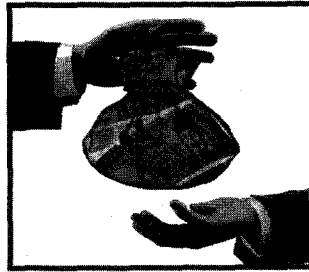


# 전자화폐, 전자서명



## 1. 전자화폐

### · 종류

칩카드에 가치를 저장해 사용하는 IC카드형(칩 카드, 스마트 카드, 인텔리전트 카드)과 PC의 하드디스크에 저장해 사용하는 네트워크형으로 나뉜다.

① IC카드형-전세계적으로 IC형 전자화폐가 대부분이며 몬덱스, 비자캐시, 프로톤 등이 대표적이다. 이는 IC칩이 부착된 플라스틱 카드에 일정한 금액을 충전했다가 현금 대신 쓸 수 있도록 만든 것으로 현재 사용되고 있는 지하철카드, 버스카드 등도 초보적인 형태의 전자화폐.

② 네트워크형-네트워크형 전자화폐는 PC나 인터넷 가상은행 계좌에 화폐가치를 저장했다가 인터넷을 통해 물건을 구입할 때 지불 수단으로 사용하는 것. 이를 '전자지갑'(e-Wallet/Digital Wallet)에 담은 전자화폐라고도 함. 전자지갑은 온라인상으로 결제가 이뤄지고 이에 대한 정보를 암호화해 주고받으며 EC 사용자의 지불보증과 구매거래장 기능을 제공한다.

디지털캐시가 개발한 e캐시가 대표적.

### · 장점

-네트워크상에서 지불이 가능해 전자상거래의 보편적 지불수단이 됨.

-실물화폐 관리에 따르는 비효율성(발행 비용, 유지관리 비용 등) 해소.

-소액단위의 현금을 다량으로 휴대해야 하는 사용자의 불편 해소.

-양도나 거래의 과정에서 화폐 위, 변조가 불가능.

### · 단점

돈세탁과 비자금 등으로 악용될 소지도 있어 현재 세계적으로 시범운영중인 전자화폐는 가치 저장한도를 대체로 수만원대 이하로 제한.

## 2. 전자서명 인증

### · 전자서명

종이문서에 사용되는 서명이나 인감과 같이 전자문서에 서명한 사람이 누구인지를 확인하고 서명된 전자문서가 변조되지 않았는지 여부를 알 수 있도록 전자문서에 부착되는 특수한 형태의 디지털 정보.

컴퓨터를 이용해 전자서명 생성과 검증에 사

용되는 한 쌍의 정보(전자서명키)가 자연인 혹은 법인이 소유하는 전자서명 생성기에 합치한다는 사실을 전문성과 공신력이 있는 공인 인증기관이 확인, 증명하는 것.

이때 전자서명 생성키는 서명자만 보관, 사용하고 전자서명 검증키는 정보 통신망을 통해 누구나 알 수 있게 공개.

공인인증기관은 서명자의 이름, 전자서명 검증키 등의 정보가 포함된 전자적 인증서를 발급한다. 서명자는 서명된 전자문서와 인증서를 함께 보내며 수신자는 인증서에 포함된 전자서명 검증키를 이용해 전자서명이 유효한 지 여부를 안전하게 확인.

· 부인봉쇄

전자서명에 대해서는 비밀키를 가지는 자가 아니면 서명할 수 없기 때문에 위조가 곤란한 사실, 전자서명을 한 사람이 본인이라는 것을 증명할 수 있는 사실, 전자서명을 한 전자문서는 변경이 곤란하다는 사실을 덧붙여 전자서명을 함으로써 본인이 자신의 의사에 의한 것이라는 사실을 부인하는 일이 곤란한 효과(부인봉쇄)가 있다.

· 전자인증

신뢰성이 검증된 개인·단체 등에 전자서명이 첨부된 인증서를 발급, 인터넷 등 가상공간에서 거래당사자간의 신뢰성을 보증해 주는 역할.

전자서명을 이용하기 위해 공인인증을 받으려는 사람은 먼저 전자문서에 본인의 신원과 해당 문서의 고유정보를 담은 전자서명생성키(비밀키)로 서명하고 수신자가 이용할 전자서명검증키(공개키)를 만들어 인증을 신청.

인증기관(CA:Certificate Authority)은 이들 전자서명키 소유자의 이름과 유효기간 전자문서 위·변조 여부를 확인한 뒤 인증서를 발급. 수신자는 전달된 전자문서의 전자서명을 인증서에 달려 있는 검증키(공개키)로 검증한 뒤 문서를 사용.

이같은 인증서비스를 제공하는 주체가 바로 인증기관이며, 국내에서는 99년 전자서명법을 통해 정부가 CA에 '공인성'을 부여했다. 공인 인증기관이 인증한 전자서명은 사설 인증기관과 달리 완벽한 법적 효력이 있으며 인증기관의 잘못으로 피해를 당했을 경우 손해배상을 받을 수 있다.

공인인증기관 자격을 얻기 위해서는 자본금 80억원에 정보통신부에서 고시하는 인증기관에 필요한 각종 설비와 인원 등을 갖춰야 한다.

용어설명

· 사이버 머니(Cyber Money)-사이버(가상) 공간에서 회원 확보 및 유지를 위해 인터넷업체들이 적립해 주는 가상의 돈을 일컫는다.

마일리지 성격으로 사이버 머니를 주는 입장에서는 현금 거래가 없기 때문에 부담이 없이 고객의 로열티를 높일 수 있으며, 고객의 입장에서도 전자 상거래 시 적립된 사이버머니를 현금 대신으로 사용할 수 있다.

· 스마트 카드-칩 카드, 인텔리전트 카드라고도 불리기도 하며 IC card를 일컫는 말이다. IC card는 신

용카드 크기의 플라스틱 카드에 집적회로 기술을 사용하여 마이크로프로세서, 기억기능등을 모은 제4세대 휴대용 카드를 말하는 것으로 넓은 의미로 집적회로가 봉입되어 있는 카드 모두를 가리킨다.

IC카드는 암호 알고리즘을 내장하고 있어 카드 소유자의 신분 확인이나 상호인증, 입출력 데이터의 암호화와 정보 저장 등이 가능하여 금융결제용, 프로그램 수납용, 공중전화용, 신분증명용 등 응용 범위가 넓은 것이 특징이다.

IC카드는 메모리와 CPU의 내장 여부에 따라 메모리 카드와 CPU 내장형 카드로 구분.