, 중앙메시징플랫폼은 FBRf를 송신한다. 송신하는 사용자는 SBRf 메시지를 서명하고 중앙메시징플랫폼은 그것이 서명되는지 여부를 결정하기 위하여 메시지를 점검한다. 그러한 경우, 중앙메시징플랫폼은 원SMsg의 송신자에게 합치하는 FBRf 메시지를 전자적으로 서명하여 송신한다.

볼레로 시스템은 UNAk와 유사한 방법으로 최종 수신자로부터 거래거부(SBRf; Sent Business Refusal)를 취급한다.

## 4.3. 사용자의 책임

볼레로 시스템에서는, 그 시스템내에서 전자적으로 서명된 메시지와 서류는 법적으로는 전자서명을 검증하는데 사용된 인증서에 포함된 사용자에 의해서 서명된 것으로 본다. 어떤 사용자가 RID에 의해서 신원이 확인될 수 있는 경우에도, 그 사용자는 특정부서, 피고용인 또는 사용자의 대표를 위한 특정 ID(specific identifiers)를 포함하고 있는 회사이다.

볼레로 시스템에 송신된 모든 메시지에 있어서 RIDs상의 특정 ID에도 불구하고, 사용자 회사는 그러한 모든 메시지에 대한 책임

이 있다. 물론, 사용자가 송신한 모든 메시지는 실제로 사용자의 대리인(피고용인, 독립계약자 및 사용자를 위하여 활동하는 기타의 자를 포함한다)의 손에 의해서 송신되거나, 또는 사용자가 그것을 위하여 행동하도록 구성한 프로그램 또는 자동화된 루틴(routines)에 의해서 송신된다. 그러한 대리인에 대한 정당한 인증의 결핍, 또는 그러한 프로그램 또는 루틴의 부당한 설계 혹은 운영은 그 서명된 메시지에 대한 책임으로부터 사용자 회사를 면제시키지 않는다. 그 사용자에 대하여 인증된 사용자의 루트 ID(Root Identifier)와 비밀키를 이용하는 모든 사람은 사용자를 구속하게 되는 자신들의 행동에 필요한 권한을 가지고 있는 것으로 본다.[38]

# V. 메시지와 서류의 암호화

## 5.1. 메시지와 서류의 암호화

메시지와 서류를 송신하는 사용자가 원하는 경우에는, 그 사용자는 그 메시지와 서류를 암호화할 수 있다. 암호화는 볼레로 규약집에 의해서 요구되지 않는다. 그러나 사용자가 원하는 경우에는 그 사용자는 메시지를 암호화하기 위하여 선택할 수 있다. 각 사용자의 사용자 시스템과 중앙메시징플랫폼은 통상적으로 암호화와 복호화의 작업을 취급한다. 그래서 암호화 및 복호화는 쉽고 조심성이 있다. 암호화는 단순히 완전한 원문(clear text)을 송신하는 것보다 더 안전한 수준으로 중앙메시징플랫폼을 통하여 송신된 메시지의 기밀성(confidentiality)을 보증하는 수단이다. 메시지를 송신하는데 사용되는 전자통신채널은 기본적인 기술수준에서 그다지 안전하지 않다. 중앙메시징플랫폼에 의해서 이용된 통신채널상의 도청은 쉽지도 않고 가능성도 없는 것처럼 보인다. 그러나 암호화는 기밀성의 보증을 요구하는 사용자를 위한 선택이며, 준거법하에서 그것을 사용할 사용자의 권리에 의존한다. 기밀성을 위하여 암호화를 이용하는 것은 공개키와 비밀키 및 인증서를 필요로 하지만, 전자서명과는 다른 방법으로 이용된다. 공개키 및 비밀키 암호화기술의 기본적인 특성은 한쌍의 키중에서 하나의 키는 다른 키가 암호화한 것을 복호화한다. 그 비밀키는 그 인증된 소지인에 의해서만 이용될 수 있다. 반면, 공개키는 누구든지 알 수 있다. 수신자의 눈을 위해서만 예정된 메시지를 암호화하는데 이러한 원칙을 적용함으로써, 그 송신자는 그 메시지를 암호화하기 위하여 수신자의 공개키를 사용한다. 수신자는 그 메시지를 복호화하기 위하여 그 비밀키를 사용한다.[39]

잘못된 공개키를 사용하여 메시지를 암호

38) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.3.3.

39) 암호화 과정은 대부분의 어플리케이션에 있어서 실제로 조금 더 복잡하다. 공개키와 비밀키 암호화 및 복호화 알고리즘은 통상의 컴퓨터상에서 매우 느리게 운영된다. 따라서, 대량의 정보를 암호화하기 위하여 이 알고리즘을 이용하는 것은 불편한 대기기간을 요구한다. 이러한 문제를 해결하기 위하여 암호화 알고리즘은 통상적으로 메시지를 암호하기 위하여 하나의 키만을 요구하는 보다 단순한 알고리즘을 사용하고 있고, 그들은 수신자의 비밀키를 이용하여 그 키를 암호화한다. 수신자는 수신자의 비밀키에 의해서 미리 암호화된 키를 복호화하기 위하여 자신의 공개키를 이용하고 메시지를 복호화하기 위하여 그 복호화된 키를 이용함으로써 메시지를 복호화한다. 이와 같이 메시지의 암호화는 실제로 신속성을 이유로 단일키 알고리즘을 이용하여 실행하고, 그 단일키를 암호화하기 위해서만 공개-비밀키 알고리즘을 이용하여 실행한다; bolero.net, Appendix to Bolero RuleBook (Operating Procedures), 2nd ed., section 2.4.

화한다면, 수신자는 메시지를 복호화하거나 읽을 수 없을 것이다. 왜냐하면, 수신자의 비밀키는 이에 합치하는 공개키로만 복호화하기 때문이다. 암호화하는 송신자는 정확한 공개키를 사용하는 것을 확신하도록, 송신자는 수신자가 소유하고 있는 비밀키에 정확하게 합치하는 그 공개키를 보증하는 인증서를 필요로 한다.

인증서는 수신자와 그 사용자 시스템이 비밀키를 관리하고 암호화기술을 실행하는 방법에 따라, 전자서명을 검증하기 위하여 동일한 것이 이용되거나 또는 다른 것이 이용될 수 있다. 흔히 관리자는 비밀키가 분실되는 경우에 암호화된 정보가 재생될 수 있도록 암호화를 위하여 이용되는 비밀키의 백업 사본(backup copies)를 간직하고 있다. 그러나, 인증을 위하여 이용된 비밀키의 사본을 여러 개 가지고 있는 것은 종종 비밀키의 인증 기능을 손상시키는 것으로 간주된다. 그러한 이유로, 암호화용과 인증용의 각각의 비밀키는 암호화된 정보의 재생이 필요한 경우에 암호화키의 사본을 가지고 있는 신뢰할 수 있는 관리자와 함께 종종 사용된다.

현재 볼레로 시스템에서 실행되고 있는 것처럼, SMsg 메시지의 송신자가 그 SMsg 메시지를 암호화[40]하여 중앙메시징플랫폼에 송신하는 경우, 중앙메시징플랫폼은 자신이 송신하는 모든 메시지(BAck/BNAk, FMsg, DNot/FNot 등)를 암호화한다. 다만, 그 메시지를 수신하는 하위계정(sub-account)은 암호화가 있는 인증서를 가지고 있어야 한다. 6.3.2.5절에서 설명하는 것처럼, 사용자 데이터베이스는 사용자의 조직내의 상대방에게 할당된 인증서가 그 사용자에 의해서 그 하위계정에 어드레스를 지정하여 전송된 메시지를 암호화하거나 또는 그것으로부터 메시지를 복호화하기 위하여 사용하도록 허용되는지 여부를 기록한다. 암호화가 준거법을 위반하는 경우, 사용자는 하위계정에 있는 모든 인증서에 대한 암호화를 무력하게 할 수 있다. 그러면, 중앙메시징플랫폼은 그 하위계정에 또는 그 하위계정으로부터 메시지를 암호화하거나 복호화하는 것을 중지할 것이다.[41]

## 5.2. 암호화된 메시지와 서류의 송수신

SMsg-FMsg 메시지 연속의 모든 흐름은 암호화가 각 단계에 추가된 것을 제외하고, 암호화되지 않은 메시지에 대한 것과 거의 동일하다(암호화가능 인증서의 유효성을 추정하면서). 암호화된 메시지의 흐름은 단계적으로 보다 상세하게 다음의 그림에서 설명하고 있다.[42]

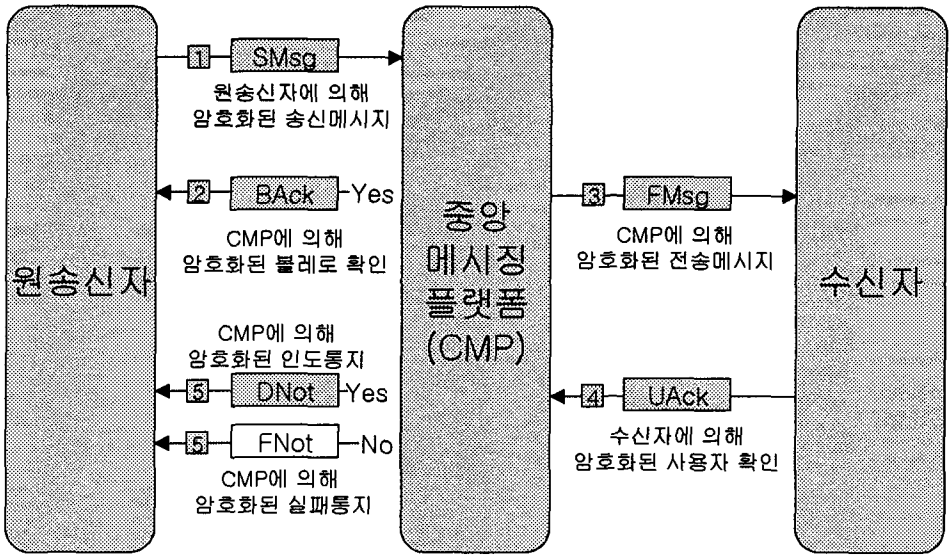
첫째, 송신자는 SMsg를 암호화하여 송신한다. 송신자는 SMsg 메시지를 작성하고, 송신자의 비밀키를 이용하여 그것을 전자적으로 서명하고, 중앙메시징플랫폼에 의해서 이용되는 비밀키에 합치하는 공개키[43]를 이

40) 운영규칙 제1조의 메시지 형식요건은 암호화와 관련되어 있다. 이것은 예정된 수신자의 공개키가 상기에서 설명된 것처럼 대칭키를 암호하는데 사용된다는 것을 요구한다. 대칭키는 3중의 DES 알고리즘으로 사용되고 있는데, 이 알고리즘은 미국정부에 의해서 공표된 FIPS 46이라고 하는 데이터 암호화 표준(DES)과 두 개 또는 세 개의 다른 키를 이용하여 세 번 연속해서 데이터 암호화 알고리즘을 적용함으로써 그 입력의 블록을 변형시키는 암호화 과정이다. 3중의 DES는 ANSI X9.52에서 표준화되어 있다.

41) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.4.

42) bolero.net, Appendix to Bolero RuleBook(Operating Procedures), 2nd ed., section 2.4.

43) 그 공개키는 그 기업자로서 볼레로 인터네셔널을 포함하고 있는 인증서부터 획득된다. 인증서는 볼레로 시스템을 통하여 널리 배포되며, 통상적으로 모든 사용자 시스




(그림 5-1) CMP를 이용한 암호화된 메시지의 흐름

용하여 그것을 암호화하고, 중앙메시징플랫폼에 그 메시지를 송신한다.

둘째, 중앙메시징플랫폼은 송신자에게 BAck/BNAk를 반송(return)한다. SMsg 메시지를 수신한 중앙메시징플랫폼은 비밀키를 이용하여 그 메시지를 복호화한다. 그 다음 중앙메시징플랫폼은 (a) 그 전자서명이 검증되고, (b) 그것이 운영규칙 제1조가 요구하는 것과 같이 기술적으로 정확한 형식이고, (c) 메시지를 암호화한 송신자가 사용자 데이터베이스내의 하위계정(sub-account)에 암호화가능 인증서(encryption-enabled Certificate)를 가지고 있는지 여부를 결정하기 위하여 SMsg 메시지를 검토한다. SMsg 메시지가 기술적으로 정확한 형식이 아니거나 암호화가능 인증서를 가지고 있지 않은 경우에는 중앙메시징플랫폼은 BNAk를 반송한다. 중앙메시징플랫폼이 SMsg 메시지상의 전자서명을 검증할 수 없는 경우에는 중앙메시징플랫폼은 그 메시지를 폐기한다.

셋째, 중앙메시징플랫폼은 수신자에게 FMsg를 전송한다. 중앙메시징플랫폼이 송신자에게 BAck 메시지를 반송하는 경우에는 그것은 또한 SMsg에 근거하고 있는 FMsg 메시지를 작성하고, 중앙메시징플랫폼의 비밀키를 이용하여 FMsg 메시지를 전자적으로 서명하고, 사용자 데이터베이스내의 수신자의 하위계정에 있는 암호화가능 인증서로부터 획득된 수신자의 공개키를 이용하여 그 메시지를 암호화한다.(그러한 인증서가 발견될 수 없는 경우, 중앙메시징플랫폼은 FMsg 메시지를 암호화하지 않는다.) 그 다음 중앙메시지플랫폼은 FMsg 메시지를 수신자에게 송신한다.

넷째, 수신자는 중앙메시징플랫폼에 UAck를 반송한다. 수신자의 사용자 시스템이 그 메시지를 수신하고, 수신자의 비밀키를 이용

템에 설치된다.

하여 그 메시지를 복호화하고, 메시지상에 볼레로 인터네셔널의 전자서명을 검증하고, 그 메시지가 기술적으로 정확한 형식으로 되어 있다는 것이 발견되는 경우에는, 수신자의 사용자 시스템은 UAck를 반송한다. 수신자의 사용자 시스템이 FMsg 메시지를 수신하지 않거나 UAck를 반송하지 못하는 경우, 중간휴식 기간(timeout period)은 결국 경과된다.

다섯째, 중앙메시징플랫폼은 송신자에게 DNot/FNot를 전송한다. 수신자의 사용자 시스템이 UAck를 반송하는 경우, 중앙메시징플랫폼은 DNot 메시지를 작성하고, 원송신자의 공개키(송신자의 암호화가능 인증서로부터 획득된)를 가지고 그 메시지를 암호화하고, 원송신자에게 DNot을 송신한다. 수신자의 사용자 시스템이 적용가능한 하나의 중간휴식기간의 경과전에 응답하지 않는 경우(2.2.2절에 설명되어 있음), 중앙메시징프랫폼은 FNot 메시지를 작성하고, 원송신자의 공개키를 가지고 그 메시지를 암호화하고, 원송신자에게 FNot를 송신한다.

암호화 알고리즘이 풀리지 않는 경우에도, 이러한 계획(scheme)이 규정하고 있는 기밀성은 한계가 있다. 메시지가 암호화될 때, 그 메시지헤더는 그 목적지에 네트워크를 통하여 메시지의 경로를 지정하기 위하여 완전한 원문(clear text)으로 남아있다. 암호화되지 않은 헤더는 또한 하나의 메일시스템으로부터 다른 메일시스템으로 메시지를 추적하고 그러한 이동의 시기를 로그하는데 필요하다. 또한 암호화되어 송신되는 경우에도, 기밀성은 중앙메시징플랫폼의 운영자로서의 볼레로 인터네셔널이 모든 메시지의 완전한 원문에 대한 접근을 가지고 있다는 점에서 한계가 있다. 운영서비스계약(Operational Service Contract)은 볼레로 인터네셔널에게 특정정보의 기밀유지를 의무로 하고 있다.

볼레로 시스템에서의 암호화와 전자서명은 메시지에 적합하다. 서류는 전통적으로 메시지의 작성으로서 암호화되거나 전자적으로 서명되는 것에 추가하여 암호화되거나 전자적으로 서명되지 않는다. 그 메시지속에 서류를 포함시키기 이전에 서류를 암호화하거나 전자적으로 서명하는 것은 불가능하다. 그러나 저절로 서류를 암호화하거나 서명하는 것(메시지의 일부로서 보다는 오히려)은 볼레로 시스템에 의해서 지원되지 않는다. 볼레로 시스템은 특정 서류상의 전자서명이 아니라 메시지상의 전자서명만을 검증할 것이다. 볼레로 시스템은 메시지를 암호화하지만, 메시지와 별도로 암호화된 서류를 복호화하지 않을 것이다. 만일 서류가 별도로 암호화된다면, 중앙메시징플랫폼은 서류의 명세에 대하여 그것을 확인하게 할 수 없을 것이다. 만일 서류가 특별히 암호화되기 때문에 서류가 확인되도록 요구되지만 될 수 없다면, 중앙메시징플랫폼은 그것에 대해서 BNAk를 반송할 것이다. 왜냐하면 그것은 요구된 서류확인을 실패하기 때문이다.

## Ⅵ. 결론

볼레로넷 서비스는 볼레로 인터네셔널사가 무역거래에 필요한 종이서류를 전자메시지로 전환하여 안전하게 교환할 수 있는 기반을 제공하는 것을 목표로 1999년 9월부터 개시하였다. 볼레로넷 서비스에 이용되는 볼레로

시스템은 볼레로규약집과 그 사용을 적용하는 운영규칙 뿐만 아니라, 메시지와 서류를 통신하고 비즈니스 거래를 촉진하기 위하여 볼레로 인터네셔널이 제공하는 디지털 정보시스템과 비즈니스 과정 및 방법으로서, 그 기술적 구조는 중앙메시징플랫폼, 권리등록기, 사용자 데이터베이스 및 사용자 지원자원, 사용자 시스템 등 5개의 기본적인 요소로 구성되어 있다. 이 중에서 사용자 시스템은 제3자 밴더(third-party vendors) 및 서비스 사무국이 제공하고, 나머지는 볼레로 시스템이 모든 사용자에게 제공하는 서비스이다.

이러한 볼레로의 전자무역시스템을 이용하는 경우에는, 첫째, 일체의 무역업무가 인터넷을 통해서 이루어짐으로써 대금결제가 신속하게 이루어질 수 있으며, 물류업무처리의 대폭적인 간소화와 효율화를 도모할 수 있다. 둘째, 무역관련서류를 규격화된 전자문서 양식으로 모두 인터넷상으로 주고 받기 때문에 비용을 절감하고 시간을 크게 단축할 수 있다. 셋째, 전자적으로 "유통성"이 안전하게 보증되기 때문에 은행의 입장에서는 결제와 무역금융거래에 관련하는 SWIFT 메시지의 전송도 가능하며, 전자상거래에 있어서의 새로운 금융서비스의 제공도 가능하게 될 것이다.

이러한 장점과 더불어 볼레로 시스템을 이용하는 경우에, 사용자의 신원을 확인하기 위하여 RID를 사용하고, 송신자의 메시지가 볼레로 시스템상의 CMP를 통하여 수신자에게 송신되고 수신자가 다시 확인메시지를 CMP를 통하여 원송신자에게 송신함으로써 메시지의 송수신이 이루어진다. 이 경우 메시지의 송수신을 위하여 비밀키로 암호화하고 이에 합치하는 공개키로 복호화함으로써 메시지의 진정성, 무결성 및 기밀성이 보장될 수 있는 것이다.

그러나 암호화 알고리즘이 풀리지 않는다고 하더라도 기밀성은 한계가 있다. 즉, 메시지가 암호화될 때, 그 메시지헤더는 그 목적지에 네트워크를 통하여 메시지의 경로를 지정하기 위하여 완전한 원문(clear text)으로 남아있다. 암호화되지 않은 헤더는 또한 하나의 메일시스템으로부터 다른 메일시스템으로 메시지를 추적하고 그러한 이동의 시기를 로그하는데 필요하다. 또한 암호화되어 송신되는 경우에도, 기밀성은 중앙메시징플랫폼의 운영자로서의 볼레로 인터네셔널이 모든 메시지의 완전한 원문에 대한 접근을 가지고 있다는 점에서 한계가 있다. 이러한 한계를 볼레로 시스템은 운영서비스계약(Operational Service Contract)을 통하여 해결하고자 하는 것이다. 즉, 운영서비스계약에서는 볼레로 인터네셔널에게 특정정보의 기밀유지를 의무로 하고 있는 것이다.

## 참고문헌

안병수, BOLERO프로젝트와 TRADE CARD 시스템; http://210.95.204.2/haksup/조대행/조대행1-8.htm.

안병수, 전자식 선적서류의 실무적용 실험의 결과고찰, 무역상무연구, 1998, 2.

朝岡良平, 電子商去來時代における貿易慣習, 早稻田商學 第376号, 1998.

金融, "bolero.net, 營業開始", 1999.11.

森岡 峰子, 船荷證券のEDI化, 國際商務論の諸問題, 同文館, 1998.

J. Livermore & K. Euarjai, Electronic Bill

of Lading: A Progress Report, Journal of Maritime Law and Commerce vol.28, No.1, January, 1997.

Marinade Ltd., MANDATE - final report for the TEDIS programme, Final version 1.3-04/4/95.

The BOLERO Consortium, BOLERO Final Report for submission to the European Commission, Issue 1.0, September 1955.

Welcome to Digital Signature in the Bolero System; http://www.bolero.net/downloads/digisigs.pdf

http://www.bsbs.co.jp/bolero/main.html

http://www.bsbs.co.jp/press/data/t000125.html

http://www.goshop.co.kr/news/092703.htm

bolero.net, Appendix to Bolero Rule-Book (Operating Procedures), 2nd ed.

bolero.net. Bolero Rulebook.

# A Study on the send and receive of the message in the Bolero System

Soon-Hwan, Jeon*

## Abstract

The purpose of this paper is to study the send and receive of the Message in the Bolero System. Bolero System is the business processes and methods, together with the digital information system, which are provided by Bolero International for communicating Messages and Documents and facilitating business transactions, as well as the Bolero Rulebook and Operating Rules governing their use.

The advantage of bolero.net include speed, cost and efficiency. First, bolero.net moves cirtical information and transactions more quickly than paper can move. Second, a message costs much less to transmit through bolero.net than via couriers and other paper means. Third, because bolero.net logs and tracks all transactions centrally, less data gets lost and fewer data entry errors occur.

Bolero International is the certifier for all certificates used in the Bolero System at present. It takes significant responsibility and liability for the certificates that it issues in each Operational Service Contract. In the future, Bolero International may devolve the task of serving as certifier to one or more other qualified institutions.

* Dept. of International Trade and Commerce, Joongbu University.