모바일 전자ID지갑 운용을 위한 NFC 기술 분석1)

전재우*, 임선희*, 윤승환*, 이옥연**, 진승헌***, 김수형***
*고려대학교 정보경영공학전문대학원
**국민대학교 자연과학대학 수학과
***한국전자통신연구원
e-mail:jjwkma61@korea.ac.kr

An analysis of NFC technology for Operating Mobile Digital ID Purse

Jae-Woo Jeon*, Sun-Hee Lim*, Seunghwan Yun*, Okyeon Yi**, Seung-Hun Jin***, Soo-Hyung Kim***
*Graduate School of Information Management, Korea University
**Department of Mathematics, Kookmin University
***Electronics and Telecommunications Research Institute

요 약

웹 기반의 전자ID지갑을 모바일 환경에서 활용하게 되면 오프라인에서 각종 인증 및 지불 등이 모바일 전자ID지갑을 통해 가능하게 된다. 모바일 전자ID지갑이 오프라인에서 활용되려면 근거리 무선망을 통한 통신이 이루어져야 하는데, 이를 위해서는 각 사업자별로 동일한 방식으로 무선 통신이 이루어져야 모바일 전자ID지갑의 상호운용성을 보장할 수 있다. 이러한 근거리 무선통신 기술로 NFC(Near Field Communication)가 세계 표준으로 지정되어 기술 개발이 이루어지고 있다. 본 논문에서는 전자ID지갑의 역할을 오프라인으로 확대시킬 수 있는 NFC 기술과 이와 관련된 보안 알고리즘, NFC와 USIM 인터페이스에 대해 연구한다.

1. 서론

전자ID지갑은 오프라인에서 지불을 위해 신용카드를 사용하고 신원확인을 위해 사용/관리하는 시스템이고, 온라인 전자ID의 역할을 실제 오프라인으로 연계하여 확대시킨 것이 모바일 전자ID지갑이다.

이러한 모바일 전자ID지갑을 오프라인에서 활용하기 위해서는 모바일 전자ID지갑과 서비스 제공자간 표준화되고 안전한 근거리 무선 통신 기술이 필요한데, 현재 세계적으로 표준화되고 있는 근거리 무선 통신 기술이 NFC(Near Field Communication)이다. 또한 모바일 전자ID지갑의 정보를 안전하게 저장하기 위한 적절한 저장매체로서 차세대 USIM이 연구 진행 중에 있다[1]. 차세대 USIM에서도 NFC 통신을 위한 표준이 제정되어 있다.

본 논문에서는 모바일 전자ID 지갑 서비스 기능을 지원하기 위한 NFC 기술과 NFC와 통신하기 위한 UICC 인터페이스를 분석하고, 이러한 기술들이 갖는 장점과 발전 방향을 제시한다.

2. NFC 통신 프로토콜 개요[2][3]

NFC(Near Field Communication, 근거리 무선 통신)는 13.56MHz의 주파수를 사용하여 10cm 이내의 근거리 통신을 가능하게 하는 기술로서, 인식속도가 빠르고(0.1초 이내) 106Kbps424Kbps로 통신이 가능하다.

3. NFC 관련 차세대 USIM 인터페이스

전자ID지갑의 정보는 민감한 정보이므로 보안에 안전한 USIM에 저장하여 활용하는 방안이 연구되고 있다. 실제로 GSMA NFC 프로젝트에서도 UICC를 가장 적절한 보안 요소(secure element)로 추천하고 있다[1].

3.1 차세대 UICC 인터페이스 규격

UICC는 총 8개의 접점을 통해 칩 외부와 물리적, 전기적으로 연결된다. 이 중 단말과의 통신이 이루어지는 접점은 C7 접점이며, C7 접점의 느린 통신 속도를 보완하기 위해 C4, C8번 접점이 UICC의 USB통신 용도로 할당되었다. 그리고 C6 접점은 UICC와 단말 사이의 인터페이스가 아닌 UICC가 외부 인터페이스와의 통신하기 위한 용도로 할당되었으며, 나머지 접점들은 전기 공급 및 UICC 제어 용도로 할당되었다[4][5].

3.2 UICC와 NFC 전용 칩 간의 통신

USIM과 NFC 리더기 사이에 NFC 통신이 이루어지려면 중간에 USIM이 외부와의 통신을 할 수 있어야 하는

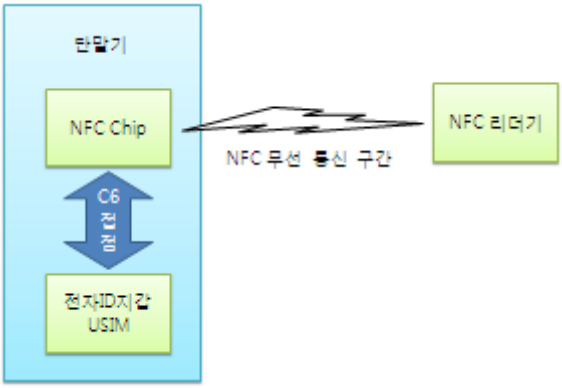
1) 본 연구는 지식경제부 및 한국산업기술진흥원의 국제공동기술개발사업의 일환으로 수행하였음.[2007-S-601-03, 자기통제 강화형 전자ID지갑 시스템 개발]

데, 이것은 외부와의 통신 용도로 할당된 C6 접점을 통해 이루어진다.

여기서 C6 접점이 통신을 하기 위해서는 C6 접점이 물리적으로 외부 인터페이스와 연결되어야 하는데, 이 때 C6 접점과 NFC 리더기 사이엔 무선 구간이므로 중간에 이를 중계할 수 있는 장치가 필요하다. 이를 위해 중간에 NFC 전용 칩이 필요하며, 이 칩은 단말 내부에 위치하여 UICC와 NFC 리더기 사이에 송/수신되는 데이터를 중계하는 역할을 하게 된다. 이 때 USIM과 NFC 전용 칩 사이의 프로토콜은 SWP(Single Wire Protocol)가 사용된다 [5][6].

4. 모바일 전자ID 지갑에서 NFC를 활용한 시나리오

NFC는 모바일 전자ID 지갑의 활용 범위를 온라인에서 오프라인으로 확장하는 역할을 한다. 각 구성 요소별 통신 방향은 아래와 같다



(그림 2) NFC를 통한 모바일 전자ID지갑 통신 구조

모바일 전자ID지갑의 발급은 오프라인이나 이동통신망의 OTA(Over-The-Air)를 통해 이루어지고, NFC는 USIM에 모바일 전자ID 지갑이 발급된 후에 이용된다.

사용자의 모바일 전자ID 지갑의 정보는 USIM에 있으며, NFC 리더기는 모바일 전자ID 지갑의 정보를 받는 쪽에 있다. USIM과 NFC 리더기 사이에는 NFC 칩이 위치한다. 모바일 전자ID 지갑의 정보가 NFC 리더기에 전달될 때에는 USIM의 C6 접점을 이용해 모바일 전자ID 지갑의 정보가 NFC 칩에 전달되며, NFC 칩은 USIM으로부터 받은 정보를 NFC 통신을 통해 NFC 리더기로 전달한다. 반대로 NFC 리더기가 사용자에게 정보를 전달하고자 할 때에는 NFC 리더기로부터 서비스 제공자의 정보가 NFC 통신을 통해 사용자 단말의 NFC 칩에 전달되고, NFC 리더기로부터 정보를 전달받은 NFC 칩은 전달받은 정보를 C6 접점을 통해 USIM에 전달하게 된다.

이러한 방식으로 모바일 전자ID 지갑과 서비스 제공자 사이에는 양방향 통신이 가능하며, 이러한 특성을 이용하여 다양한 서비스 모델을 생각해 볼 수 있다. 예를 들어 모바일 결제시 사용자의 멤버십 정보를 함께 전달하면 이러한 정보를 전달받은 서비스 제공자는 사용자에게 추가 할인이나 적립 쿠폰 등을 제공하는 서비스가 가능하다. 또한 시간 정보가 함께 전달될 경우 USIM에 사용자의 구매 기록 등을 USIM에 저장할 수 있으며, 이러한 정보는 사용자 동의하에 서비스 제공자가 사용자에게 맞춤식 서비스 제공을 할 수 있는 기초 자료가 될 수 있다.

5. 결론

모바일 전자ID지갑을 USIM에 보관하고 이것을 오프라인에서 NFC를 통한 서비스가 제공된다면 USIM의 안전성으로 모바일 전자ID지갑의 안전성을 보장함과 동시에 사용의 편리성도 증대될 것이다. 특히 NFC 기반의 서비스를 구축하면 기반체계가 표준화되어있기 때문에 모바일 전자ID지갑 서비스와 더불어 이를 이용한 다른 오프라인 서비스도 추가 비용 없이 제공할 수 있어 사업자들의 기반 구축비용도 크게 절감할 수 있다.

이러한 모바일 전자ID지갑을 효과적으로 구현하고 활용하기 위한 NFC와 관련 기술들의 표준화가 대부분 완료되었지만, 아직까지 NFC를 지원하는 단말기가 많지 않고, NFC 통신이 가능한 UICC가 개발 중이다[7]. 또한 모바일 전자ID지갑에 관련된 기술들이 표준화되어 상호운용성을 확보하는 것이 필수적이다.

참고문헌

[1] GSMA, “Mobile NFC Technical Guidelines - version 2.0”, pp. 15, Nov. 2007.

[2] NFC Forum, "Type 1~4 Tag Operation Specification", Jul. 2007.

[3] ECMA, "Near Field Communication Interface and Protocol(NFCIP-1)", Dec. 2004.

[4] ETSI TS 102 221 "Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 8)", Aug. 2009.

[5] 나준채, “차세대 USIM 기술”, TTA Journal No.116-표준기술동향, pp. 82, Apr. 2008.

[6] ETSI TS 102 613 "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 7)", Jun. 2009.

[7] Toshiba, "Toshiba Develops USIM Card Compatible with NFC Mobile Phones", http://www.toshiba.co.jp/about/press/2009_02/pr0901.htm, Feb. 2009.