RFID 기반 유가증권 보호 기술 동향

Trend of RFID-Based Securities Protection Technology

강유성 (Y.S. Kang) RFID/USN보안연구팀 선임연구원
이석준 (S.J. Lee) RFID/USN보안연구팀 선임연구원
김호원 (H.W. Kim) RFID/USN보안연구팀 팀장

목 차

* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행되었음. [2005-S-088-03, 안전한 RFID/USN을 위한 정보보호 기술]

최근 3~4년 동안 국내외적으로 RFID 기술에 대한 많은 연구와 시범 사업들이 진행되어 왔다. RFID 기술의 응용 중 하나로 RFID 태그를 유가증권에 장착하여 안전하고 신뢰성 있는 유가증권 시스템을 구축하려는 연구가 진행되기도 하였다. 그러나 RFID 기반 유가증권 보호 시스템의 선도적인 개념을 정리한 연구결과는 있었으나 전제 조건이 현재의 기술 수준과 비용 부담을 넘어서기 때문에 실제 적용하기에는 한계가 있다. 본고에서는 RFID 기반 유가증권 보호 시스템의 구성 요소를 중심으로 현재의 기술 개발 동향을 살펴보고, 각 구성 요소의 기술 수준과 보안 요구사항을 고려하여 RFID 기반 유가증권 보호 시스템에 대해 단계적으로 보안 강도를 높여 나갈 수 있는 보안 대책을 제시한다. 본 고의 분석과 제언은 RFID 기반 유가증권 보호 시스템을 상용화하는 데 참조될 수 있을 것이며, 다양한 변형 구조로 발전할 수 있을 것으로 기대된다.

I. 서론

RFID(Radio Frequency Identification) 시스템은 교통, 물류, 출입관리 등 다양한 분야에 적용될 수 있도록 많은 기술 개발이 진행되어 왔다. 국내에서는 수동형 RFID 시스템을 활용하는 시범 사업을 통해 유통물류, 도로교통정보 수집, 문서 관리, 농수산물 이력 관리, 폐기물 관리, 문화재 관리 등의 신규 서비스 제공이 가능함을 입증하기도 하였다.

다양한 RFID 응용 시스템 중 가장 혁신적이며 사용자의 피부에 와닿는 응용 중 하나는 RFID 태그를 유가증권(예를 들면, 수표, 지폐, 어음, 채권, 상품권, 양도성 예금증서 등이 유가증권에 해당함)에 내장시켜 유가증권의 위변조 방지 및 효율적인 관리를 추구하는 RFID 기반 유가증권 보호 시스템이다.

기존의 유가증권 활용 환경에서는 컬러복사기, 스캐너, 디지털 인쇄기 등으로 유가증권을 위조하는 사례가 빈번하게 발생하였다. 예로써, 지난 2004년 K 도시가스의 한 직원이 자사의 기업어음을 컬러복사기로 위조한 후 시중은행에 제시하여 400억 원 가량을 횡령한 사건이 있었고[1], 2005년 문화관광부 국정감사에서는 도안과 특수문자, 홀로그램, 바코드까지 동일하게 사용된 시가 50억 원에 이르는 불법 게임상품권의 유통 움직임이 있었다는 경고도 있었다[2]. 이렇듯, 기존의 유가증권은 악의적인 공격자가 정교하게 위변조할 경우, 일반인뿐만 아니라 은행 담당자들도 속아 넘어갈 정도로 위변조 공격에 취약하다. 이러한 배경 속에서 유가증권의 위변조 취약점을 극복하고 또한 금융업무의 효율화를 위하여 유가증권에 RFID 기술을 적용시키려는 노력이 시작된 것이다.

● 용 어 해 설 ●

유가증권: 재산적 가치를 가지는 사권(私權)을 표시하는 증권

위조: 권한이 없는 자가 진정하게 성립된 유가증권의 외관과 유사 또는 동일하게 유가 증권을 작성하는 행위

변조: 진정하게 성립된 유가증권의 일련번호 및 금액, 날짜 등 기재 내용에 변경을 가하는 행위

유가증권에 RFID 태그를 내장시키는 주요 목적은 돈세탁을 방지하고 유가증권의 불법 유통을 추적하거나 위조 지폐를 탐지해 내기 위함이다. 유가증권에 대한 추적 및 위조 탐지는 유가증권 발행, 유통을 책임지는 기관이 추구하는 목적인 반면 유가증권 사용자들은 프라이버시 보호 측면에서 볼 때, RFID 태그의 사용을 오히려 자신들의 프라이버시에 대한 보안 위협으로 생각할 수도 있다. 즉, 만일 아무나 유가증권에 포함된 RFID 정보를 읽을 수 있다면 많은 유가증권을 소유한 사람은 자신이 가진 전체 유가증권 정보가 노출되어 범죄의 대상이 될 수 있다. 또한 누구라도 RFID 정보를 덮어쓸 수 있다면 공격자의 악의적인 금액 변경이 가능하므로 유가증권 유통 질서가 혼란해질 가능성도 존재한다. 그러므로 RFID 기반 유가증권 보호 시스템은 불법적인 읽기와 쓰기 공격에 대한 방어가 튼튼하도록 설계되어야 한다.

현재는 RFID 기반 유가증권 보호 시스템과 관련하여 일부 연구논문 차원에서 선도적인 개념 정립의 공개자료만 있을 뿐 국제적으로 공인된 표준화된 기술 규격이 없는 상태이다. Financial Cryptography 2003 컨퍼런스에서 발표된 Ari Juels와 Ravikanth Pappu의 논문은 RFID 지폐 보호 시스템과 관련된 대표적인 연구결과이다[3]. Juels-Pappu의 RFID 지폐 보호 시스템에서는 수동형 RFID 태그의 사용을 전제하면서도 현재의 기술 수준과 부담 가능한 비용을 고려하지 않고 유가증권에 내장되는 RFID 태그의 기능을 너무 높게 설정하였다. 따라서 Juels-Pappu 시스템은 실물 경제에 바로 적용하기에는 한계가 있다는 평가를 받고 있다.

본 고에서는 RFID 기반 유가증권 보호 시스템의 구성 요소를 중심으로 현재의 기술 개발 동향을 살펴보고, 각 구성 요소의 기술 수준과 보안 요구사항을 고려하여 RFID 기반 유가증권 보호 시스템에 대해 단계적으로 보안 강도를 높여 나갈 수 있는 보안 대책을 제시한다. 이를 위하여 본 고는 다음과 같은 구성을 가진다. 제 II장에서 Juels-Pappu 시스템을 참조하여 RFID 기반 유가증권 보호 시스템의 구성

요소의 기능에 대하여 설명하고, 각 구성 요소별로 보안 요구사항을 분석한다. 그리고 제 Ⅲ장에서 기술 발전 수준과 연동하여 진화할 수 있는 단계별 보안 대책을 제시한다. 끝으로, 제 Ⅳ장에서 본 고의 분석과 제언이 RFID 기반 유가증권 보호 시스템을 상용화하는 데 도움이 되기를 기대하는 희망을 피력하며 본 고의 결론을 맺는다.

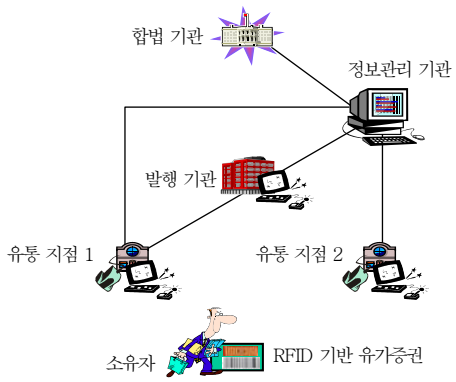
Ⅱ. RFID 기반 유가증권 보호 시스템 개요

RFID 기반 유가증권 보호 시스템이 불법적인 돈세탁 방지, 불법적인 유통의 추적, 위변조 유가증권 탐지와 같은 기본적인 요구사항을 만족시키기 위해서는 다음과 같은 5개의 구성 요소로 이루어져야 한다[4].

- 발행 기관: 발행 기관은 RFID 기반 유가증권을 발행하는 기관으로서, 유가증권에 일련번호를 부여하고 유가증권 관련 정보를 정보관리 기관에 전달하는 역할을 한다. 발행 기관은 실질적으로 RFID 기반 유가증권의 신뢰성 있는 유통을 책임져야 하는 기관이기 때문에 관심을 가지는 주된 보안 관련 사항은 위변조 유가증권 방지 및 탐지이다.
- 합법 기관: 합법 기관은 RFID 기반 유가증권에 대해 합법적으로 유통 흐름을 파악할 수 있는 권한을 부여받은 기관으로서 오직 자신만이 RFID 기반 유가증권의 유통 흐름을 추적할 수 있는 특권을 가지기를 희망하는 기관이다. 따라서 합법 기관이 아닌 다른 기관들은 RFID 기반 유가증권의 유통 정보를 얻을 수 없어야 한다.
- 정보관리 기관: 정보관리 기관은 데이터베이스 서버의 구축, 관리, 유지, 보수를 책임지는 기관이다. 합법 기관 또는 유통 지점으로부터 유가증권의 유통 흐름 확인이나 위변조 탐지를 요청 받아 자신의 데이터베이스에 기초하여 그 결과를 알려주는 역할을 한다.
- 유통 지점: 유통 지점은 RFID 기반 유가증권이 사용되는 곳으로서, 유가증권을 받고 그 정당성을 확인하는 것이 가장 큰 역할이다. 또한 RFID 기반 유가증권에 포함된 정보가 비정상적인 경우에 이를 보고하는 역할도 수행해야 한다.
- 소유자: 소유자는 RFID 기반 유가증권을 지니고 있는 사용자이다. 보안과 관련된 소유자의 주요 관심은 자신의 프라이버시 보호, 그리고 불법적인 추적의 방지이다.

(그림 1)은 위의 5개 구성 요소가 연계된 RFID 기반 유가증권 보호 시스템의 구성도를 보인 그림이다. 현재 가장 현실적인 대안으로 주목 받는 RFID 기반 유가증권 보호 시스템에서는 RFID 기반 유가증권이 바코드와 RFID 태그를 동시에 포함하고 있는 것을 전제로 하고 있다.

(그림 2)는 RFID 기반 유가증권을 보인 그림이다. RFID 태그와 바코드를 동시에 내장한 유가증권



(그림 1) RFID 기반 유가증권 보호 시스템 구성도

(그림 2) RFID 기반 유가증권

보호 시스템의 궁극적인 목적인 합법 기관의 유통 흐름 확인과 유통 지점의 위변조 유가증권 식별, 그리고 유가증권의 발행 절차를 설명하면 다음과 같다.

유가증권 보호 시스템의 활용 시나리오상 가장 먼저 고려할 것은 유가증권의 발행 절차이다. 먼저 발행 기관은 RFID 태그의 사용자 메모리 영역에 유가증권의 일련번호, 금액과 같은 정보를 기록하고, 동일한 정보를 정보관리 기관의 데이터베이스에 저장한다. 그리고 발행 기관은 RFID 태그의 사용자 메모리 영역에 기록한 정보를 적절히 조작하여(예를 들면 위의 정보에 대한 전자서명 계산) 생성된 값을 바코드화하여 유가증권에 인쇄한다. RFID 태그의 연산 능력과 저장 능력에 따라 정보 기록시 암호화 기법을 사용할 수도 있으며 보다 많은 양의 부가정보를 기록할 수도 있다. 그리고 바코드에 기록된 값은 접촉식 바코드 스캐너로만 읽을 수 있으므로 유가증권 소유자 몰래 바코드 정보가 노출될 수 없다고 가정하여 바코드 정보를 RFID 태그의 사용자 메모리 영역에 접근할 수 있는 패스워드로 사용할 수 있다. 즉, 유가증권에 바코드 인쇄를 포함시키는 가장 큰 이유는 RFID 태그의 사용자 메모리 영역에 기록되는 정보를 보호하는 패스워드를 손쉽게 관리하기 위함이다.

합법적인 유통 흐름을 확인하고자 하는 합법 기관은 유가증권 소유자도 모르게 유가증권의 일련번호, 금액 등의 정보, 위변조 여부 또는 유통 과정 등을 파악할 수 있는 법적인 근거를 가진 기관이다. 따라서 합법 기관은 유가증권의 바코드에 대한 스캐닝 없이 단지 RF 신호로 노출되는 정보만 가지고 해당 유가증권에 관한 주요 정보를 알아낼 수 있어야 하며, 합법 기관을 제외한 다른 모든 리더들은 RF 신호만을 가지고 유가증권의 정보를 얻을 수 없어야 한다. 유가증권이 RFID 태그의 사용자 메모리 영역에 직접 보유하고 있는 정보 외에 정보관리 서버가 관리하는 정보를 요청할 수도 있으며 정보관리 서버는 오직 합법 기관이 요구하는 경우에만 해당 정보를 알려 주어야 한다. 즉, 합법 기관이 시중에 유통되는 유가증권 중 특정 지역 또는 특정인의 유가증권을 확인하고자 할 때, 소유자 모르게 원격에서 RFID 정보를 읽고, 이 정보와 정보관리 서버의 회신에 근거하여 위변조 여부 및 유통 과정을 확인할 수 있다. 이러한 경우에 시스템 구축시 고려해야 할 점은 RF 신호로 모두에게 전달되는 정보는 반드시 합법 기관만 해석할 수 있어야 된다는 것이다. 해결 방법으로는 합법 기관의 공개키로 암호화한 데이터를 RFID 태그의 사용자 메모리 영역에 기록해 놓는 방법도 있고, 합법 기관이 해당 RFID 태그에 접근할 수 있는 패스워드를 미리 확보하고 있는 방법도 있을 수 있으며, 보다 높은 보안성이 요구된다면 RFID 태그에서 사용자 메모리 영역에 있는 정보 자체를 암호화하여 통신하는 방법도 있을 수 있다.

유통 지점에서는 유가증권의 위변조 탐지와 정보의 무결성을 확인해야 한다. 일반적인 RFID 기반 유가증권 보호 시스템에서는 유통 지점이 바코드 스캐너와 RFID 리더를 동시에 구비하고 있음을 전제로 한다. 따라서 RFID 기반 유가증권을 받은 유통 지점은 바코드 스캐너로 바코드 정보를 읽고, 그 바코드 정보를 패스워드로 사용하여 RFID 태그의 사용자 메모리 영역에 있는 정보를 획득할 수 있다. 이러한 경우에 바코드 정보와 RFID 태그의 사용자 메모리 영역 정보의 상관 관계(예를 들면 바코드 정보가 RFID 정보의 전자서명이라면 이에 대한 검증을 수행하여 그 결과를 파악)를 이용하여 유가증권의 위변조 여부를 확인할 수도 있고, 또한 유통 지점이 RFID 정보를 정보관리 서버에게 전달하여 해당 유가증권의 위변조 여부를 문의할 수도 있다.

위에서 설명한 내용은 일반적인 RFID 기반 유가증권 보호 시스템이 동작하는 방식을 비교적 간단하게 요약한 것이다. Juels-Pappu 구조의 보다 자세한 분석은 참고문헌 [3]을 참조할 수 있고, Juels-Pappu 구조의 한계를 극복하고 효과적인 복제 지폐 탐지와 합법적 유통 흐름 확인을 지원하는 향상된 시스템에 대한 이해는 참고문헌 [4]를 참조하면 된다.

비록 다양한 방법과 동작 절차의 정의를 통해 유가증권의 위변조 식별과 합법적 유통 흐름 추적이 가능하긴 하지만 현재의 RFID 태그 기술과 비용, 그

리고 유가증권에 내장되는 형태라는 점을 고려하여 구현 가능성을 염두에 두고 현실적으로 시스템을 구상하는 것이 필요하다. 예를 들면, 유가증권의 일련번호, 금액 등의 정보를 RFID 태그에 안전하게 기록하고 읽기 위해서는 RFID 태그가 충분한 크기의 저장 공간이 있어야 하고 패스워드를 사용한 읽기/쓰기 접근 제어 기능을 제공해야 한다. 만일 RFID 태그에서 데이터 암복호 연산을 수행할 수 있다면 별도의 암호 프로토콜을 적용하여 보안성이 향상된 시스템을 구축할 수도 있다. 그러나 ISO/IEC 18000-6의 C 타입 수동형 RFID 태그[5]를 사용하는 RFID 기반 유가증권 보호 시스템에서는 데이터 암복호 연산 능력이 없어서 직접적인 암호 알고리듬의 사용이 불가능하다.

따라서 본 고에서는 보다 현실적인 접근 방안을 제공하고자 (그림 1)의 구성 요소 각각이 요구하는 보안 요구사항을 분석한 후, RFID 기반 유가증권이 구현될 수 있는 다양한 형태(예를 들면, 읽기만 가능한 RFID 태그를 장착한 형태, 읽기/쓰기가 가능한 RFID 태그를 장착한 형태, 읽기/쓰기 접근제어와 암호 연산이 가능한 RFID 태그를 장착한 형태 등)를 고려하여 단계적으로 보안 강도를 높여 나갈 수 있는 보안 대책을 제시하며, 각 단계에서 보안 요구사항을 어느 정도 충족시키는지 분석한다.

<표 1>은 RFID 기반 유가증권 보호 시스템의 구성 요소, 즉 발행 기관, 합법 기관, 정보관리 기관, 유통 지점 및 소유자의 보안 요구사항을 정리한 표이다.

Ⅲ. RFID 기반 유가증권 보호 시스템 단계별 보안 대책

안전한 유가증권 보호 시스템은 <표 1>의 보안 요구사항을 모두 만족하는 시스템으로 구현되는 것이 최종 목표지만 유가증권에 내장되는 RFID 태그 비용 및 기술 규격 발전을 고려하면 활용 환경에 따라 단계적인 해결 방안을 적용하는 것이 비용 대비 효과를 높이는 방법이 될 것이다. 본 고에서는 비용 부담 및 개발 어려움이 가장 큰 RFID 태그의 기능에 따라 단계적인 접근 방안을 제시한다.

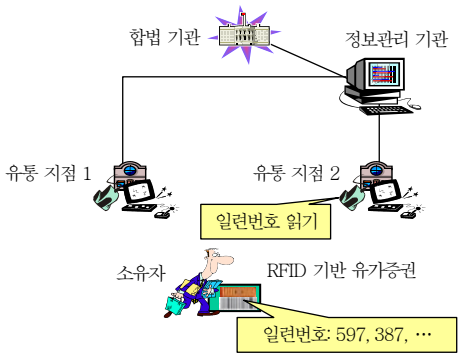
〈표 1〉 구성 요소별 보안 요구사항

1. 발행 기관	ⓐ 유가증권 위변조를 방지하고 싶다. ⓑ 위변조 유가증권을 식별하고 싶다. ⓒ 유가증권의 최종 종착지로서, 유가증권 폐기 직전에 유가증권의 유통 흐름을 확인하고 싶다.
2. 합법 기관	ⓓ 소유자 모르게 유가증권 정보를 알고 싶다. ⓔ 유가증권의 유통 흐름을 확인하고 싶다. ⓕ 소유자 모르게 유가증권 정보 및 유통 흐름을 확인하는 기능은 오직 합법 기관만 특권적으로 가지고 싶다.
3. 정보관리 기관	ⓖ 데이터베이스의 정보를 요청하는 기관이 믿을만한 기관인지 알고 싶다. ⓗ 정보 요청 기관과 안전한 통신을 하고 싶다. ⓘ 데이터베이스는 항상 정확한 최신 정보를 유지하고 싶다.
4. 유통 지점	ⓙ 위변조 유가증권을 식별하고 싶다. ⓚ 위변조 유가증권 발견시 정보관리 기관에게 알리고 싶다.
5. 소유자	ⓛ 합법 기관 이외에는 자신이 모르는 상황에서 유가증권 정보가 노출되는 것을 막고 싶다. ⓜ 유가증권을 소유하고 있다는 것이 노출되는 것을 막고 싶다. ⓝ 위변조 유가증권을 식별하고 싶다. ⓞ 위변조 유가증권 발견시 정보관리 기관에게 알리고 싶다.

1. 제 1단계 – 읽기 전용 태그

제 1단계 해결 방안은 유가증권에 읽기 전용 RFID 태그를 장착하는 방안이며, (그림 3)은 제 1단계 환경을 나타낸 그림이다. RFID 태그에는 유가증권을 식별할 수 있는 일련번호가 저장되어 있으며, 이는 변경되지 않는 고정값이다. 그리고 제 1단계 환경은 일련번호에 대한 접근 제어 기능이 없기 때문에 모든 리더의 요청에 일련번호를 응답한다.

제 1단계 환경의 가장 큰 장점은 현재 상용화되어 있는 RFID 태그를 사용하여 비교적 저렴한 비용으로 유가증권의 제작이 가능하다는 점이다. 히타치의 뮤칩[6] 또는 EPCglobal의 Gen2 통신 규격[7]을 준수한 임핀지, 필립스, TI의 칩들이 대표적인 사용 가능 칩들이다. 실제 EPCglobal Gen2 규격은 사용자 메모리 영역을 별도로 정의하고 있어서 읽기/



(그림 3) 제 1단계: 읽기 전용 태그 환경

쓰기가 가능하도록 규정하고 있지만, 상용화된 많은 Gen2 태그들은 저가 구현을 위하여 단지 식별자 정보만을 응답하는 단순한 구조를 가지고 있으며, 제 1단계 환경에서는 이러한 Gen2 태그의 활용을 전제로 하고 있다. 따라서 제 1단계 해결 방안은 컬러 복사기, 스캐너, 디지털 인쇄기 등에 의한 위변조를 방지할 수 있으며, 신속한 계수 및 식별자 획득의 장점이 있다.

그러나 (그림 1)에서 보듯이 소유자가 지닌 RFID 기반 유가증권은 모든 리더들에게 자신의 식별자를 응답하기 때문에 오히려 공격자들에게 소유자가 유가증권을 가지고 있다는 사실을 노출시키는 프라이버시 침해의 빌미가 되는 단점이 있다.

단계별 보안 대책의 보안 요구사항 만족 여부를 <표 2>로 비교 정리하였다. <표 2>의 제 1열에 있는 항목들은 <표 1>의 보안 요구사항을 의미한다. 제 1단계 환경의 경우, 기존의 컬러 복사기, 스캐너, 디지털 인쇄기 등의 위변조는 방지할 수 있지만 일련번호가 공격자에게 손쉽게 노출되기 때문에 일련번호에 대한 위조는 막을 수 없으며, 위조된 유가증권이 유통되는 경우 쉽게 식별할 수 있는 방법이 없다. 그리고 위조된 유가증권의 유통은 정보관리 기관의 데이터베이스를 혼란시킬 가능성이 있다. 따라서 <표 2>의 제 1단계 요약은 위와 같은 분석에 기반하여 작성된 것이며, 주로 △로 표기된 항목은 기존의 컬러 복사기에 의한 공격은 방지하되, 동일한 RFID 태그를 내장한 위변조 유가증권은 방지하기 어렵다는 의미를 담고 있다.

〈표 2〉 단계별 보안 대책의 비교

항목*	제 1단계	제 2단계	제 3단계
1.ⓐ	△	○	○
1.ⓑ	△	○	○
1.ⓒ	○	○	○
2.ⓓ	○	△	○
2.ⓔ	○	△	○
2.ⓕ	×	△	○
3.ⓖ	○	○	○
3.ⓗ	○	○	○
3.ⓘ	×	○	○
4.ⓙ	△	○	○
4.ⓚ	○	○	○
5.ⓛ	×	○	○
5.ⓜ	×	△	○
5.ⓝ	△	○	○
5.ⓞ	○	○	○
특징	읽기 전용 태그	읽기/쓰기 태그 바코드 병행	암호 연산 태그 바코드 병행

○: 지원 가능, △: 일정 조건 하에서 지원 가능, ×: 지원 불가
*항목은 <표 1> 참조

2. 제 2단계 – 읽기/쓰기 태그

제 2단계 해결 방안은 유가증권에 읽기/쓰기가 가능한 RFID 태그의 내장과 바코드 인쇄가 병행되는 방안이며, (그림 4)와 같은 환경으로 이루어진다. RFID 태그의 사용자 메모리 영역에는 유가증권 일련번호, 금액과 같은 정보와 어느 유통 지점에서 읽혔는지, 몇번째 유통인지와 같은 유통 흐름 정보가 기록되며, 위의 정보들은 정보관리 기관에서도 동일하게 유지한다. 그리고 제 2단계 환경에서는 RFID 태그의 쓰기 동작은 패스워드에 의한 접근 제어를 하지만 읽기 동작은 별도의 접근 제어가 없다. 즉, 제 2단계 보안 대책은 ISO/IEC 18000-6 C 타입 규격의 읽기/쓰기 규칙을 준수하면서 비교적 저용량 메모리를 사용하는 환경을 전제로 한다.

제 2단계 환경의 가장 큰 장점은 국제 표준을 준용하는 RFID 태그를 사용하여 사용자 프라이버시가 강화된 유가증권 보호 시스템을 구축할 수 있다는 것이다. 제 2단계 해결 방안은 제 1단계 해결 방안에 비해 비용 증가가 예상되지만 점차 RFID 태그 기술의 발전과 더불어 현실적인 대안이 될 수 있을 것으로 판단된다.

제 2단계 해결 방안에서는 RFID 태그 읽기 동작에 대한 별도의 접근 제어가 없기 때문에 소유자 프라이버시 보호를 위해서는 RFID 태그의 사용자 메모리 영역에 기록하는 정보를 평문으로 저장해서는 안된다. 즉, 저장시 패스워드를 이용하여 암호화시킨 후에 암호문을 저장시켜 놓아야 하며, 패스워드를 가진 리더에서만 그 암호문을 해독할 수 있어야 한다. 이러한 경우에 현실적으로 가장 큰 문제는 모든 리더들이 유가증권마다 해당 패스워드를 알아내야 하는 패스워드 관리 문제이다. 이러한 패스워드 관리 문제를 간단하게 해결한 것이 바코드 인쇄이다. 즉, 바코드에 패스워드를 기록해 놓는 것으로서 소유자가 유가증권을 제출했거나 또는 소유자가 지켜보는 가운데 바코드 스캐너를 통해 쉽게 패스워드를 얻을 수 있는 장점이 있다. 이렇게 확보한 패스워드를 이용하여 RFID 태그 정보를 암복호화 하고, 쓰기 동작의 접근 권한을 얻을 수 있다.

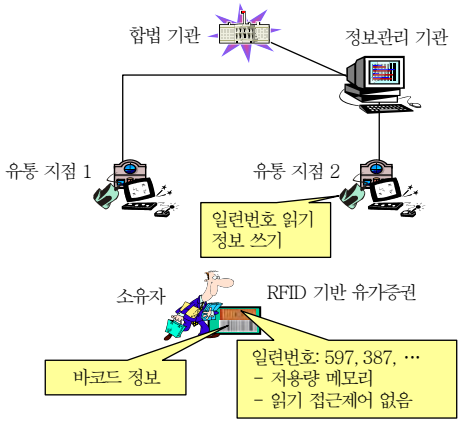
<표 2>의 제 2단계 보안 대책의 요약을 보면, 제 1단계에 비해 소유자 프라이버시 보호가 향상된 것을 확인할 수 있다. 이는 패스워드를 가진 리더만이 RFID 태그 정보를 해독할 수 있기 때문이다. 합법 기관의 보안 요구사항 해결은 주로 △로 판단할 수 있다. 즉 합법 기관이 소유자 모르게 RFID 태그 정보를 알기 위해서는 바코드 스캐닝 없이 패스워드를 얻어야 하는데, 별도의 패스워드 관리 방법에 의해서 합법 기관이 모든 유가증권의 패스워드를 확보할 수 있다면 보안 요구사항을 만족할 수 있지만 현실적으로는 거의 불가능하다는 것을 의미한다.

3. 제 3단계 – 암호 연산 태그

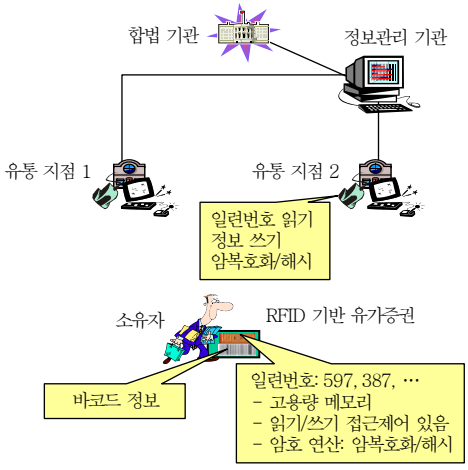
제 3단계 해결 방안은 유가증권에 암호 연산이 가능한 고성능의 RFID 태그와 바코드 인쇄를 병행하는 방안으로써 (그림 5)와 같은 환경으로 구성된다. 제 3단계 환경은 RFID 태그가 충분한 메모리 공간과 자체적인 암호 연산 능력을 가지고 있어서 유가증권 일련번호와 같은 중요 정보뿐만 아니라 태그 식별자도 허가받은 리더에게만 공개되어 유가증권의 소유 자체도 노출시키지 않는 환경이다.

제 3단계 환경의 가장 큰 장점은 RFID 태그의 암호 연산을 통해 보안 통신이 강화됨으로써 <표 1>에서 분석한 보안 요구사항을 모두 만족시키는 안전한 시스템을 구축할 수 있다는 점이다. 그러나 수동형 RFID 태그에서 충분한 메모리를 보유하고, 메모리 읽기/쓰기에 대하여 패스워드를 이용한 접근 제어를 수행하며 또한 데이터 보호를 위한 대칭키 암복호, 해시 연산 등을 수행하는 것은 비용 측면이나 기술 수준 측면에서 현재로서는 매우 구현하기 어려운 전제 조건이다.

<표 2>의 제 3단계 보안 대책의 요약을 보면, 제 2단계에서 해결하지 못한 합법 기관의 보안 요구사항을 모두 만족시키는 것을 볼 수 있는데, 이는 충분



(그림 4) 제 2단계: 읽기/쓰기 태그 환경



(그림 5) 제 3단계: 암호 연산 태그 환경

한 메모리 공간에 합법 기관의 공개키로 암호화한 공개키 암호문을 저장시켜서 합법 기관만이 자신의 비밀키로 암호문을 해독할 수 있도록 했기 때문이다. 또한 경우에 따라서는 RFID 태그에서 직접 공개키 암호화 연산을 수행하여 전달해도 된다.

4. 단계별 보안 대책의 비교

<표 2>를 요약하면 다음과 같다. 제 1단계 보안 대책은 비교적 저가 구현이 가능하지만 소유자 프라이버시 침해에 취약하고, 제 2단계 보안 대책은 제 1단계에 비해 비용 증가는 있지만 국제 표준을 따르는 현실적인 구현이 가능하면서 소유자의 프라이버시 보호 기능이 강화된 해결 방안이다. 그리고 제 3단계 보안 대책은 최종 목표 시스템을 지향하고 있지만 현재의 기술 수준과 비용 측면에서 단기간 내에 적용하기에는 어려운 시스템이다.

Ⅳ. 결론

유가증권의 사용은 일상생활에서 매우 빈번하게 발생하는 금융활동이다. 유가증권 시스템에 RFID 기술을 적용하여 보안성 강화와 효율성 증대를 추구하는 것은 IT와 금융간의 융합 서비스 제공과 관련되어 있다. 본 고에서는 RFID 태그를 유가증권 시스템에 적용할 때 요구되는 보안 요구사항을 분석하고, RFID 태그의 기술 개발 수준을 고려하여 3단계의 접근 방안을 제시하였다.

유가증권에 내장될 RFID 태그의 기술적 수준에 따라 3단계 접근 방법을 제시하였는데, 제 1단계 시스템은 읽기 전용 태그, 제 2단계 시스템은 읽기/쓰기가 가능한 저용량 메모리를 가지며 바코드 정보를 패스워드로 사용하는 태그, 그리고 제 3단계 시스템은 읽기/쓰기가 가능한 고용량 메모리를 가지며 바코드 정보를 패스워드로 사용하고 암호 연산이 가능한 태그를 사용하도록 구성하였다. 본 고에서는 RFID 기반 유가증권 보호 시스템의 기본 구성 요소를 발행 기관, 합법 기관, 정보관리 기관, 유통 지점 및 소유자로 구성하였고, RFID 태그 기능에 영향을 받는 소유자와 유통 지점을 제외한 나머지 구성 요소는 동일한 기능을 제공한다고 가정하였다.

본 고에서는 구성 요소의 보안 요구사항을 만족하는 기능을 중심으로 <표 2>의 최종 분석이 정리되었다. 분석 결과, 제 1단계 보안 대책은 소유자 프라이버시 침해에 취약하므로 적용하기에는 적절치 않으며, 제 2단계 보안 대책이 국제 표준을 준수하면서 소유자 프라이버시 보호가 가능하므로 현실적 대안이 될 수 있을 것으로 분석되었다. 제 3단계 보안 대책은 RFID 태그 기술 수준 및 비용을 고려할 때 현재적 대안이 되기는 힘들 것으로 판단되었다. 본 고의 제언 및 분석과 더불어 향후 구체적인 성능과 비용에 대한 분석이 추가된다면 RFID 기반 유가증권 보호 시스템을 상용화하는 데 밑거름이 될 수 있을 것으로 기대한다.

참 고 문 헌

[1] 중앙일보, http://thinkpool.joins.com/concert/joins/i/newsRead.jsp?name=news&page=1&key=&code=015360&number=368149&num=137160

[2] 아이뉴스24, http://www.inews24.com/php/news_view.php?g_serial=173581&g_menu=020500

[3] Ari Juels and Rabikanth Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes," *In Proc. of Financial Cryptography - FC'03*, Jan. 2003, pp.103-121.

[4] YouSung Kang, Haedong Lee, Howon Kim, and Kyoil Chung, "Privileged Tracking and Clone Detection for RFID-Enabled Banknotes," *Industrial Track Proc. of ACNS 2006*, June 2006, pp.28-40.

[5] ISO/IEC 18000-6, Information Technology - Radio Frequency Identification(RFID) for Item Management - Part 6: Parameters for air interface communications at 860MHz to 960MHz, ISO/IEC JTC1 SC31 WG4 SG3, Aug. 2004.

[6] Hitachi, The Mu Chip, http://www.hitachieu.com/mu/Products/Mu%20Chip.htm

[7] EPCglobal, "EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz - 960MHz Version 1.0.9," Jan. 2005.