한국지능정보시스템학회논문지 제12권 제3호 2006년 9월(pp.1~13)

연결완전성 제고와 프라이버시 보호를 위한 유비쿼터스 지불 프로세스의 설계*

이경전
경희대학교 경영학부
(klee@khu.ac.kr)

정무정
경희대학교 경영학부
(mjinlove@khu.ac.kr)

본 연구는 U-Commerce의 주요 특성이자 이슈인 Seamlessness(연결완전성)와 프라이버시가 강화된 U-Payment 메쏘드를 제안한다. 유비쿼터스 환경에서 나타나는 중요한 사용자 결제환경의 특성은, 사용자의 결제정보 생성 및 변환, 전송 등이 Seamless하게 이루어지는 것과 사용자의 결제 디바이스 기능 및 정보처리능력, 저장능력 등이 매우 강해진다는 점이다. U-Payment 환경에서 예상되는 이러한 특성은 이전의 결제방식과는 다른, 새로운 결제방식을 가능하게 할 것으로 예상되는데, 본 논문은 RFID와 사용자 단말의 강화, 금융기관 계정의 결합을 통해 사용자의 Seamless한 가치를 창출하고, 동시에 프라이버시 보호의 개선이 가능한 U-SDT(Secure Direct Transaction) 프로토콜을 시나리오와 시스템 아키텍처를 통해 설명한다. 또한 이에 수반되는 바람직한 특징으로 결제정보소유의 분리적 구조를 제시한다.

논문접수일 : 2005년 11월 게재확정일 : 2006년 9월 교신저자 : 이경전

1. 서론

상거래에서 이루어지는 다양한 비즈니스간의 거래는 기본적으로 어떠한 형태이던 간에 다소의 거래비용을 수반한다. 판매자는 상품을 알리기 위해 여러 매체를 통해 광고를 하며, 구매자는 자신이 원하는 상품을 찾기 위해 주변 사람에게 말로 물어보거나 검색창에 검색어를 입력하는 행위를 통해 정보를 찾아내고자 한다. 맘에 드는 물건을 발견하면 금액을 지불하기 위해 자신의 신용카드번호나 상대방의 계좌번호를 키보드로 타이핑하고, 마찬가지로 판매자는 결제를 위해 구매자에게 가격을 말로 설명하거나 가격표를 만들어 진열한다. 또한 결제 시마다 고객을 응대하여 돈을 받아 세고 잔돈을 거슬러주거나, 고객의 신용카드를 받아 리더기에 긁어주고 영수증을 손으로 쥐어 주는 행위를 매 거래마다 반복하는 것이 비즈니스간 거래비용이 나타나는 일반적인 모습이다. 이러한 다양한 프로세스들이 막히지 않고 마지막까지 이루어졌을 때 한 건의 구매행위라는 거래가 발생하며, 만약 각 프로세스의 어떠한 과정에서든 끊김이 발생한다면 구매라는 행위는 발생할 수 없다.

인터넷의 등장을 통해 디지털(Digital) 정보가 무수히 생성됨에 따라 이러한 정보를 이용한 e-Commerce

* This research is supported by the Ubiquitous Autonomic Computing and Network Project, the Ministry of Information and Communication (MIC) 21st Century Frontier R&D Program in Korea.

라는 새로운 상거래 영역이 생성되고 이것이 물리적(Physical or Local) 상거래와 맞물림에 따라, 상거래는 디지털 정보와 물리적 정보가 혼재하여 두 정보의 연결을 통해 거래가 발생하는 새로운 양상을 띠게 되었다. 그러나 이러한 상거래는 새로운 종류의 거래비용을 발생시키게 되었는데 이는 물리적 정보가 디지털 정보로 변환되거나 반대로 디지털 정보가 물리적 정보로 변환되는 과정에서 나타나는 전환비용이다. 예를 들어 상품에 붙어있는 물리적인 가격표를 보고 이를 신용카드나 계좌이체와 같은 e-Payment로 결제하려고 했을 때, 판매자 혹은 구매자는 해당 물건의 가격과 신용카드 번호, 계좌이체 번호와 같은 숫자를 결제 디바이스에 '입력해야 하는 수고(Hassle)'를 가진다. 마찬가지로 가격이 디지털 상태로 기록되어 있다고 해도 이를 구매자에게 로컬하게 보여주기 위해서는 물리적인 가격표를 만들어야 하는 수고를 들여야 하는데, 이는 두 정보(물리적 정보와 디지털 정보)의 특성이 상이함으로 인해 나타나며 이 과정에서 거래자는 '끊김'을 경험하게 된다. 이와 같은 끊김은 위와 같은 종류의 거래를 방해하는 요소가 되며 이 과정에 있어 높은 어려움을 겪는 거래자는 거래를 중단하고자 하는, 다시 말해 구매를 중단하고자 하는 의도 혹은 행위를 가지게 된다.

유비쿼터스 환경이 진행됨에 따라 이러한 끊김은 상당부분 '끊김이 없는(Seamless)' 상태로 변화하는 양상을 보인다. 상품에 RFID 태그가 내장됨에 따라 기존에 '입력'이 요구되던 과정은 리더기의 단순한 '인식(Reading)'으로 대체되고, Bluetooth나 IrDA와 같은 근거리 통신 기술은 동적(Dynamic)으로 생성되는 디지털 정보를 상대방의 디바이스로 끊김이 없이(USB에 저장해 다시 상대 디바이스로 저장하는 것과 같은 탈부착 행위 없이) 전송한다. 이러한 기술을 기반으로 U-Commerce는 'the real-world seamless communication of each entity's digital information'(이경전, 주정인, 2005)이 구현되며 U-Payment에 있어서도 마찬가지로 Seamless한 결제과정의 구현이 가능해진다.

또 하나의 이슈는 많은 유비쿼터스 컴퓨팅 관련 논문에서 중요하게 언급하고 있는 프라이버시의 문제이다. 기존 논문들에서 Floerkemeier et al.(2004)의 'Watchdog Tag'는 RFID의 프라이버시 침해 방지를 위해 목적성을 수반한 스캐닝의 RFID Protocol을 제안하고 있다. Roussos and Moussouri (2004)는 MyGrocer에 대한 사용자 FGI를 통해, 사용자들은 자신의 정보는 해당 자신이 소유해야 하며, 이것이 기업 등의 외부에 노출되는 것에 대한 높은 우려를 보여주었다. Acquisti(2002)는 프라이버시 보호기술에 대한 경제적 효용을 설명했고, Langheinrich(2001, 2002)는 프라이버시 보호에 대한 원칙과 보이지 않는 서비스에 대한 책임을 부여하는 방법으로 유비쿼터스 환경의 프라이버시 보호를 설명한다. Zugenmaier and Hohl(2003)은 유비쿼터스 환경에서 사용자의 ID를 노출시키지 않기 위한 익명성을 강조하고 있다. 그러나 다른 분야와 비교하여, 지불결제는 프라이버시 문제와의 관련성에 있어 더욱 높은 위상을 가진다.

그 이유는 다음과 같다. 일반적으로 프라이버시의 보호를 위해 기존의 상거래간 각 과정에서는 고객의 필요와 의도에 의해 소위 '가면을 쓴 상거래'가 가능했다. 상품을 검색하고 비교하고 협상하는 과정에서 고객은 자신이 원하고 또한 노력한다면, 자신의 개인 정보를 밝히지 않은 상태에서 이 과정을 수행하는 것이 어느 정도 가능했다. 그러나 이러한 노력에도 불구하고, 결국 최종적인 '지불'의 과정에서 상품 구매에 대한 정보가 외부에 저장되어 프라이버시가 침해되는 결과가 발생하게 된다. 때문에 앞서의 프라이버시를 지키기 위해 썼던 가면은 아무

소용이 없어지는 것이다.

기존의 결제방법 중 위의 문제를 가장 잘 해결하고 있는 수단은 바로 현금결제이다. 이후 개발된 지불결제수단은 상거래간 지불편의성을 높이기 위한 방향으로 발전했지만, 오히려 프라이버시 문제에 있어서는 점점 취약해지는 결과를 초래했다. 마찬가지로 전자지불결제(e-Payment)와 같은 디지털 형태의 지불결제수단이 생겨남에 따라 전자화폐(e-cash)는 이러한 문제를 해결할 수 있는 대안이 될 수 있다. 그러나 현재까지의 전자화폐 발전양상을 볼 때 앞으로 유비쿼터스 환경이 진행됨에 따라 보편적이고 범용적으로 통용되는 전자화폐가 생겨날 확률은 매우 낮다. 이는 결제수단이란 결국 제도와 여러 사업자간 규약 및 통합의 이슈와 관련되기 때문이며, 이로 인해 특정집단에서만 사용 가능한 사이버 머니(Cyber Money)와 같은 종류의 전자화폐가 등장할 가능성이 높다. 그러나 이것은 확장성(Scalability)이 매우 떨어지므로 보편적인 결제수단의 대안이 되기에 매우 어려운 측면이 있다. 때문에 앞으로의 결제시스템은 은행계좌이체와 같은 매우 공증된 기관에서만 다소의 정보를 소유하는 방식이나, 신용카드 류의 경우에도 개인정보가 넘겨져서(신용카드를 주거나 번호를 판매자가 받아서 결제하는 것과 같은) 결제가 이루어지는 것이 아닌, 개인정보의 제공이 최소한으로 통제되는 상태에서 지불자가 주도적으로 결제를 진행할 수 있는 방향으로 발전할 가능성이 높다. 이것은 지불편의성을 위해 결제 서버의 개입을 어느 정도 인정하면서도 프라이버시를 유지하는 대안이 될 수 있다.

본 연구는 U-Payment의 주요 특성이자 이슈인 Seamlessness(연결완전성)와 프라이버시가 강화된 U-Payment 메쏘드를 제안하고자 한다. 이를 위해 유비쿼터스 환경의 중요한 사용자 특성과 바람직한 현상을 설명하고, 이러한 특성이 나타나는 시나리오를 제시하며, 이에 대한 구체적인 시스템 아키텍처를 제시하는 과정으로 본 연구를 진행하고자 한다.

2. U-Payment 환경의 특성

유비쿼터스 환경에서 나타나는 중요한 사용자 결제환경의 특성은, 사용자의 결제정보 생성 및 변환, 전송 등이 Seamless하게 이루어지는 것과 사용자의 결제 디바이스 기능 및 정보처리능력, 저장능력 등이 매우 강해진다는 점이다. U-Payment 환경에서 예상되는 이러한 특성은 이전의 결제방식과는 다른, 새로운 결제방식을 사용자에게 제안할 것이다.

2.1 연결완전성(Seamlessness)

Seamless한 결제정보처리는 사용자의 결제양상을 간결하게 변화시킬 뿐 아니라 이를 통한 새로운 결제가치를 제공한다. 예를 들어 지하철을 탄다고 했을 때, 이전에는 개찰구를 통과하기 위해, 따로 마련된 창구에서 자신의 현금을 승차권이라는 결제대체수단으로 교환하여 서비스를 이용했다. 그러나 현재는, IC칩이 내장된 스마트카드의 접촉을 통해 나의 결제정보가 Seamless하게 지하철의 결제시스템으로 전달된다. 이 과정에서 기존의 '현금'이라는 물리적 결제정보는 매우 Seamless하게 디지털 결제정보로 변환되어 판매자에게 전송되게 된다. 또한 현재의 스마트카드 상황에서도 결제처리과정이 판매자(Payee) 시스템 위주로 설계됨에 따라 Seamless한 결제가 이루어지지 않는 상황이 발생한다. 이것은 예를 들어 현재 노약자나 장애인의 혜택으로 개찰구를 무임으로 승차하려고 할 때, 노약자나 장애인은 매 결제마다 무임승차권을 발급

받기 위해 승무원의 확인과정을 거쳐야 한다. 여기에서 만약 더욱 Seamless해지는 결제상황을 생각해본다면 노약자나 장애인은 자신을 증명하는 결제 ID가 내장된 스마트카드를 접촉하는 것만으로 자신의 무임승차자격을 증명할 수 있고, 이러한 결제과정은 매우 Seamless하게 이루어질 수 있을 것이다.

일반 상점(Local Shop)에서 상품을 구매하는 경우에도 마찬가지 양상이 나타난다. 현재의 상품결제는 결제정보변환에 있어 사용자의 높은 수고를 수반한다. 예를 들어 일반 상점에서 모바일 계좌이체를 통해 전자제품을 결제하는 경우, 판매자의 계좌번호와 가격을 일일이 입력하여 결제금액을 판매자의 은행계정으로 전송하고, 이를 판매자가 재확인 후, 결제과정이 종료되어 상품의 인수가 이루어진다. 그러나 만약 각 상품 안에 RFID 태그가 부착되고 태그 안에는 가격과 판매자의 결제계좌주소가 저장되어 있다면, 그리고 이를 구매자의 모바일 디바이스가 원터치로 인식하여 자신의 은행계정을 통해 판매자의 은행계정으로 직접 금액을 전송할 수 있다면, 구매자와 판매자는 쌍방의 거래비용을 대폭 줄인 상태에서 Seamless한 결제를 실현할 수 있을 것이다.

U-Payment 환경에서 나타나는 Seamlessness는 결제정보의 프로세싱과 네트워킹에 관련하여 사용자의 결제양상을 변화시키는 매우 중요한 특성이다. 이전 결제환경의 물리적 정보와 디지털 정보가 만나 각기 다른 종류로 변환되는 인터페이스에서 이 과정은 사용자의 높은 전환비용을 감수하며 이루어질 수 밖에 없었다. 오프라인 상거래에서 상품의 가격 및 결제수단 등의 결제정보는 물리적인 가격표 혹은 종이 매뉴얼에 의해 저장되어 있고, 상당부분은 아예 형식화(Codify)되지 않은 채 판매자의 머리 속에 무형지로 존재하고 있다. 그러나 이러한 정보들이 Seamless하게 디지털 정보로 변환되면서 나타나는 결제환경의 간결성은 기존에 사용자가 겪어야 했던 높은 수고를 대폭 줄이고, '끊김이 없는 결제(Seamless Payment)'를 제공하게 될 것이다.

그러나 이것은 'Calm Payment'와는 또 다른 이슈이다. Boddupalli et al.(2003)는 U-Payment의 필요조건 중 유용성(Usability)에서, 사용자 비인지 상태의 결제과정(Calmness)과 사용자 관여과정(User Involvement)이 균형을 이루어야 하며, 특히 사용자 비인지 상태에서 이루어지는 결제과정은 주로 파급이 적은 거래(Low Value Transaction)에서만 이루어져야 한다고 설명한다. 마찬가지로 U-Payment의 Seamlessness는 기본적으로 'Calm Payment'에 동의하지 않는데, 이는 사용자의 결제에 관련한 심리적 특성을 전혀 반영하지 못한, 단지 기술중심의 결제개념이기 때문이다. 'Calm Payment'라는 매우 사용자 무의식적(Unconscious) 결제방식이 이루어진다고 했을 때, 기본적으로 사용자는 자신의 허락 또는 확인과정 없이 진행되는 결제를 용인하지 않을 가능성이 높다. 왜냐하면 결제는 사용자의 실제적인 '돈'이 이동되는 행위이며, 이것은 사용자의 매우 높은 수준의 관여도가 수반되어야 하는 과정이기 때문이다. 여기에서 말하는 Seamlessness는 사용자의 결제확인과정과 같은 의식(Consciousness)이 생략되는 Seamlessness가 아닌, 사용자의 정보전환비용이 생략되는 Seamlessness로 이해하는 것이 정확하다.

2.2 Strong User Device

U-Commerce 환경의 각 개인은 일종의 UDA (Ubiquitous Digital Assistant)와 같이, 강력한 정보처리와 네트워킹이 가능한 개인의 모바일 디바이스를 가지게 될 가능성이 높다. 이는 유비쿼터스 환경의 모든 거래의 본질이 기본적으로 정보의 프로세싱

과 네트워킹에 의한 과정이며, 특히 비즈니스에 관련된 거래를 수행하는데 있어 각 개인은 독립적인 거래의 주체가 되기 때문이다. 또한 이러한 디바이스가 칩의 형태로 사람의 신체 안에 내장되는 것은 사회통념상 매우 어렵고, 매우 작은 단위의 객체들(Object, 포장된 휴지 등의 작은 제품과 같은)은 경제성으로 인해 각각이 컴퓨팅 기능을 가지지 못한 상태에서 디지털 태그 정도만이 부착될 가능성이 높다. 때문에 각 개인은 유비쿼터스적인 디바이스를 필수적으로 휴대하게 될 것이다.

이러한 사용자 단말(User Device)은 결제거래에 있어 개인의 결제 디바이스의 기능을 수행하며, 이후 강력해지는 결제주체로서의 역할은 강력한 정보처리 및 네트워킹 능력을 가진 사용자 단말기기를 요구할 것이다. 이에 따라 U-Payment 환경에서는 강력한 능력을 가진 독립적인 사용자 결제단말(Personal Payment Device)이 나타나게 될 가능성이 높다.

결제과정에 있어 사용자 단말은 다음의 3가지 기능을 수행하게 된다.

- ***정보수집(Information Gathering)***

구매자 결제단말(Payer Device)은 Seamless한 결제관련정보 인식기능을 수행한다. 앞서 예를 든 일반 상점의 전자제품 결제 과정에서, 구매자 결제단말은 상품의 RFID 태그에 기록된 가격과 판매자 계좌정보를 Seamless하게 인식하여 결제의 초기과정을 수행하였다. 이와 같이 구매자 결제단말은 정적(Static)으로 기록된 RFID 태그의 결제정보와 동적(Dynamic)으로 생성되는 서비스가격 등의 결제정보를 Bluetooth와 같은 방식으로 수집하여 사용자에게 정보변환의 Seamless 가치를 제공할 것이다.

- ***정보처리(Information Processing)***

구매자 결제단말은 인식한 결제정보의 처리과정을 단말기 내에서 자체적으로 수행한다. 이것은 사용자의 단말기 상에서 은행의 어플리케이션을 실행하여, 사용자 인증을 통해 금융정보를 판매자 은행계정으로 전송하고, 그 결과를 확인하는 등의 대부분 결제처리과정을 구매자 결제단말 중심(Payer Device Oriented)으로 처리하는 것이 가능해짐을 의미한다.

- ***정보저장(Information Storing)***

위와 같은 결제처리간, 결제처리 이후의 모든 결제관련정보는 구매자 결제단말 내에 주도적으로 저장될 것이다. 이전의 결제에서 결제정보는 대부분 서버의 역할을 담당하는 신용카드사 혹은 은행에 저장되었으나 이러한 정보가 구매자 결제단말의 PIB(Personal Information Base)에 저장됨에 따라 U-Payment는 결제자의 프라이버시가 강화되는 구조로 변화할 것이다.

강력한 사용자 단말의 등장에 따라 나타나는 결제양상변화의 의의는, 유비쿼터스 환경의 결제가 판매자 시스템 기반(Payee System Oriented)에서 구매자 단말 기반(Payer Device Oriented)으로, 결제시스템의 주도권이 이동한다는 점이다. 또한 이러한 양상이 심화됨에 따라 더욱 유비쿼터스화된 환경의 구매자 결제단말은, 자체적으로 구매자와 판매자의 기능을 동시에 수행하며, 결과적으로 각 개인이 독립적인 비즈니스 주체로 진화하는 U-Commerce 환경을 예상할 수 있다.

3. U-SDT 프로토콜

지금까지 살펴본 바와 같이, U-Payment 환경에서 나타나는 중요한 특성인 Seamlessness와 사용자 단말의 강화, 그리고 유비쿼터스의 중요한 이슈인

프라이버시 보호는, U-Payment 메쏘드를 설계하는데 있어 초기부터 고려되어야 하는 필수적인 요소이다. 지금부터 이러한 요소들을 반영하여 RFID와 구매자 결제단말, 금융기관의 결합을 통해 결제 참여자에게 새로운 가치를 제공하는 U-Payment 메쏘드, U-SDT(Secure Direct Transaction) Protocol을 제안한다.

3.1 결제 시나리오

• *상품 시나리오*

IT 직종에 근무하는 회사원 James는 여자친구와의 1주년 기념일을 위한 선물을 사기 위해 백화점 쇼핑을 나섰다. 한참을 돌아다니다 여성의류 샵의 쇼윈도에서 맘에 드는 원피스를 발견한 James는 상점에 들어가 쇼윈도에 걸려 있던 하늘색 원피스를 가져다 달라고 요청한다. 옷감 및 여러 상태를 살펴본 후 원피스가 매우 마음에 들어 구매를 결정한 James는 점원에게 결제를 요청한다. 원피스를 상점결제기에 가져간 점원은 결제기로 상품 태그정보를 인식(Reading)하고, 결제 모니터에 상품 및 가격이 전시되자 James는 자신의 UDA로 결제기의 결제정보를 인식한다. James의 UDA에는 결제 어플리케이션이 실행되고, UDA 화면을 통해 상품명과 치수, 가격 등을 확인한 James는 공인인증서의 인증 후 결제명령을 완료한다. 몇 초 후 James의 은행계좌에서 전송완료 확인창이 James의 UDA 화면에 표시되고, 상점의 점원은 상점의 계좌 확인창이 실행되어 있는 상점의 모니터를 통해 결제확인 후 원피스의 도난경고신호 제거 및 영수증 생성을 위한 메뉴를 클릭한다. 혹시 여자친구가 맘에 안 들어 교환이나 환불을 할지도 모른다고 생각한 James는 상점의 결제기를 향해 인식버튼을 눌러 전자영수증을 전송 받고, 한 손에 원피스가 든 쇼핑백을 든 채 기쁜 마음으로 여자친구를 향해 발걸음을 옮긴다.

• *무형재 및 서비스 시나리오*

이후 James는 여자친구와 함께 커피숍에 들어간다. 둘은 커피와 샌드위치를 주문한 후, 선물을 전달하고 즐겁게 담소를 나눈다. 어느덧 시간이 늦어 집에 돌아갈 시간이 되고, James는 결제를 위해 커피숍의 결제기를 향해 UDA의 결제버튼을 클릭한다. 결제화면에는 상품명과 상품가격, 거래 ID가 나타나고, 마찬가지로 사용자 인증을 거친 후 결제를 완료한다. 전자영수증을 받기 위해 다시 결제기를 향해 인식버튼을 누른 후 James는 여자친구와 함께 커피숍을 나온다.

• *C2C 거래 시나리오*

여자친구를 집에 바래다주는 길에 길거리의 조그만 자판에서 독특한 수공예 목걸이를 발견한 James는 여자친구와 함께 1주년 기념 커플목걸이를 맞추기로 마음먹는다. 그러나 마침 현금이 떨어진 James는 상인에게 UDA 결제를 요구한다. 그러자 상인은 자신의 UDA를 꺼내어 상품가격을 입력 후 수금버튼을 누르자 상인의 은행계좌와거래 ID가 포함된 결제정보가 생성되고, James는 결제버튼을 눌러 상인 UDA의 결제정보를 인식한다. 이후 이전 결제과정과 마찬가지로, 인증과정을 거쳐 제품가격을 송금하고 상인에게 전자영수증을 인식한 후, 서로의 목에 목걸이를 걸고 즐거운 마음으로 여자친구의 집으로 향한다.

위의 세 가지 시나리오는 유비쿼터스 환경에서 구매자의 디바이스를 중심으로 처리되는 상품과 서비스의 결제 양상을 구체적으로 그려 본 것이다. 이는 표면적으로 기존의 여러 논문에서 나타난 결제 시나리오(BluePay와 MyGrocer의 결제 시나리오,

구매자의 모바일 디바이스를 이용해 상품의 RFID Tag를 인식하여 자동적으로 결제되는)와 유사하나, 그 이면의 결제정보 흐름 및 저장위치, 정보처리의 주도적 디바이스 등에서 뚜렷한 차별점이 존재한다.

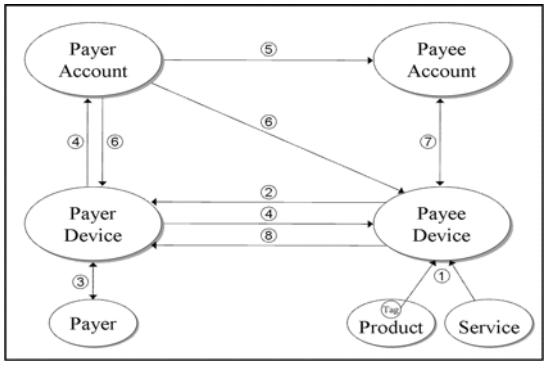
위 시나리오에서 상품구매의 경우, 상품 내에 부착된 태그를 이용하여 판매자의 결제 디바이스가 결제 관련정보(가격, 판매자 결제계정, 판매자 측 거래 ID)를 생성하며, 태그가 부착될 수 없는 무형재 및 서비스의 경우, 판매자의 결제 디바이스가 태그의 활용 없이 직접 결제정보를 생성하여 결제과정이 이루어진다. 이들 간 거래에는 지불편의성을 높이기 위한 금융기관이 개입되나, 이전 결제와의 가장 큰 차이점은 결제정보의 처리 및 저장 등의 과정이 판매자(혹은 수취인)의 디바이스나 금융기관의 서버가 아닌, 구매자(혹은 지불인)의 디바이스에서 주체적으로 이루어진다는 점이다. 이는 U-SDT에 있어 사용자의 프라이버시가 강화되는 요인이 될 것이다.

향후 유비쿼터스 환경에서는 활성화된 C2C 상거래로 인해 각 개인이 비즈니스 주체가 되는, 이른바 'Indipany(Individual + Company) 상거래'가 등장하게 될 가능성이 높다. 이를 지원하기 위한 필수적 결제환경은 구매자와 판매자의 결제시스템이 통합된 개인결제단말(Personal Payment Device)의 등장이다. 세 번째 시나리오와 같이, 판매자가 카드리더기와 같은 추가적인 결제 디바이스를 갖추지 않더라도, 개인의 강력해지는 디바이스는 피어(Peer)간의 결제행위를 원활하게 지원하게 된다. 이를 통해 각 개인은 각자가 구매자이자 판매자의 역할을 동시에 수행하는 것이 가능하다.

시나리오에서 드러나지 않는 다른 한 가지 중요한 측면은, 결제거래 이면의, 거래 ID(TID : Transaction ID)에 기반한 결제시스템의 등장이다. 이는 기존 현금결제 이외의 모든 결제 시 필수적으로 수반되던 구매자와 판매자 ID의 노출 없이, 금융기관을 이용한 결제를 가능하게 하는 중요한 요소이다. 거래 ID의 생성 역시 기존의 구매자 단말에 의존적 시스템이 아닌, 구매자와 판매자가 동등한 권한으로 상호 생성 및 인증하는 시스템으로 설계되며, 구매자 단말과 판매자 단말에 의해 만들어진 두 거래 ID의 결합을 통해 하나의 고유한 거래 ID가 생성된다. 각 결제에 대한 고유성과 대표성을 가지는 거래 ID는 환불과정에 있어서도 중요한 역할을 담당한다. 기존의 환불과정에서는 거래내역 확인 및 금융기관을 통한 결제내역의 확인과정을 거쳐 구매자의 계좌주소를 확인 후 판매자 계좌에서 송금하는 방식으로 환불처리가 이루어졌다. 그러나 거래 ID를 통한 환불과정에서는, 구매자의 금융기관(Payer Account)에 해당 거래의 거래 ID에 대한 환불 인증과정만을 거치면 판매자의 금융기관(Payee Account)에서 해당 거래 ID가 대표하는 결제관련 정보를 확인하여 환불처리가 이루어지게 된다. 이와 같이 거래 ID는 결제에 대한 프라이버시와 효율성을 강화하는 역할을 수행한다.

3.2 U-SDT 프로토콜 시스템 아키텍처

U-SDT 프로토콜의 시스템 아키텍처는 다음과 같다.



[그림 1] U-SDT System Architecture

① 판매자 단말이 상품 태그를 인식 혹은 서비스 ID를 입력
② 구매자 단말이 판매자 단말이 생성한 상품 ID, 가격, 암호화된 판매자 ID(ID와 계좌주소), 판매자 TID(Transaction ID)를 인식
③ 상품목록 및 가격 확인 후 공인인증서 인증(구매자의 결제승인)
④ 판매자 단말로 구매자 TID(Payer_TID) + 판매자 TID(Payee_TID) 전송, 동시에 구매자 금융기관에 TID와 함께 지불명령
⑤ 송금
⑥ TID와 송금결과 전송
⑦ 수금 확인
⑧ 판매자의 결제완료확인이 인증된 영수증 TID 생성(Receipt_TID, 최종 TID), 이를 구매자 단말이 인식

• ***결제관련 주체***

U-SDT의 결제 관련 주체는 크게 네 가지로 구분된다.

첫 번째로 구매자 단말은 결제관련정보의 수집과 처리, 저장 기능을 수행한다. 세부적으로 판매자 단말로부터 결제관련정보를 인식하며, 판매자 단말이 생성한 거래 ID에 구매자의 거래 ID를 추가하여 상호 대등하며 고유한 거래 ID를 생성한다. 구매자와의 공인인증서 인증을 통해 금융기관 등이 개입되지 않는 사용자 인증과정을 거치며, 실제 금액을 전송하는 결제과정 역시 구매자 단말상에서 실행되는 어플리케이션에 의해 처리된다. 이와 같이, 구매자 단말은 U-SDT간 가장 주도적인 개체이며 가장 많은 결제관련정보를 소유한다.

두 번째는 판매자 단말로, 최초의 결제관련정보를 상품 태그 혹은 서비스 ID의 입력을 통해 생성하며, 판매자의 거래 ID를 생성한다. 결제 이후 거래 ID의 승인과정을 통해 구매자 단말로 전송하기 위한 전자영수증 정보를 생성하고, 상품 태그의 미결제상태를 결제완료 상태로 수정하는 신호를 상품 내 태그로 전송한다.

세 번째와 네 번째는 구매자의 금융기관과 판매자의 금융기관으로, 실제 금융정보가 거래되는 주체이다. 이 두 주체에서 실제적인 결제과정이 이루어지며 사용자에게 금융서버 개입에 따른 지불편의성의 가치를 제공한다. 그러나 이전의 은행이나 신용카드사와 같은 결제관련정보의 독점이 아닌 금융정보 교환의 최소한의 기능만을 담당하며, 때문에 이들의 역할은 이전보다 한층 가벼워진다.

• ***결제정보의 흐름***

U-SDT의 결제를 위한 정보흐름은 다음과 같이 진행된다.

① 최초 판매자 단말은 상품 태그의 인식을 통해 상품 ID를 확인하고 상품목록 및 가격, 암호화된 판매자 계좌주소정보와 판매자 TID를 생성한다. ② 구매자 단말은 판매자 단말의 결제관련정보를 인식하여 결제수행을 위한 어플리케이션을 실행한다. ③ 구매자와 구매자 단말은 공인인증서의 사용자 인증을 통해 구매자를 식별하고, ④ 구매자 단말은 판매자 단말로, 새로 생성된 구매자 TID+판매자 TID를 전송함과 동시에 구매자 금융기관에 가격, 암호화된 판매자 계좌주소정보, 거래 ID를 전송한다. ⑤ 구매자 금융기관은 해당금액을 판매자 금융기관으로 전송하고 ⑥ 결제완료 확인정보를 TID와 함께 구매자와 판매자의 단말로 전송한다. ⑦ 판매자 단말은 판매자 금융기관의 입금정보를 확인한 후 기존 TID에 결제완료인증을 추가한 영수증 TID를 생성하고 ⑧ 구매자 단말은 이를 인식 및 저장한다.

3.3 각 결제주체간 정보소유 구조

U-SDT 프로토콜의 또 다른 특성은 각 결제주체가 해당 주체의 결제수행에 필수적으로 필요한 결제정보만을 소유하는 최대한의 프라이버시가 강화되는 정보소유 구조를 가진다. 이를 위해 구매자 단말과 판매자 단말은 상대방의 ID 정보를 소유하지 않으며, 구매자 금융기관과 판매자 금융기관은 상품목록 정보를 소유하지 않는다.

- ***결제관련정보의 분류***

U-SDT의 결제수행을 위한 필수적 결제관련정보는 다음과 같다.

① 가격
상품 및 서비스의 가격정보로, 복수의 상품 및 서비스일 경우 총 가격을 의미한다.

② 암호화된 판매자 계좌 주소
판매자의 계좌 주소는 Seamless한 결제에 요구되는 가장 중요한 결제관련정보이다. 이는 판매자의 프라이버시를 보호하기 위해 암호화하여 전송된다.

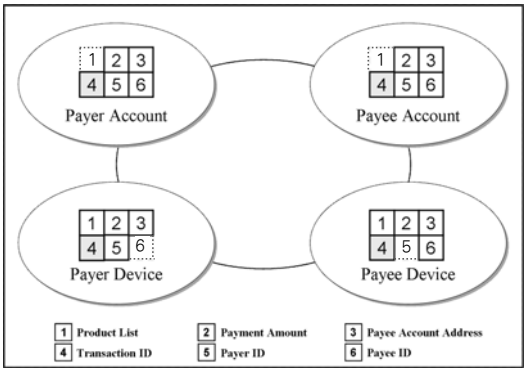
③ 상품목록
개별 상품명은 구매자가 아닌 기타 주체가 소유할 경우 심각한 프라이버시의 위협이 요구되는 정보이다. 때문에 이 정보는 반드시 직접적인 결제참여자만이 소유해야 한다.

④ 구매자 ID
금융기관의 금융거래간 판매자의 결제확인을 위해 필요한 정보이다.

⑤ 판매자 ID
금융기관의 금융거래간 구매자의 결제확인을 위해 필요한 정보이다.

⑥ 거래 ID
각 거래마다 고유한 거래 ID는 구매자와 판매자가 서로의 ID를 소유하지 않더라고 해당 거래에 대한 ID를 통한 결제 및 환불과정을 가능하도록 한다. 이러한 거래 ID는 구매자와 판매자에 의해 독립적으로 생성된 정보를 결합하여 하나의 거래 ID로 기능한다.

- ***각 결제주체의 정보소유 구조도***



[그림 2] 각 결제주체간 정보소유 구조도

위의 그림에서 나타나는 중요한 특징은 구매자 금융기관과판매자 금융기관이 상품목록을 소유하지 않으며, 구매자와 판매자 역시 서로의 ID를 소유하지 않는다는 점이다. 금융기관의 경우, 금융정보 거래를 위한 상대 ID 및 금융기관 주소를 소유하나, 결제의 외부주체이기 때문에 구매자의 프라이버시를 침해할 수 있는 상품 목록에 대한 정보는 소유하지 않는다. 판매자와 구매자의 경우, 결제 및 결제확인간 각 금융기관은 구매자와 판매자의 ID를 노출하는 대신에 거래 ID로의 대체를 통해 거래자의 ID와 같은 프라이버시정보의 유출을 방지한다.

결국 사용자의 Seamlessness에 따른 가치가 제공되며 동시에 프라이버시의 보호가 이루어지기 위해서는 각 결제주체가 결제수행에 반드시 필요

한 최소한의 결제정보를 분리해서 소유하는 구조가 필요하며, 특히 구매자 금융기관과판매자 금융기관은 상품 목록을, 구매자와 판매자는 상대의 ID를 소유하지 않는 방향으로 전체적인 U-Payment 아키텍처가 설계되어야 할 것이다. 또한 이를 가능하게 하기 위해서는 기본적으로 구매자 ID 기반이 아닌, 거래 ID 기반의 결제가 이루어지는 것이 바람직하다.

4. Related Works

Kourouthanasis et al.(2002)의 MyGrocer 중 In-Store 시나리오에서는 스마트 쇼핑카트가 자동적으로 결제서버(Cashier)에 결제정보를 전송하는 내용이 언급되나 이에 대한 구체적인 정보흐름이나 시스템 아키텍처는 제시되지 않았다. Boddupalli et al.(2003)의 경우 Jane의 시나리오에서 노트북에 저장된 전자지갑(Remote Wallet)과 전자태그(e-tag)를 통한 결제시스템을 설명하고 있으나 구체적인 아키텍처 제시가 아닌, U-Payment 디자인을 위한 요구사항을 제시하는 데에 중점을 두고 있다. Seigneur and Jensen(2004)의 경우 휴대폰에 저장된 익명 디지털캐시(Anonymous Digital Cash)를 통한 U-Payment를 제안하고 있으나 이는 소액결제의 분야로 한정되는 약점이 존재한다. Gross et al.(2004)의 경우 Mobey Forum의 PPA(Preferred Payment Architecture)에 기반한 U-Payment 테스트 플랫폼 'BluePay'를 제안하며, 이를 구체적인 아키텍처와 정보흐름을 통해 설명한다. BluePay의 경우 PTD(Personal Trusted Device)로 불리는 사용자 디바이스를 결제에 이용하고, RFID 및 Bluetooth 기술을 통해 POS(Ubicomp Retail Scenario에서 언급된 판매자 결제 디바이스)와 근거리 무선 통신으로 결제정보를 전송하며, POS는 상품의 태그를 자동적으로 인식하는 기능을 가진다. 또한 지불과정에서 고객의 '명시적 상호작용 행위(Explicit Interaction)'를 제거하거나 감소하기 위해 노력한다는 점과 일반 상거래에서 결제자의 결제관련정보가 PTD 내에 저장된다는 점에서 본 연구의 제안과 유사한 측면이 있다. 그러나 사용자 인증을 위해 PTD는 오직 고객 ID만을 저장하고, 신용카드나 계좌번호와 같은 심화된 지불정보는 은행이나 제 3주체(third parties)의 백엔드 시스템에 저장되어 ID 인증을 통해 로딩하는 방식으로 사용자 인증이 이루어지는데, 이러한 개인정보의 외부주체에 의한 저장은 프라이버시 침해의 이슈가 존재한다. 이를 위한 방지책으로 본 연구에서는 공인인증서에 기반한 구매자와 구매자 단말간의 내부 인증시스템으로 이를 대체한다. 또 다른 차이점은, 기존의 결제시스템과 마찬가지로 주요한 결제처리는 POS 내에서 외부 금융 DB 및 고객 DB와 연결되어 이루어지는데, 이는 기본적으로 결제의 주도권이 판매자에게 편중되어 있음을 의미한다. 이로 인해 판매자는 고성능 · 결제 디바이스를 보유해야 하고, 구매자는 자신의 금융정보를 판매자에게 전달해야 결제가 가능해지는 약점을 가진다. 본 연구는 이의 대안으로 구매자의 단말에서 판매자의 결제정보 인식을 통해 주요 결제처리가 구매자 단말에 기반한 결제시스템을 제안하며, 이후 개인의 단말 내에 구매자와 판매자의 결제시스템이 통합된 Peer-to-Peer 결제방식을 설명한다. 또한 결제정보흐름에 있어 거래 ID를 활용하여 각 주체의 ID를 노출시키지 않는 방식을 제안한다.

본 연구가 제안하는 결제시스템의 기존과 차별성은 사용자의 강화된 디바이스에 기반한 결제시스템과 이러한 모든 정보를 직접적인 결제참여자가 주도적으로 소유한다는 점, 또한 거래 ID를 통해

최대한 결제자의 ID 유출을 방지하여 프라이버시를 강화하는 것이라 할 수 있다.

이외에도 Labrou et al.(2004)이 제안한 UPTD (Universal Pervasive Transaction Device)에서 Wireless Wallet Application을 이용한 결제시스템, Acquisti(2002)의 익명성을 강조한 결제시스템, Divyan et al.(2004)의 거래 ID를 이용하여 사용자의 ID를 감추는 구조는 본 연구에서 강조하는 개념들과 부분적으로 맞닿아있다.

5. 결론

본 연구에서는 RFID와 사용자 단말의 강화, 금융기관 계정의 결합을 통해 사용자의 Seamless한 가치를 창출하고, 동시에 프라이버시 보호의 개선이 가능한 U-SDT 프로토콜을 시나리오와 시스템 아키텍처를 통해 설명하였다. 또한 이에 수반되는 바람직한 특징으로 결제정보소유의 분리적 구조를 제시했다. 우리의 접근에 있어 핵심 이슈는, 유비쿼터스 환경 이전에 발생하던 물리적 정보와 디지털 정보의 전환에 수반되는 높은 거래비용을, 유비쿼터스 기술의 Seamlessness 특성을 통해 대폭 감소시키고, 이와 동시에 더욱 침해될 것이라고 예상되던 유비쿼터스 환경의 프라이버시의 보호를 어느 정도 개선하는 방향으로 U-Payment 메쏘드를 설계하는 것이다. 만약 그것이 가능하다면, 이는 사용자에게 있어 높은 가치로 제안될 뿐 아니라, PayPal과 같은 독립적이고 스마트한 결제 비즈니스 모델과 메쏘드를 만들어낼 수 있을 것이라는 가능성에서 본 연구는 출발했다. 이를 위한 첫 단계가 바로 U-SDT Protocol이며, 이를 기반으로 각 결제사업자와 결제참여자를 만족시키는 비즈니스 모델과 메쏘드의 설계가 이후 연구에서 제안되어야 할 것이다.

참고문헌

[1] 이경전, 주정인, “연결완전성 제고와 프라이버시 보호를 위한 유비쿼터스 상거래의 설계 방안”, 2005 추계 지능정보시스템학회 논문집, (2005).

[2] Acquisti, A., “An User-centric MIX-net Protocol to Protect Privacy”, *Workshop on Privacy in Digital Environments : Empowering Users,* 2002.

[3] Acquisti, A., “Protecting Privacy with Economics : Economic Incentives for Preventive Technologies in Ubiquitous Computing Environments”, *Workshop on Socially-informed Design of Privacy-enhancing Solutions, 4th International Conference on Ubiquitous Computing (UBICOMP 02)*, 2002.

[4] Boddupalli, P., F. Al-Bin-Ali, N. Davies, A. Friday, O. Storz, and M. Wu, “Payment Support in Ubiquitous Computing Environments”, *IEEE Workshop on Mobile Computing Systems and Applications*, (2003), 110-121.

[5] Divyan, M. Konidala, C. Yeun, and K. Kim, “A Secure and Privacy Enhanced Protocol for Location-based Services in Ubiquitous Society”, *GLOBECOM*, 2004.

[6] Floerkemeier, C., R. Schneider, and M. Langheinrich, “Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols”, *Institute for Pervasive Computing,* 2004.

[7] Gross, S., E. Fleisch, M. Lampe, and R. Müller, “Requirements and Technologies

for Ubiquitous Payment", *Multikonferenz Wirtschaftsinformat, Techniques and Applications for Mobile Commerce*, 2004.

[8] Kourouthanasis, P., D. Spinellis, G. Roussos, and G. Giaglis, "Intelligent cokes and diapers : MyGrocer ubiquitous computing environment", *In First International Mobile Business Conference*, (2002), 150–172.

[9] Labrou Y., J. Agre, L. Ji, J. Molina, and W. Chen, "Wireless Wallet", *MobiQuitous*, (2004), 32-41.

[10] Langheinrich, M., "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems", *Ubicomp*, (2001), 273-291.

[11] Langheinrich, M., "A Privacy Awareness System for Ubiquitous Computing Environments", *Ubicomp*, (2002), 237-245.

[12] Roussos, G. and T. Moussouri, "Consumer perceptions of privacy, security and trust in ubiquitous commerce", *Personal and Ubiquitous Computing*, Vol.8, No.6 (2004), 416-429.

[13] Seigneur, J. and C. D. Jensen, "Trust Enhanced Ubiquitous Payment without Too Much Privacy Loss", *In Proceedings of the 19th Annual ACM Symposium on Applied Computing*, Vol.03(2004), 1593-1599.

[14] Zugenmaier, A. and A. Hohl, "Anonymity for Users of Ubiquitous Computing", *Security-Workshop at UbiComp,* 2003.

Abstract

Design of Ubiquitous Payment Process for Enhancing Seamlessness and Privacy

Kyoung Jun Lee* · Mu Jeong Jeong*

Ubiquitous computing is a study area explained in a myriad of contexts and technological terms. Payment, however, refers in nature to an act of money transfer from one entity to another, and it is obvious that a payment method will be valued as long as the transaction can be completed with safety no matter what technology was used. The key to U-payment is convenience and security in the transfer of financial information. The purpose of this paper is to find a desirable U-payment scheme by looking at the characteristics of seamlessness under the ubiquitous environments, strong personal device, and peer-based information transactions. We also propose U-SDT Protocol integrating technologies such as Radio Frequency Identification (RFID), Bluetooth, Personal Payment Device, Account Managing Application and Transaction ID as a way to make transactions between users seamless and secure better privacy protection.

Key words : Ubiquitous Computing, Payment, Seamlessness, Privacy, Personal Device

* School of Business, Kyung Hee University