전자화폐 프로토콜 기술

송유진 • 동국대학교 정보산업학과 교수
동국대학교 정보산업학과 부설 전자상거래연구소 연구위원

1. 개요

최근 인터넷과 정보통신기술이 활성화됨에 따라 네트워크상에서의 전자적인 거래가 일반화되고 있다. 전자상거래가 급속히 보급됨으로써 건전한 지불방법의 확립이 중요하게 되었고 전자지불 수단인 전자화폐가 중요한 이슈로 떠오르고 있다.

여기서, 전자화폐란 디지털 정보인 비트열이 현금의 역할을 하는 것을 말한다. 즉, 비트열에 은행의 서명이 들어감으로써 일정한 가치를 지니게 되고 부정한 사용도 막게 되며 사용할 수 있는 권한 역시 부여되는 것이다. 디지털 정보의 형태는 일반적으로 IC카드에 저장하거나 통신망을 통한 전송이 쉽다는 장점을 갖는다. 그러나 전자화폐는 디지털 정보이기 때문에 데이터로서의 취급이 용이한 반면 위조에 대한 대책이 필요하고 사용자의 지불 이력이 수집, 관리되어 사용자 프라이버시가 침해될 우려도 있다.

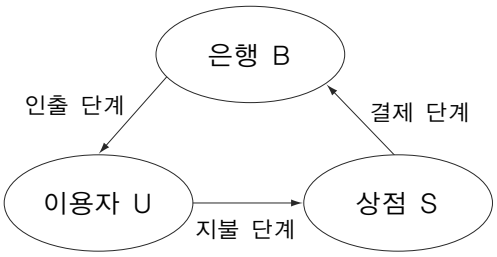
이와 같이, 전자화폐는 보안과 관련된 많은 문제가 발생한다. 부정사용 방지와 같은 보안 요구사항 뿐만 아니라 사용자 프라이버시 보호가 중요한 이슈이다. 사용자의 프라이버시 보호는 관리적, 법적대책 이외에 블라인드 서명과 같은 암호학적 도구의 사용으로 거래시 사용자의 익명성을 유지하는 전자화폐 프로토콜 구현이 가능하다.

전자화폐 프로토콜에 대한 연구는 Chaum, Fiat, Naor[CFN88]이 제안한 cut & choose 방식에 근거한 추적 불가능한 전자화폐 프로토콜, 그리고 Brands[Br93a]의 challenge response 방식에 근거한 전자화폐 프로토콜이 많은 연구의 기초가 되고 있다.

본 고에서는 전자화폐 프로토콜의 기본적인 개념과 구성에 대해 살펴보고자 한다.

2. 전자화폐 프로토콜

전자화폐의 기본 프로토콜은 < 그림 1 >과 같이 3단계로 구성된다. 즉, 이용자와 은행간에 이루어지는 인출단계(withdrawal phase), 물건을 사고 발행단계에서 받은 전자화폐를 상점에 지불하는 지불단계(payment phase), 이용자로부터 받은 전자화폐를 예치하여 상점의 계좌로 자금을 이체시켜 주는 결제단계(deposit phase)로 구성된다.



〈그림 1〉 전자화폐 프로토콜

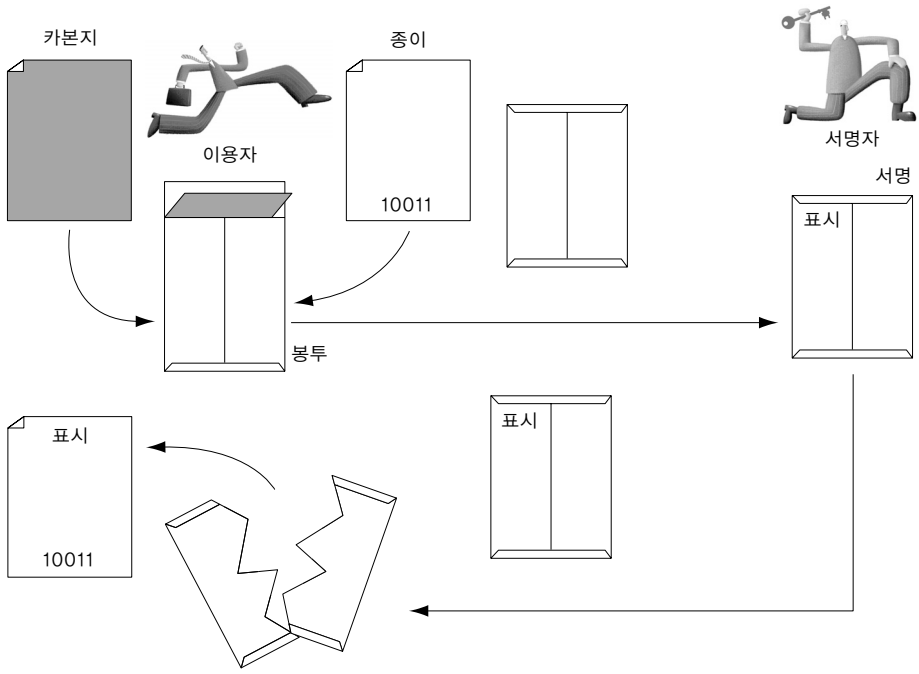
2.1 인출 프로토콜

은행에서 현금을 인출하는 과정을 가정한다. 일단 은행에 가서 인출청구서를 쓰고, 은행원에게 건네어 주면, 은행원은 비밀번호와 계좌번호를 확인한 후 정당할 경우 지급한다. 전자화폐를 은행으로부터 인출하는 방식도 이와 동일하다. 자신의 신원과 계좌번호, 찾고자 하는 액수를 기록한 후 확인을 거쳐 전자화폐를 인출하게 된다.

전자화폐의 인출 프로토콜은 이용자가 은행으로부터 전자화폐를 인출하는 단계의 프로토콜이다. 이해를 돕기 위해 색종이의 예를 들어 설명한다.

- 이용자는 예를 들면, 100^{140}색의 색종이 가운데 1색을 선택하여 복사용 먹지와 함께 봉투에 넣는다.
- 계좌의 소유자인 것을 증명하는 ID카드와 인출할 금액을 위에서 작성한 봉투에 넣어 은행에 전달한다.
- 은행은 ID카드에 의해 이용자를 인증하고 이용자의 계좌로부터 지정된 금액을 인출하고 봉투 위에 서명한다.
- 이용자는 봉투를 개봉하고 색종이에 은행이 서명했음을 확인한다.

인출 프로토콜에서는 이용자가 랜덤하게 선택한 색종이를 봉투에 넣어 내용이 보이지 않도록 해서 은행에게 서명(블라인드 서명)시킴으로써 전자화폐의 익명성을 구현한다<그림 2>.



〈그림 2〉 블라인드 서명의 원리

블라인드 서명처리에 의해 나중에 이 전자화폐(서명된 색종이)가 은행에 예치되더라도 이 전자화폐가 어떤 이용자에 의해 인출된 것인가에 대해 은행은 전혀 알 수 없다. 따라서, 이용자는 익명성을 유지한 채 전자화폐를 상점 등에 지불할 수 있다. 전자화폐의 익명성은 블라인드 서명[Ch82]에 근거한 전자화폐 인출 프로토콜에서 구현된다.

RSA 암호에 근거한 전자화폐 인출과정에 대해 설명한다.

우선, 전자화폐를 $(x, f(x)^{d_B})$ 형태로 나타낸다. 여기서, x는 이용자가 작성한 난수, f는 일방향성 함수, d_B는 전자화폐의 액면금액에 대응한 은행의 비밀키(은행은 전자화폐의 금액에 대응한 복수의 비밀키를 갖고 있음), mod n의 n은 은행의 RSA모듈러 값이다. 이와같이 전자화폐는 난수와 그 난수에 대한 은행의 RSA 서명으로 구성되고 전자화폐의 위조는 RSA 서명위조의 어려움에 의존한다.

- 이용자는 x와 블라인드 변수 r을 랜덤하게 선택하고 인출금액에 대응하는 은행의 공개키 e_B를 사용하여 $B = r^{e_B} f(x)$를 계산한다.
- 이용자는 ID카드를 제시하고 인출하고자 하는 금액(예를 들어, 10만원)과 함께 B를 은행에 송신한다.
- 은행은 B에 10만 원에 대응한 서명 $B^{d_B} \pmod n$을 계산하고 이용자에 보낸다. 동시에 이용자의 계좌로부터 10만 원을 인출한다.
- 이용자는 B^{d_B}를 r로 나누어 $C = f(x)^{d_B}$을 얻는다. 또한, $C^{e_B} = f(x)$에 의해 은행의 서명을 확인한다.

여기서, B^{d_B}는 $(r^{e_B})^{d_B} \equiv r \pmod n$의 관계로부터 $r \cdot f(x)^{d_B}$의 형태로 되며 이용자는 이를 r로 나누면 최종적으로 은행이 서명한 정당한 전자화폐 $(x, f(x)^{d_B})$를 얻을 수 있다.

이러한 인출 프로토콜에서 은행은 B밖에 수신할 수 없으므로 x나 C의 값에 대해 전혀 알 수 없다. 실제 전자화폐로써 이용되는 C의 내용을 모른채 B에 서명해도 은행의 리스크는 없다.

2.2 지불 및 결제 프로토콜

인출된 전자화폐를 사용하는 지불 프로토콜은 다음과 같다.

- 이용자와 상점간에 상품과 금액의 교섭이 성립되면, 이용자는 상품을 지정해서 전자화폐를 상점에 지불한다.
- 상점은 전자화폐의 이중사용 유무를 은행에 검사의뢰한다.
- 은행은 전자화폐에 부가되어 있는 은행의 서명을 확인하고 동일한 전자화폐가 과거에 예치된 적이 있는가를 은행 데이터베이스를 사용하여 조사한다. 만약 예치되어 있지 않으면 새로 예치하고 데이타베이스에 이 전자화폐를 등록한다.
- 상점은 전자화폐가 은행에 정확히 예치된 것을 확인하면 상품을 이용자에게 배달한다.

지불과정을 수식으로 설명하면 다음과 같다.

- 이용자는 (x, C)를 상점에 송신한다.
- 상점은 이를 수신하면 은행과 연결하여 동일한 (x, C)가 이미 예치되어 있는가를 조회한다.
- 은행은 전자화폐의 서명을 $C^{e_B} = f(x)$에 의해 확인하고 만약, 예치되어 있지 않으면 (x, C)를 예치한다.
- 예치상태를 확인하면 상점은 상품을 이용자에게 배달한다. 은행은 과거에 예치된 전자화폐를 모두 데이터베이스에 등록하고 새로 예치되는 전자화폐를 이 데이터베이스와 비교함 으로써 이중사용을 검출한다.

이와같이, 결제 프로토콜에서는 과거 은행에 축적된 전자화폐를 모두 데이타베이스에 기록해 두고 새롭게 예치되는 전자화폐와의 중복을 검사한다. 은행

은 만약 동일한 전자화폐가 예치된 경우, 이중사용으로 간주하고 상점의 전자화폐 예치를 거부한다.

3. 전자화폐 프로토콜 구성

대표적인 전자화폐 프로토콜을 구성하고 분석한다.

3.1 Chaum, Fiat, Naor 전자화폐 프로토콜

먼저, cut & choose 방식에 대해 설명한다.

은행은 이용자가 제시한 전자화폐의 구성을 확인할 수 있도록 안전성 변수 k/2개 항(term)의 구성을 보여줄 것을 요구하고 이용자는 요구된 항에 대해 은닉되었던 값들을 보여줌으로써 은행이 이를 확인하게 한다. 이후 은행은 나머지 k/2개의 은닉된 항에 서명을 하여 이용자에게 전달한다. 마지막으로, 이용자는 항의 은닉을 위해 이용했던 자신만이 알고 있는 정보를 제거하는 것으로 전자화폐를 인출한다.

인출된 전자화폐를 정상적으로 사용한 이용자에 대해서는 이용자가 상점에 제공하는 힌트 정보에도 이용자의 계좌번호가 전혀 검출되지 않지만 전자화폐가 이중사용이 되었을 경우, 은행에 저장된 이용자, 은행, 상점간에 주고받은 모든 정보들을 근거로 동일한 전자화폐를 제시한 둘 이상의 상점들의 challenge 정보 중 일치하지 않는 인덱스 정보에서 이용자의 계좌를 검출한다.

Chaum, Fiat, Naor [CFN88]의 전자화폐 프로토콜은 이중사용자 검출이 가능한 cut & choose 방식의 전자화폐이다. 색종이를 이용하여 개념을 설명한다.

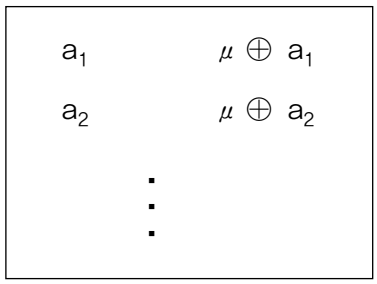
가. 인출단계

이용자가 은행으로부터 전자화폐를 인출할 때 RSA 서명을 사용하여 추적 불가능한 전자화폐를 구현한다. 이용자는 전자화폐를 얻기위해 자신의 신원정보가 쓰여진 은닉된 메시지들을 생성하여 은행에 제시하는데 영지식 증명방식을 이용하여 이것을 은행에게 확인시킨다. 그러면 은행은 블라인드 서명을 이용하여 서명한 전자화폐를 이용자에게 전달하게 되고, 이용자는 자신만이 알고 있는 정보를 이용하여 지불가능한 전자화폐를 인출한다.

색종이를 이용해 이러한 내용을 단계별로 설명한다.

(1단계)

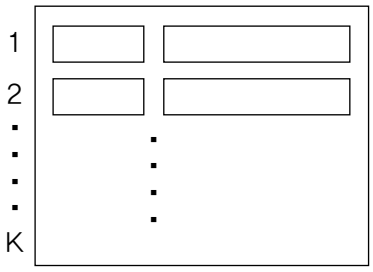
이용자는 난수 $\{a_1, a_2, \cdots, a_k\}$를 선택하여 <그림 3 >과 같은 보통종이 위에 기록한다. 여기서, μ는 이용자의 계좌번호이다.



〈그림 3〉 보통종이

(2단계)

이용자는 기록된 보통종이 위에 색종이를 붙여서 은행에 송신한다. <그림 4 >



〈그림 4〉 색종이

(3단계)

은행은 k/2 개의 난수로 이용자가 숨긴 내용을 밝히기를 요구한다. (간단히 k/2 개의 난수를 {k/2+1, …, k}로 한다.)

(4단계)

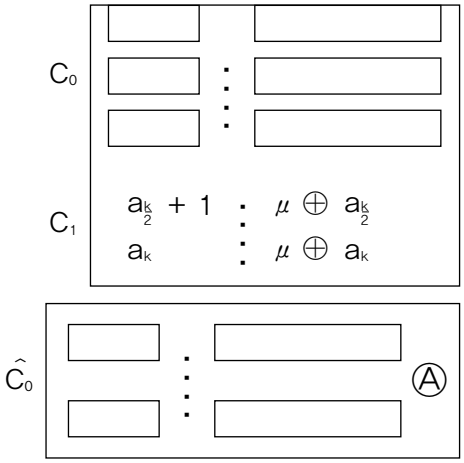
이용자는 은행이 지정한 난수 번호 {k/2+1, …, k}에 해당하는 색종이를 떼어서 1단계의 그림에서와 같은 형태의 식으로 되어 있다는 것을 증명한다.

(5단계)

은행은 색종이를 떼어 낸 C_1부분을 확인한다. (<그림 5 >의 상단부분 참조)

(6단계)

은행은 색종이가 떼어지지 않은 부분에 서명해서 이용자에게 양도하고 이용자 계좌에서 해당금액을 빼낸다. 은행으로부터 수령한 이것이 전자화폐 $\hat{C}_0$가 되게 된다. (<그림 5 >의 하단 부분 참조).



〈그림 5〉 색종이를 이용한 전자화폐

나. 지불단계

전자화폐를 상점에 지불하는 경우, 상점은 지불된 전자화폐가 올바른 정보로 구성되었고 은행의 서명을 받은 것임을 확인한 다음 지불된 전자화폐에 대한 금액을 은행에게 입금할 것을 요구하게 된다. 여기서, 누구나 전자화폐의 올바른 구성과 은행으로부터 서명을 받은 전자화폐임을 확인할 수 있지만, 은행이 특정한 전자화폐를 그 전자화폐 수령인의 계좌와 연결시킬 수 없다는 점이 고객에 대한 추적을 불가능하게 해준다. 또한 오프라인으로 지불이 이루어져도 동일한 전자화폐를 두번 사용한 이용자는 은행에 의해 추적될 수 있다. 이를 위해 cut & choose 방식을 이용한다. 색종이를 이용하여 단계별로 설명한다.

(1단계)

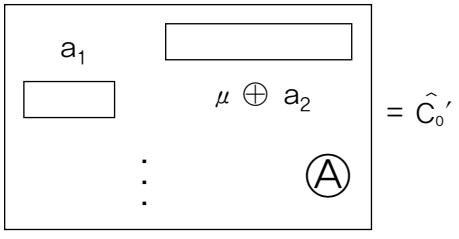
이용자는 상점에 상품구매와 함께 전자화폐를 제시한다.

(2단계)

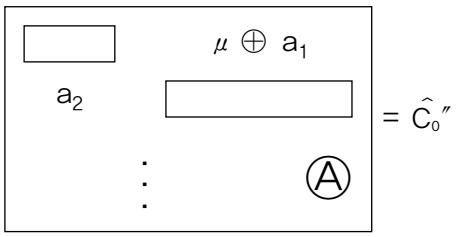
상점에서는 난수열 $\{e_1, e_2, \cdots, e_{k/2}\}$를 이용자에게 건네주며 전자화폐 가운데 색종이로 덮힌 부분을 보여줄 것을 요구한다.

(3단계)

이용자는 ei = 0인 경우 a_i를, e_i = 1인 경우는 $\mu \oplus$ ai의 색종이를 떼내어 상점에 보여준다. 예를 들어, $(e_1, e_2, \cdots) = (0, 1, \cdots)$라면 <그림 6 >의 $\hat{C}_0'$와 같이 된다.



〈그림 6〉 전자화폐 $\hat{C}_0'$



〈그림 7〉 전자화폐 $\hat{C}_0''$

다. 결제단계

(1단계)
상점은 은행에 $\hat{C}_0'$ 를 예치한다.

(2단계)
은행은 상점의 계좌에 해당금액을 이체시켜 준다.

라. 이중사용자 검출

이용자가 $\hat{C}_0'$ 를 다른 상점에 다시 사용하여 이중사용하였다고 가정해 보자. 이때, 그 상점이 건네 준 난수열을 (1, 0, …)라고 하면, 이용자는 <그림 7>과 같은 $\hat{C}_0''$를 상점에 건네주게 되며 은행은 이들 정보를 상점으로부터 받게된다. 은행은 상점들로부터 받은 $\hat{C}_0'$, $\hat{C}_0''$를 이용하여 a_i과 $\mu \oplus a_i$로부터 이중사용자의 계좌번호인 μ를 알게 된다. 여기서, 이중사용자의 검출확률이나 안전성은 상점이 건네주는 난수열의 랜덤성과 길이에 의존하게 된다.

3.2 Brands 전자화폐 프로토콜

cut & choose 방식은 오프라인에서 이중사용 검출시 매우 효과적이지만, 안전성을 위한 정보 k에 따른 통신 데이터량의 증가와 이용자와 은행간에 주고받는 데이터 중 반 정도만이 전자화폐가 될 수 있는 비효율적인 측면이 있다.

Brands[Br93a]가 제안한 전자화폐 프로토콜은 cut & choose 방식의 비효율적인 발행단계를 보다 개선한 challenge response 방식의 전자화폐 프로토콜이다.

프로토콜 구성을 위한 표기는 다음과 같다.

- $a \in_R G$: 집합 G속에 있는 원소를 임의(random)로 선택.
- p : 512-bit 소수.
  q : q는 $p-1$을 나누고 160-bit 소수이다.
- $g, g_1, g_2, d \in Z_p$: g, g_1, g_2, d는 Z_p의 원소이고 위수(order)가 q이다.
- x : 비밀키. h : $h = g^x \pmod p$이고, 공개키임.
- u_1, u_2 : 사용자의 신원과 관련된 값.
- H : 일방향 해쉬함수
- ? = : 맞는지 틀리는지를 검사. 만일 틀리다면 프로토콜을 끝냄.

가. 인출단계

(1단계)
이용자는 식 (1)을 만족하는 x_1, x_2, y_1, y_2를 임의로 선정한 다음, $I_A = f(\mu)$를 공개하고 G를 계산한다. 여기서 H는 암호적으로 안전한 일방향 해쉬함수이다.

$$\begin{cases} a = x_1 + x_2 \bmod P-1 \\ \\ a + \mu = y_1 + y_2 \bmod P-1 \end{cases} \quad \cdots(1)$$

$$G = H(g_1^{x_1}, g_2^{y_1}, g_1^{x_2}, g_2^{y_2}) \quad \cdots(2)$$

(2단계)
이용자는 은행에 $Z = r^e \times G \bmod N$ …(3)을 송신한다.

(3단계)

이용자는 영지식 증명으로 (I_A, Z)가 식(1), (2), (3)을 만족하고 있음을 은행에 증명한다.

(4단계) 은행은 $Z^d = r \times G^d$를 계산하여 이용자에게 전달함으로써 전자화폐 C를 얻게 된다.

$C = (G, G^d, g_1^{x_1}, g_2^{y_1}, g_1^{x_2}, g_2^{y_2})$

나. 지불단계

(1단계)

이용자는 상점에 전자화폐 C를 제시한다.

(2단계)

상점은 $G \stackrel{?}{=} H\ (g_1^{x_1}, g_2^{y_1}, g_1^{x_2}, g_2^{y_2})$, $(G^d)^e \stackrel{?}{=} G$를 검사한다.

(3단계)

상점은 이용자에게 난수 α를 보낸다.

(4단계)

이용자는 상점에 υ, ω를 보낸다.

$$\begin{cases} \upsilon = x_1 + \alpha\ x_2 \bmod P-1 \\ \omega = y_1 + \alpha\ y_2 \bmod P-1 \end{cases}$$

(5단계)

상점은 다음 식이 성립하는지 검사한 후 맞으면 요구하는 상품을 이용자에게 제공한다.

$g_1^{\upsilon}, g_2^{\omega} \stackrel{?}{=} g_1^{x_1}, g_2^{y_1}(g_1^{x_2}, g_2^{y_2})^{\alpha} \bmod P$

다. 결제단계

(1단계)

상점은 은행에게 이용자와 주고받은 모든 통신내용, C, α, υ, ω를 은행에 예치한다.

(2단계)

은행은 이중사용 여부를 확인한 후 전자화폐 C에 해당하는 현금을 상점계좌에 예치한다.

라. 이중사용자 검출

이용자가 만일 이중사용을 하게 되면 은행은 상점들의 다음과 같은

$$\begin{cases} \upsilon_1 = x_1 + \alpha_1\ x_2 \\ \upsilon_2 = x_1 + \alpha_2\ x_2 \end{cases} \qquad \begin{cases} \omega_1 = y_1 + \alpha_1\ y_2 \\ \omega_2 = y_1 + \alpha_2\ y_2 \end{cases}$$

거래정보로부터 (x_1, x_2), (y_1, y_2)를 구할 수 있다. 따라서, 식 (1)로부터 이중사용자의 계좌번호인 μ를 알게 되어 이중사용자를 검출한다.

〈참고문헌〉

[St95] W. Stallings, Network and Internetwork Security, Prentice Hall, 1995

[Br93a] S. Brands. "Untraceable off-line Cash in Wallets with Observers," Advances in Cryptology - Proceedings of Crypto '93, pp. 302-318

[Br93b] S. Brands. "An efficient off-line electronic cash system based on the representation problem." Technical Report CS-R9323, CWI, Amsterdam, 1993.

[Ch82] D. Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology - Proceedings of Crypto '82, pp. 199-203

[CFN88] D. Chaum, A. Fiat and M. Naor. "Untraceable Electronic Cash." Advances in

Cryptology – Proceedings of Crypto '88. pp.319–327
송유진, 이임영 공역, 현대암호, 생능출판사, 1999
송유진 외 5인 공저, 전자상거래 보안기술, 생능출판사, 2000
송유진, 주재훈 공저, 전자화폐 : 전자상거래 보안 응용, 동국대 출판부, 2001

TV애니타임 표준화 활기

서버 등 개인용 저장장치를 기반으로 자기가 원하는 방법으로 원하는 시간에 기존의 방송 서비스는 물론이고 온라인 대화형 동영상 서비스 등을 시청할 수 있는 TV애니타임(TV-Anytime) 서비스의 국제 표준화가 활발하게 이뤄지고 있어 이른 시일내에 서비스가 가능할 전망이다. 현재 전세계적으로 유럽 · 미국 · 아시아의 주요 방송사, 인터넷 방송사, 콘텐츠 제작업체, 가전업체, 통신사 등 150여 개 기관이 참여한 TV애니타임포럼이 결성돼 관련 기술표준을 제정 중이다. 여기에 우리나라에서도 한국전자통신연구원(ETRI)을 비롯, 삼성 · LG · 대우 등 가전 3사와 알티캐스트 · 휴맥스 등의 9개 업체가 회원사로 참여하고 있다. 하지만 국내 회원사들의 활동이 주로 표준화 동향파악 및 정보입수의 목적 위주로 진행되고 있는 데 반해 선진국은 활발한 활동을 펼치고 있어 이에 대한 적극적인 대응이 요구된다. 유럽의 방송사 및 가전업체를 중심으로 추진되던 것이 일본으로도 확산됐다. 일본은 방송사 · 가전사 · 통신서비스업체 등이 양방향 데이터 방송 및 방송콘텐츠 메타데이터에 기반한 TV애니타임 형태의 서비스 · 기술개발을 진행중이며 연구개발된 기술을 TV애니타임포럼에 표준규격으로 반영시키기 위한 움직임을 전개하고 있다. ATSC기반의 디지털방송 환경을 갖춘 미국 업체들도 초기에는 PVR(Personal Video Recoders) 업체들만 관심을 가졌으나 지난해부터 적극적인 관심과 기술기고 활동이 전개되고 있다. TV애니타임포럼은 현재 표준화 작업을 요구 규격과 기술표준 단계로 나뉘어 진행하고 있는데 요구 규격은 마무리됐으며 콘텐츠 보호관리(RMP:Right Management and Protection) 규격을 제외한 메타데이터(metadata), 콘텐츠 참조(content referencing), 시스템 기술(system description) 등의 기술표준 작업이 상당 부분 진행됐다. 지난 2월에는 단방향 방송서비스 모델에 기반한 버전 1.1 표준안이 발표됐으며, 상대적으로 진행상황이 늦었던 RMP도 표준 초안이 발표됐다. 앞으로 단방향 방송서비스 환경을 고려한 최종 표준 규격이 올해 하반기에 실질적으로 완성될 예정이며, 현재 양방향 네트워크 서비스와 휴대형 · 이동서비스 모델에 기반한 기술표준 관련 논의 및 표준 규격안 작업활동이 주요 이슈로 떠오르고 있다. 이에 따라 TV애니타임 국제표준 규격이 완성돼 서비스가 본격적으로 시행되면 관심 있는 프로그램과 정보를 시청자가 직접 검색 · 선택할 수 있으며, 개인의 취향 등에 맞춰진 지능형 또는 정보맞춤형 방송서비스가 가능할 것으로 예상된다.