PROTON : 선불 카드형 시스템

Proton은 카드형 시스템으로서 선불(Prepaid)체제이나 제3자에게 가치이전을 할 수 없다는 점이 MONDEX와 다르다. 벨기에 국적의 PROTON은 '95년 2월부터 레우벤 등 2개 도시에서 실험을 개시했다. 이 카드는 어디까지나 소액결제시장을 목표로 자동판매기 등에서 지불이 가능하도록 한 전자현금이다. 시험서비스에 참가한 점포는 약 300개이고, 지불단말 1,322대, 자동판매기 73대, 공중전화 50대 등이다. 소매점에서 취급대금의 0.7%, 자동판매기에서 2%를 수수료로 징수한다.

현재 Proton은 벨지움 국내에 3만매 이상의 카드를 발행하여 브르셀 등 대도시에도 사용이 가능해지고 있다. 현재는 은행의 크레디트카드와는 별도로 발행하고 있으나 '97년에는 일체화 할 계획도 있어, 이른바 본격적인 "전자지갑" 형태로 발전될 전망이다.

FSTC : 암호기술 이용 전자수표

전자수표에는 FSTC가 연구하고 있는 방식이 있다. FSTC란 미국의 정부계 연구기관과 금융기관이 공동으로 금융서비스에 관한 기술연구를 하고 있는 기관의 이름이다. 이 방식의 전자수표는 PC카드에 들어 있으며, 지불인이나 수취인과 은행간의 전자수표 수불은 전자메일을 이용하고, 전자수표에 대한 서명이나 이서는 암호기술의 응용인 전자서명을 이용하고 있다. ◆

전자머니의 핵심은 '암호' 위조 및 개변조 막는 관건

전자머니의 암호기술은 누구나 단순한 디지탈신호를 돈으로 인정하고 네트워크로 결제할 수 있도록 하기 위한 기반이다.

장차 국가의 개념까지 뒤흔들 '위력'을 내포하고 있다는 전자머니에 암호기술이 어떻게 관련되어 있는 것일까. 전자머니의 정체를 탐색하는 것은 정보사회의 기반을 파악하는 것이기도 하다. 카피를 막는 것이 암호이다.

공통키와 공개키

전자머니란 단적으로 말해 은행의 서명이 달린 금액 정보인데, 화폐의 위폐를 만드는 것은 어렵지만 디지탈 수치는 간단히 카피되어 버리므로 위조나 개조 및 변조 되지않는 전자머니를 실현하는 기술은 전적으로 암호기술에 의존되고 있다.

현대의 암호는 2가지 방식이 있다. 공통 키 방식과

공개 키 방식이다.

공통 키 방식은, 평문(平文)을 암호화하는 방법(암호화 키)과 암호문을 평문화하는 방법이 있다.

한편 공개 키 방식은 1976년에 그 개념이 나타난 정보화사회의 새로운 암호방식이다. 공통 키 암호와 다른점은 평문을 암호화 하는 방법, 즉 암호화 키를 공개한다는 점이다.

그런데 이를 해독하는 복호키가 받는 쪽마다 각각 달리 비밀로 되어있다. 누구나 정보를 암호화 할 수 있으나 이를 해독할 수 있는 것은 특정개인에 한정되는 상태를 만들어 낼 수 있다.

전자머니처럼 카피를 절대적으로 방지해야하는 정보에서는 공개키 방식이 공통 키 방식보다 뛰어나다고 할 수 있다. 공통 키 방식의 경우 '키'의 비밀은 절대적으로 지켜져야 한다. 만일 '키'가 누설될 경우 전자머니의 카피가 만연하여 시스템자체가 붕괴 될 수도 있기 때문이다. 그러나 공개 키 방식의 경우는 가령 개인의 복호키가 누설되더라도 손해는 개인에 한정되어 시스템 전체가 붕괴되는 사태까지 이르지는 않는다.

공개 키 방식에서 또 중요한 것은 인증기능이다. 인증은 2가지 의미로 쓰인다. 하나는 본인 확인이며, 다른 하나는 데이타가 개변조되어 있지 않음을 확인하는 것이다. 우선 본인 확인은 카드를 소지하고 있다는 것과 비밀번호를 알고 있다는 사실로서 확인을 하고 있다.

인증과 복제방지

또한 데이타나 문장이 개변조 되지 않았음을 검증한다는 의미에서의 인증은 평문에 의미있는 문장(성명이나 날짜등)이 포함되어 있음 경우, 평문에 고유의 복호 키를 작용시켜 만든 문장을 송신하고, 수신자가 송신자의 공개 암호화키로 평문화시켜 그 의미 있는 문장이 나타나면 통신도중 개변조되지 않았다고 판단해도 된다.

따라서 개변조 여부의 검증에도 공개 키 방식은 활용할 수 있다.

공개 키 방식에서의 전자머니 유통은 어떤 형태가 될 것인가. 우선 '인증센터'라는 컴퓨터가 필요해 진다. 센터는 전자머니를 거래하는 사람이 어떤자 인지와, 그리고 디지탈 신호가 머니임을 확인하는 기능을 지닌다. 어떤 사람이 네트워크상에서 은행으로부터 1만원의 전자머니를 인출하여 상점에 지불할 경우, 먼저 은행은 인출을 요구한 사람을 확인하여 그 사람의 IC카드에 1만원이라는 머니로 변화를 할 수 있는 디지탈 신호를 보낸다. 이 신호를 받은 사람은, 이번에는 상점의 IC카드에 전자머니를 입금하지 않으면 안된다.

이때 중요한 것은 확실히 상품거래 상대방으로부터의 전자머니임이 분명하고 가짜돈이 아닌 진짜돈임을 확인해야 된다는 것이다.

모든 것을 네트워크상에서 처리해 버리기 위해서는 '서명한다'는 행동까지도 디지탈 신호에 끼어 넣을 필요가 있는 것이다. 여기서 공개키 방식의 특징을 상기해 주기 바란다.

이 방식에서는 암호화하는 키는 공개되어 있으나 복호하는 키는 각자 고유한 것이라는 점이다. 서명(사인)이 각자 고유한 것인 것 처럼 공개 키 방식에서 각자 고유의 키가 있다는 것은 '서명하고 이를 확인하는'역할을 담당 할 수 있음을 말한다.

공통 키 방식은 이와 같은 거래에 사용하기엔 어려움이 있다. 각자 고유의 키가 없으므로 네트워크상에서 A로부터 B로 전자머니를 지불할 때에는 미리 '지금부터 송금하는 돈은 내 돈이다'는 등 연락이 필요해 진다. 사전연락이 필요없게 하기 위해서는 은행등 중개센터가 반드시 필요해 진다.

이상 공개 키 방식은 다시말해 어떤 개인이 비밀키와 공개 키라는 2종류의 키를 소유하고 ① 복제방지에 이용할 경우는 어떤 통신 상대이든 내가 공개한 키로 암호화시켜 수신한 암호문을 나 자신만 가지고 있는 비밀키로 복호한다. ② 인증에 이용할 경로는 먼저 비밀키로 서명하여 누구든 공개 키로 검증 시킨다는 방법이다.

어느 경우건 비밀키는 나만이 사용하고 공개키는 다른 다수의 사람들에게 사용케 한다.