(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0071221
(43) 공개일자 2011년06월29일

(51) Int. Cl.
H04L 9/32 (2006.01)
(21) 출원번호 10-2009-0127727
(22) 출원일자 2009년12월21일
심사청구일자 없음

(71) 출원인
한국전자통신연구원
대전 유성구 가정동 161번지
세종대학교산학협력단
서울 광진구 군자동 98 세종대학교
(72) 발명자
이윤경
대전광역시 유성구 관평동 898 대덕테크노밸리 꿈에그린 910-1202
이석준
대전광역시 유성구 용산동 대덕테크노밸리 우림필유 1207-1102
(뒷면에 계속)
(74) 대리인
특허법인지명

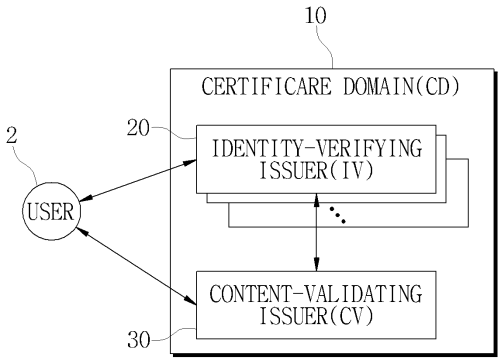
전체 청구항 수 : 총 1 항

(54) 실명 추적이 가능한 익명 인증서를 이용한 프라이버시 보호 방법

(57) 요 약

실명 추적이 가능한 익명 인증서를 이용한 프라이버시 보호 방법이 제공된다. 이 방법은 계정 검증 관리자로 접근하는 사용자에 대하여 신원을 확인하고 사용자에게 부분 인증서를 발급하는 단계; 사용자로부터 받은 부분 인증서에 상응하는 콘텐트를 확인하고 콘텐트에 대한 익명 인증서를 발급하는 단계; 사용자에게 서비스를 제공하는 서비스 제공자로부터 요청에 따라 콘텐트 인증 관리자가 계정 검증 관리자에게 익명 인증서를 사용하는 사용자의 추적을 요청함으로써 익명 인증서 또는 콘텐트를 추적 및 폐기하는 단계; 및 사용자에게 서비스를 제공하는 서비스 제공자로부터 요청에 따라 콘텐트 인증 관리자가 계정 검증 관리자에게 익명 인증서를 사용하는 사용자의 추적을 요청함으로써 익명 인증서에 상응하는 사용자의 신원을 파악하는 단계를 포함한다.

대 표 도 - 도1



(72) 발명자

황정연

경기도 수원시 권선구 세류2동 1108-7 대우연립 10동 201호

정병호

대전광역시 유성구 도룡동 391 타운하우스 7-203

조현숙

대전광역시 유성구 관평동 대덕테크노밸리 7단지 금성백조아파트 701-501

권태경

서울특별시 강남구 도곡동 아카데미스위트 3709

이 발명을 지원한 국가연구개발사업

과제고유번호 2008-F-036-02

부처명 지식경제부

연구관리전문기관

연구사업명 IT원천기술개발

연구과제명 익명성 기반의 u지식정보보호기술 개발

기여율

주관기관 세종대학교 산학협력단, 한국전자통신연구원

연구기간 2008.03.01 ~ 2012.02.29

특허청구의 범위

청구항 1

계정 검증 관리자와 콘텐트 인증 관리자를 포함한 인증 도메인에서 실명 추적이 가능한 익명 인증서를 이용하여 프라이버시를 보호하는 방법에 있어서,

상기 계정 검증 관리자로 접근하는 사용자에 대하여 신원을 확인하고 상기 사용자에게 부분 인증서를 발급하는 단계;

상기 사용자로부터 받은 상기 부분 인증서에 상응하는 콘텐트를 확인하고 상기 콘텐트에 대한 상기 익명 인증서를 발급하는 단계;

상기 사용자에게 서비스를 제공하는 서비스 제공자로부터 요청에 따라 상기 콘텐트 인증 관리자가 상기 계정 검증 관리자에게 상기 익명 인증서를 사용하는 상기 사용자의 추적을 요청함으로써 상기 익명 인증서 또는 상기 콘텐트를 추적 및 폐기하는 단계; 및

상기 사용자에게 서비스를 제공하는 서비스 제공자로부터 요청에 따라 상기 콘텐트 인증 관리자가 상기 계정 검증 관리자에게 상기 익명 인증서를 사용하는 상기 사용자의 추적을 요청함으로써 상기 익명 인증서에 상응하는 상기 사용자의 신원을 확인하는 단계를 포함하는

실명 추적이 가능한 익명 인증서를 이용한 프라이버시 보호 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 실명 추적이 가능한 익명 인증서를 이용하여 프라이버시를 보호하는 방법에 관한 것으로, 보다 상세하게는, 개인의 신분이 드러나지 않는 익명인증서를 발급하는 방법, 익명인증서 관리 구조, 익명인증서를 이용하여 온라인 서비스를 이용하는 사용자가 불법적인 행위를 한 경우 이 사용자의 신분을 확인하는 방법에 관한 것이다.

[0002] 본 발명은 지식경제부 IT원천기술개발 사업의 일환으로 수행한 연구로부터 도출된 것이다[과제관리번호: 2008-F-036-02, 과제명: 익명성 기반의 u지식정보보호기술 개발].

배 경 기 술

[0003] 최근 들어 대형 사이트가 해킹되어 수만 명의 개인정보가 유출되는 사건이 종종 발생하고 있다. 또한, 사이트 내부자의 실수 혹은 고의로 많은 사람의 개인정보가 유출되는 사건도 발생하고 있다.

[0004] 개인정보는 한 번 유출되면 되돌릴 수 있는 정보도 있지만, 대부분의 경우 되돌리기 힘들거나, 되돌리는 것이 불가능하다. 따라서, 서비스 제공자의 사이트에서 개인의 신분 정보를 직접 관리하지 않고, 익명성 기반의 인증 방법을 이용하여 서비스를 제공하다가, 필요한 경우 익명 사용자의 실제 신분을 확인할 수 있는 익명인증 방법이 필요하다.

발명의 내용

해결 하고자하는 과제

[0005] 본 발명의 목적은 온라인 상에서 개인의 프라이버시를 보호하되, 익명성을 오용 또는 남용하여 타인에게 피해를 줄 경우 해당 사용자의 신분을 확인할 수 있는 방법을 제공함에 있다.

[0006] 또한, 본 발명의 목적은 실명 추적이 가능한 익명 인증서를 이용하여 프라이버시를 보호하는 방법을 제공함에 있다. 특히, 개인의 신분이 드러나지 않는 익명인증서를 발급하는 방법, 익명인증서 관리 구조, 익명인증서를 이용하여 온라인 서비스를 이용하는 사용자가 불법적인 행위를 한 경우 이 사용자의 신분을 확인하는 방법을 제

공함에 있다.

과제 해결수단

[0007] 상기 기술적 과제를 해결하기 위하여 본 발명의 일 측면에 따르면, 계정 검증 관리자와 콘텐트 인증 관리자를 포함한 인증 도메인에서 실명 추적이 가능한 익명 인증서를 이용하여 프라이버시를 보호하는 방법에 있어서, 계정 검증 관리자로 접근하는 사용자에 대하여 신원을 확인하고 사용자에게 부분 인증서를 발급하는 단계; 사용자로부터 받은 부분 인증서에 상응하는 콘텐트를 확인하고 콘텐트에 대한 익명 인증서를 발급하는 단계; 사용자에게 서비스를 제공하는 서비스 제공자로부터 요청에 따라 콘텐트 인증 관리자가 계정 검증 관리자에게 익명 인증서를 사용하는 사용자의 추적을 요청함으로써 익명 인증서 또는 콘텐트를 추적 및 폐기하는 단계; 및 사용자에게 서비스를 제공하는 서비스 제공자로부터 요청에 따라 콘텐트 인증 관리자가 계정 검증 관리자에게 익명 인증서를 사용하는 사용자의 추적을 요청함으로써 익명 인증서에 상응하는 사용자의 신원을 파악하는 단계를 포함하는 실명 추적이 가능한 익명 인증서를 이용한 프라이버시 보호 방법이 제공된다.

[0008] 본 발명의 또 다른 측면에 따르면, 익명 인증서(TAC)를 발급 및 관리하는 주체인 인증 도메인(CD: Certificate Domain)은 Identity-Verifying Issuer(IV)와 Content-Validating Issuer(CV)로 구성되어 있고, TAC의 발급 및 검증, 실명추적(trace), revoke 과정은 이들 IV와 CV의 협력에 의해서 이루어지는 인명인증서 발급 및 관리 방법이 제공된다.

[0009] CV는 실명인증서 발급구조에서의 CA(Certificate Authority)에 대응되고, IV는 RA(Registration Authority)에 대응되며, TAC는 X.509 기반의 익명 인증서일 수 있다.

[0010] 하나의 CD는 여러 개의 IV를 가질 수 있다. 그리고, 모든 TAC의 발급 및 검증, 실명추적(trace), revoke 과정은 IV와 CV의 협업에 의해 수행되며, IV와 CV의 권한이 분산되어 있을 수 있다. 이 경우, 사용자의 프라이버시가 더욱 확실히 보장될 수 있다.

[0011] 익명인증서 발급 및 관리 방법은 IV는 사용자의 실제 identity를 확인하고, half certified TAC를 사용자에게 발급하고, 사용자가 half certified TAC를 CV에 전송하면, CV는 half certified TAC의 내용을 확인하고, 사용자가 실제 사용 가능한 TAC를 발급하도록 이루어질 수 있다.

[0012] IV와 CV는 각각 자신의 정책에 따라서, TAC에 추가적인 내용을 첨부할 수 있다.

[0013] 익명인증서 발급 및 관리 방법은 사용자가 TAC를 오용 또는 남용하는 것을 SP가 인지할 경우, SP는 이를 CV에게 알리고, CV는 IV의 도움을 받아서 해당 TAC 소유자의 실제 identity를 추적할 수 있다.

[0014] 익명인증서 발급 및 관리 방법은 TAC 관리를 위하여 실명 인증서 관리에 사용하는 방법인 CRL(Certificate Revocation List) 혹은 OCSP(Online Certificate Status Protocol)를 적용할 수 있다.

[0015] 본 발명의 또 다른 측면에 따르면, 사용자가 TAC의 초기 내용을 구성하되, TAC의 내용은 X.509 기반 인증서의 내용에 바탕을 두어 m = <version, serial number, pseudonym, pk_{PN}, …> 등이 들어가고, pseudonym 으로는 “anonymous” 혹은 사용자가 원하는 어떠한 pseudonym도 가능하지만, 이러한 pseudonym PN은 TAC를 구분지을 수 있는 값으로써 하나의 certificate domain(CD)내에서 유일한 값이어야 하며, 사용자가 새로운 서명 키 쌍 <pk_{PN}, sk_{PN}>을 생성하는 것을 특징으로 하는 TAC 구조가 제공된다.

[0016] 또한, 본 발명의 또 다른 측면에 따르면, 사용자가 blinding factor b를 생성하되, b를 해쉬한 후에 e 멱승을 하여($u = H_1(m) \cdot H_2(b)^e$), CV 혹은 IV에게 전달함으로써, CV와 IV의 공모로 인해 사용자가 피해를 보지 않도록 하는 것을 특징으로 하는 TAC 발급 방법이 제공된다.

[0017] 본 발명의 또 다른 측면에 따르면, 사용자가 자신의 비밀키 sk_{UN}을 이용하여 $u = H_1(m) \cdot H_2(b)^e$ 인 u에 대해서 자신의 서명 c_1을 생성하고, 이를 이용하여 IV에게 줄 digital envelope <δ_1, η_1>을 생성하되, $\delta 1$은 사용자와 IV 사이의 세션키 k_1을 IV의 공개키로 암호화한 값이고, η_1은 사용자가 IV에게 전송하고자 하는 내용인 (u, c_1, Θ)를 세션키 k_1으로 암호화한 값인 것을 특징으로 하는 half certified TAC 발급 방법이 제공된다.

[0018] 본 발명의 또 다른 측면에 따르면, IV는 $\omega = u^{d1} \bmod N$을 연산하고, 필요하다면 CD의 policy에 따라서 policy-based filter α를 생성하고, <ω, α>를 CV의 공개키를 이용하여 암호화 하고($v_0 = \varepsilon_{pkCV}(\omega, \alpha)$), 세션 키 k1

으로 또한 암호화($v_1 = E_{k1}(v_0)$) 하는 것을 특징으로 하는 half certified TAC 발급 방법이 제공된다.

[0019] 본 발명의 또 다른 측면에 따르면, IV가 익명성을 오/남용 하는 사용자를 trace 하고 revoke 할 때 이용하기 위해서 (ω, $M_{kIV}(UN)$, $\varepsilon_{pkIV}(c_1*, \Theta)$)으로 구성된 trace transcript $T_1=<\omega, M_{kIV}(UN), \varepsilon_{pkIV}(c_1*, \Theta)>$을 생성하여 저장하는 것을 특징으로 하는 TAC 발급 방법이 제공된다.

[0020] 본 발명의 또 다른 측면에 따르면, Half certified TAC를 발급받은 사용자가 대칭 암호화키 k_2를 랜덤하게 생성하고, 자신의 pseudonym PN에 대한 키 쌍 SK_{PN}과 PK_{PN}을 생성 후, SK_{PN}을 이용하여(b, v_0, m)에 대해 서명 c_2를 생성한 후, CV에게 줄 digital envelope $<\delta_2, \eta_2>$을 생성하되, $\delta 2=\varepsilon_{pkCV}(k_2)$ 이고, $\eta_2= E_{k2}(b, v_0, m, c_2)$인 것을 특징으로 하는 TAC 생성 방법이 제공된다.

[0021] 본 발명의 또 다른 측면에 따르면, CV가 δ_2를 복호화 하여($D_{skCV}(\delta_2)$) k_2를 찾고, 이를 이용하여 η_2을 복호화($D_{k2}(\delta_2)$)하여 < b, v_0, m, c_2 >를 얻게 되며, 또한 자신의 비밀키로 v_0를 복호화 하여($D_{skCV}(v_0)$) $<\omega, \alpha>$를 얻고, 이를 이용하여 $Z= \omega^{d2} \bmod \cdot N$ 을 연산한 후 $H_1(m) \cdot H_2(b)^e = Z^e \bmod \cdot N$이 되는지를 확인한 후, CV는 m으로부터 PK_{PN}을 얻고, 이를 이용하여 $P_2(m, \alpha)=1$이고 $V_{PKPN}(<b, v_0, m>, c_2)=1$인지를 검증하여, 검증이 성공할 경우, 사용자에게 $v_2 (=k_2(z))$를 전송하고, v_2를 받은 사용자는, 세션키 k_2로 v_2를 복호화 하여($D_{k2}(v_2)$) z를 얻고, $z \cdot H_2(b)^{-1} \bmod N$을 연산하여 σ를 얻으며, 사용자가 CD의 RSA 서명과 $H_1(m)=\sigma^e \bmod \cdot N$을 비교하여 검증하고, 검증이 실패하면 현재 세션을 종료하고, 검증이 성공하면 $<m, \sigma>$로 구성된 TAC를 얻은 후 세션을 종료하는 것을 특징으로 하는 TAC 발급 방법이 제공된다.

[0022] 본 발명의 또 다른 측면에 따르면, CV가 익명성을 오/남용 하는 사용자를 trace 하고 revoke 할 때 이용하기 위해서 $<\omega, M_{kCV}(PN), \varepsilon_{pkCV}(c_2*, m)>$으로 구성된 trace transcript $T_2=<\omega, M_{kCV}(PN), \varepsilon_{pkCV}(c_2*, m)>$를 저장하는 것을 특징으로 하는 TAC 발급 방법이 제공된다.

[0023] 본 발명의 또 다른 측면에 따르면, 사용자가 하나의 half certified TAC를 이용하여 여러 개의 TAC를 발급받을 수 있고, 발급받은 TAC를 이용하여 SP가 제공하는 서비스를 익명으로 이용할 수 있는 것을 특징으로 하는 TAC 발급 시스템이 제공된다.

[0024] 본 발명의 또 다른 측면에 따르면, 사용자가 익명성을 오/남용할 경우, 해당 사용자를 revoke하고, trace 하기 위해서, CV는 PN에 대한 MAC을 계산하고, 이 MAC값을 이용하여 해당 trace transcript $T_2 = <\omega, M_{kCV}(PN), \varepsilon_{pkCV}(c_2*, m)>$를 찾아낸 후, 안전한 채널을 이용하여 IV에게 ω를 전송하면, ω를 받은 IV는 ω를 이용하여 자신이 가진 trace transcripts에서 해당 $T_1 = <\omega, M_{kIV}(UN), \varepsilon_{pkIV}(c_1*, \Theta)>$을 찾고, $\varepsilon_{pkIV}(c_1*, \Theta)$을 복호화 하여 Θ를 얻으면, 이로부터 UN을 알게 되고, CV와 IV가 해당 사용자의 서명 $<c_1*, c_2*>$으로부터 사용자의 <UN,PN>을 trace 할 수 있는 것을 특징으로 하는 TAC 발급 및 관리 방법이 제공된다.

[0025] 본 발명의 또 다른 측면에 따르면, 특정 UN을 사용하는 사용자가 가진 모든 TAC를 revoke 하고자 할 때, IV는 UN에 대한 MAC을 계산하고, 이를 이용하여 모든 trace transcripts $T_{1i}=<\omega_i, M_{kIV}(UN), \varepsilon_{pkIV}(c_{1i}*, \Theta)>$를 찾아낸 후, 찾아낸 transcripts로부터 $<\omega_1, \cdots, \omega_n>$을 안전한 채널을 이용하여 CV로 전송하면, CV는 ω_i, $1 \le i \le n$에 해당하는 모든 Transcripts $T_{2i}=<\omega_i, M_{kCV}(PN_i), \varepsilon_{pkCV}(c_{2i}*, m_i)>$를 찾아내며, CV는 transcripts에서 $\varepsilon_{pkCV}(c_{2i}*, m_i)$, $1 \le i \le n$을 모두 복호화 하여 PNs를 찾아냄으로써, IV와 CV가 $<UN, PN_1, \cdots, PN_n>$에 해당하는 사용자를 trace 할 수 있고, 따라서 해당 TAC들을 revoke 할 수 있는 것을 특징으로 하는 TAC 발급 및 관리 방법이 제공된다.

[0026] 본 발명의 또 다른 측면에 따르면, 사용자가 blinding factor b를 생성하되, b를 MAC 키로 사용하여 인증서 내용 m에 대한 MAC 계산을 하여 CV혹은 IV에게 전달함으로써, CV와 IV의 공모로 인해 사용자가 피해를 보지 않도록 하는 것을 특징으로 하는 TAC-MAC 발급 방법이 제공된다.

[0027] 본 발명의 또 다른 측면에 따르면, 사용자가 자신의 비밀키 sk_{UN}을 이용하여 $u=M_b(m)$인 u에 대해서 자신의 서명 c_1을 생성하고, 이를 이용하여 IV에게 줄 digital envelope $<\delta_1, \eta_1>$을 생성하되, $\delta 1$은 사용자와 IV 사이의 세션키 k_1을 IV의 공개키로 암호화한 값이고, η_1은 사용자가 IV에게 전송하고자 하는 내용인 (u, c_1, Θ)를 세션키

k_1으로 암호화한 값인 것을 특징으로 하는 half certified TAC-MAC 발급 방법이 제공된다.

[0028] 본 발명의 또 다른 측면에 따르면, IV는 자신의 비밀키 sk_{IV}를 이용하여 u=M_b(m)인 u에 대해서 자신의 서명 w를 생성하고, 필요하다면 CD의 policy에 따라서 policy-based filter α를 생성하고, <ω, α>를 CV의 공개키를 이용하여 암호화 하고($v_0=\varepsilon_{pkCV}(\omega, \alpha)$), 세션 키 k1으로 또한 암호화($v_1=E_{k1}(v_0)$) 하는 것을 특징으로 하는 half certified TAC-MAC 발급 방법이 제공된다.

[0029] 본 발명의 또 다른 측면에 따르면, CV가 δ_2를 복호화 하여($D_{skCV}(\delta_2)$) k_2를 찾고, 이를 이용하여 η_2을 복호화($D_{k2}(\delta_2)$)하여 <b, v_0, m, c_2>를 얻게 되며, 또한 자신의 비밀키로 v_0를 복호화 하여($D_{skCV}(v_0)$) <ω, α>를 얻고, 이를 이용하여 u=M_b(m)인 u를 계산한 후, w가 u에 대한 IV의 서명이 맞는지 확인한 후, CV는 m으로부터 PK_{PN}을 얻고, 이를 이용하여 P_2(m, α)=1이고 V_{PKPN}(<b, v_0, m>, c_2)=1인지를 검증하며, 검증이 성공할 경우, 필요한 경우 추가 내용 β를 생성하여 m의 내용에 추가한 후, CD의 비밀키 sk_{CD}를 이용하여 m에 대하여 CD의 서명 σ를 생성한 후, 사용자에게 v_2 (=Ek_2(σ, β))를 전송하고, v_2를 받은 사용자는, 세션키 k_2로 v_2를 복호화($D_{k2}(v_2)$) 하여 σ와 β를 얻고, 자신이 생성했던 m의 내용에 β를 추가한 후, 사용자가 σ가 CD의 m에 대한 서명인지 검증하고, 검증이 실패하면 현재 세션을 종료하고, 검증이 성공하면 <m, σ>로 구성된 TAC를 얻은 후 세션을 종료하는 것을 특징으로 하는 TAC 발급 방법이 제공된다.

효 과

[0030] 본 발명에 따르면, 실명 추적이 가능한 익명 인증서(TAC)를 이용하여 프라이버시를 보호함으로써, 개인의 신분을 노출하지 않으면서 자유롭게 온라인 서비스를 이용할 수 있다. 또한, 온라인 상에서 익명성의 오용 또는 남용으로 타인에게 피해를 주는 행위를 하는 사용자의 신분을 추적할 수 있고, 그에 의해 익명성 제공에 따른 폐해를 막을 수 있다.

[0031] 또한, SP가 개인정보를 수집할 필요가 없으므로 개인정보 유출의 문제가 발생하지 않고, 개인의 신분이 드러나지 않는 TAC를 이용하여 온라인 서비스 이용시 인증을 받게 되므로 프라이버시를 보호할 수 있다는 장점과 기존 X.509 사용 환경에서 이용 가능하다는 장점이 있다.

발명의 실시를 위한 구체적인 내용

[0032] 이하, 첨부한 도면들 및 후술되는 내용을 참조하여 본 발명의 바람직한 실시예들을 상세히 설명한다. 그러나, 본 발명은 여기서 설명되는 실시예들에 한정되지 않고 다른 형태로 구체화될 수도 있다. 오히려, 여기서 소개되는 실시예들은 개시된 내용이 철저하고 완전해질 수 있도록 그리고 당업자에게 본 발명의 사상이 충분히 전달될 수 있도록 하기 위해 제공되는 것이다. 명세서 전체에 걸쳐서 동일한 참조번호들은 동일한 구성요소들을 나타낸다. 한편, 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급되지 않는 한 복수형도 포함된다. 명세서에서 사용되는 용어 "포함한다(comprise)" 및/또는 "포함하는(comprising)"은 언급된 구성요소, 단계, 동작 및/또는 소자가 하나 이상의 다른 구성요소, 단계, 동작 및/또는 소자의 존재 또는 추가를 배제하지 않는다.

[0033] 도 1은 본 발명의 실시예에 따른 익명성 보장을 위한 TAC 발급 기관에 대한 개략적인 구성도이다.

[0034] 도 1을 참조하면, 실명추적이 가능한 익명 인증서(traceable anonymous certificate; TAC)를 발급 및 관리하는 주체인 인증 도메인(certificate domain; CD)(10)은 계정 검증 관리자(identity verifying issuer; IV)(20)와 콘텐트 인증 관리자(content validating issuer; CV)(30)를 구비한다.

[0035] 콘텐트 인증 관리자(30)는 실명인증서 발급 구조에서의 인증기관(certificate authority; CA)에 대응되고, 계정 검증 관리자(20)는 등록기관(registration authority; RA)에 대응된다고 할 수 있다. 인증 도메인(10)은 복수의 계정 검증 관리자(20)를 구비할 수 있다. 실명인증서 발급 구조는 공개키 기반 구조(public key infrastructure; PKI)에서 사용하는 표준 인증서 형식, 예컨대, X.509 인증서를 포함한다.

[0036] TAC를 발급받는 과정을 간략히 설명하면 다음과 같다.

[0037] 먼저, 계정 검증 관리자(20)는 사용자의 실제 신원(identity)을 확인하고, 부분적으로 인증된 TAC(half certified TAC)(이하, 부분 TAC라고 함)를 발급한다. 이때, 계정 검증 관리자(20)는 자신의 정책에 따라서 사용

자의 신원을 확인하고, 그 결과를 부분 TAC에 반영할 수 있다.

[0038] 여기서, 사용자는 유무선 통신망, 인터넷, 케이블 통신망 등을 통해 인증 도메인(10)에 접근할 수 있는 사용자 단말을 포함한다.

[0039] 그 후, 사용자가 부분 TAC를 콘텐트 인증 관리자(30)에 전송하면, 콘텐트 인증 관리자(30)는 부분 TAC의 내용을 확인하고, 사용자에게 실제 사용 가능한 TAC를 발급한다. 이때, 콘텐트 인증 관리자(30)는 자신의 정책에 따라서 부분 TAC를 확인하고, 필요한 경우 부분 TAC의 내용을 업데이트한 후, 사용자가 실제 사용할 수 있는 TAC를 발급할 수 있다.

[0040] 본 실시예에서, TAC는 X.509 인증서 구조를 따른다. 따라서, TAC에는 인증서 내용에 대한 서명이 포함된다. 이때, 인증 도메인(10)의 비밀키를 이용하여 TAC 내용에 대한 서명이 이루어진다. 그리고, TAC의 순서 번호(serial number)는 중복되지 않는 범위 내에서 랜덤 값을 이용할 수 있다.

[0041] TAC 발급 과정에서 계정 검증 관리자(20)가 사용자의 실제 신원을 확인하는 방법은 실명 인증서를 이용하여 온라인으로 확인하는 방법과, 오프라인으로 사용자의 신분증을 이용하여 확인하는 방법의 두 가지 중 하나를 이용할 수 있다.

[0042] 만약, 사용자가 TAC를 오용 또는 남용하는 것을 서비스 제공자(service provider; SP)가 인지하는 경우, 서비스 제공자는 이를 콘텐트 인증 관리자(30)에게 알린다. 그러면, 콘텐트 인증 관리자(30)는 계정 검증 관리자(20)의 도움을 받아서 해당 TAC 소유자의 실제 신원을 추적할 수 있다.

[0043] 또한, TAC 관리를 위하여 실명 인증서 관리에 사용하는 방법인 인증서 폐기 목록(certificate revocation list; CRL) 혹은 온라인 인증서 상태 프로토콜(online certificate status protocol; OCSP)를 적용할 수 있다.

[0044] 도 2는 본 발명의 일 실시예에 따른 TAC 생성 방법을 설명하기 위한 도면이다.

[0045] 도 1 및 도 2를 참조하면, 사용자(User)는 인증 도메인(10) 내에 있는 콘텐트 인증 관리자(30)와 계정 검증 관리자(20)에게 자신을 증명하고, 익명인증서 TAC를 발급받는 과정을 포함한다.

[0046] 사용자는 자신의 실제 신분을 나타내는 인증서 Θ를 갖고 있거나, 오프라인으로 자신을 증명하기 위해서 계정 검증 관리자(20)를 직접 대면하여야 한다. 인증서 Θ는 서명키 쌍(pk_{UN}, sk_{UN})에 대해서 인증기관이 발급한 것이다.

[0047] 계정 검증 관리자(20)와 콘텐트 인증 관리자(30)는 자신들의 공개키 쌍인 $<pk_{IV}, sk_{IV}>$와 $<pk_{CV}, sk_{CV}>$를 각각 소유하고 있으며, 이들 공개키 쌍은 각각 인증기관에 의해서 확인되어야 한다.

[0048] 계정 검증 관리자(20)와 콘텐트 인증 관리자(30)는 동일한 공개키 <e, N>을 공유한다. 그리고, 비밀 지수(private exponent) d를 최소 두 개로 나누어 공유하고, 이들 각각을 d_1과 d_2라고 한다. 즉, 계정 검증 관리자(30)가 d_1을, 콘텐트 인증 관리자(30)가 d_2를 소유하면, $d=d_1d_2 \bmod \phi(N)$이다.

[0049] 또한, 여러 개의 계정 검증 관리자들(20)을 이용하게 되면, 문턱 전자 서명 기법(threshold digital signature scheme)을 적용할 수 있다.

[0050] 계정 검증 관리자(20)와 콘텐트 인증 관리자(30)는 각각 자신의 MAC 키(message authentication code key)인 k_{IV}와 k_{CV}를 소유하고 있다.

[0051] 전술한 기본 가정하에서, TAC를 생성하는 방법은 다음과 같다.

[0052] 설명의 편의를 위해서, 도 2의 각 단계를 각각 step 1-1(user ⇒ IV), step 1-2(IV ⇒ user), step 2-1(user ⇒ CV), step 2-2(CV ⇒ user)로 표현하고자 한다.

[0053] (1) Step 1-1 (User ⇒ IV : $<\delta_1, \eta_1>$)

[0054] 사용자(User)는 TAC의 내용을 구성한다. TAC의 내용으로는, m = <version, serial number, pseudonym, pk_{PN}, …> 등이 들어가고, 대화명 또는 필명(pseudonym)으로는 "anonymous" 혹은 사용자가 원하는 어떠한 필명도 가능하다. 그리고, 새로운 서명키 쌍, $<pk_{PN}, sk_{PN}>$을 생성한다.

[0055] 이때, 사용자 필명 식별자(user's pseudonymous identifier)로써의 PN(pseudo noise)은 TAC를 구분 지을 수 있

는 값으로써 하나의 인증 도메인 내에서 유일한 값이어야 한다. 그래서, PN 값으로는 주로 랜덤 시리얼 넘버와 서명키 쌍의 값들을 이용한다.

[0056] 사용자는 블라인딩 팩터(blinding factor) b를 생성하고, 대칭 암호화 키(symmetric encryption key)인 k_1을 랜덤으로 생성한다. 그리고, 사용자는 $u=H_1(m)\cdot H_2(b)^e \bmod N$을 연산한 후, 자신의 비밀키 sk_{UN}을 이용하여 결과 값 u에 대한 자신의 서명 c_1을 생성한다. 이를 이용하여, 사용자는 계정 검증 관리자(IV, 20)에게 줄 전자 봉투(digital envelope) $<\delta_1, \eta_1>$을 생성한다. 이때, $\delta_1=\varepsilon_{pkIV}(k_1)$이고, $\eta_1=E_{k1}(u,c_1,\Theta)$이다. 생성한 전자 봉투 $<\delta_1, \eta_1>$은 계정 검증 관리자(20)에게 전송된다. 여기서, η_1은 사용자가 계정 검증 관리자(20)에게 전송하고자 하는 내용인 (u,c_1,Θ)를 세션키 k_1으로 암호화한 값이다.

[0057] 전자 봉투 $<\delta_1, \eta_1>$을 받은 계정 검증 관리자(20)는 δ_1을 복호화($D_{skIV}(\delta_1)$)하여 k_1을 알아낸다. 그리고, k_1을 이용하여 η_1을 복호화($D_{k1}(\delta_1)$)하여 $<u,c_1,\Theta>$를 얻는다.

[0058] 계정 검증 관리자(20)는 인증서 Θ를 이용하여 $P1(\Theta)=1$이고, $V_{pkUN}(u,c_1)=1$인지를 검증한다. 즉, 사용자의 실제 신분을 나타내는 인증서 Θ를 이용하여 해당 사용자가 인증 도메인의 정책(policy)에 적합한 사람인지 여부를 판단하고, 해당 사용자의 공개키 pk_{UN}을 이용하여 u에 대한 사용자의 서명 c_1을 검증한다. 인증 도메인의 정책에 적합한 사람이라면 $P1(\Theta)=1$이 된다. 서명 검증이 성공하면, $V_{pkUN}(u,c_1)=1$이 된다. 그리고 서명 검증이 실패하면, 계정 검증 관리자(20)는 현재 세션을 종료한다.

[0059] (2) Step 1-2 (IV ⇒ User: v_1)

[0060] 서명 검증이 성공할 경우, 계정 검증 관리자(IV, 20)는 $\omega=u^{d1} \bmod N$을 연산하고, 필요하다면 인증 도메인(10)의 정책에 따라서 정책 기반 필터(policy-based filter) α를 생성한다. 그 후, 계정 검증 관리자(20)는 $<\omega, \alpha>$를 콘텐트 인증 관리자(30)의 공개키를 이용하여 암호화($v_0=\varepsilon_{pkCV}(\omega, \alpha)$)하고, 또한 세션 키 k_1으로 암호화($v_1=E_{k1}(v_0)$)한다. 계정 검증 관리자(20)는 결과값 v_1을 사용자에게 전송한다. 또한, 계정 검증 관리자(20)는 추적 기록(trace transcript) $T_1=<\omega, M_{kIV}(UN), \varepsilon_{pkIV}(c_1*, \Theta)>$을 생성하여 저장한다. 이때, $M_{kIV}(UN)$은 UN(User's real identifier)에 대해서 계정 검증 관리자(20)의 MAC 키 k_{IV}를 이용하여 생성한 MAC 값을 의미한다.

[0061] (3) Step 2-1 (User ⇒ CV : $<\delta_2, \eta_2>$)

[0062] 사용자는 대칭 암호화 키 k_2를 랜덤하게 생성하고, $S_{skPN}(b, v_0, m)$에서 가명 또는 필명 서명(pseudonymous signature) c_2를 얻는다. 사용자는 콘텐트 인증 관리자(30)에게 줄 전자 봉투 $<\delta_2, \eta_2>$를 생성한다. 이때, $\delta_2=\varepsilon_{pkCV}(k_2)$이고, $\eta_2=E_{k2}(b, v_0, m, c_2)$이다. 생성된 전자 봉투 $<\delta_2, \eta_2>$는 콘텐트 인증 관리자(30)에게 전송된다.

[0063] 전자 봉투를 받은 콘텐트 인증 관리자(CV, 30)는 δ_2를 복호화($D_{skCV}(\delta_2)$)하여 k_2를 찾고, 이를 이용하여 η_2를 복호화($D_{k2}(\delta_2)$)하여 $<b, v_0, m, c_2>$를 얻는다. 또한, 콘텐트 인증 관리자(30)는 자신의 비밀키로 v_0를 복호화($D_{skCV}(v_0)$)하여 $<\omega, \alpha>$를 얻는다. 그리고, 이를 이용하여 $Z=\omega^{d2} \bmod N$을 연산하고, $H_1(m)\cdot H_2(b)^e=Z^e \bmod N$이 되는지를 확인한다. 또한, 콘텐트 인증 관리자(30)는 m으로부터 PK_{PN}을 얻고, 이를 이용하여 $P_2(m, \alpha)=1$이고 $V_{PKPN}(<b, v_0, m>, c_2)=1$인지를 검증한다. 여기서, PK_{PN}은 필명(pseudonym) PN을 사용하는 사용자의 공개키를 칭한다. 만약, 검증이 실패한다면, 콘텐트 인증 관리자는 현재 세션을 종료하게 된다.

[0064] (4) Step 2-2 (CV ⇒ user : v_2)

[0065] 검증이 성공하면, 콘텐트 인증 관리자(30)는 사용자에게 $v_2(=k_2(z))$를 전송한다. 콘텐트 인증 관리자(30)는 이 세션에 대한 추적 기록(trace transcript) $T_2=<\omega, M_{kCV}(PN), \varepsilon_{pkCV}(c_2*, m)>$를 저장한다. 이때, $M_{kCV}(PN)$는 PN에 대한 MAC 값을 의미하고, PN은 m으로부터 얻을 수 있다.

[0066] v_2를 받은 사용자는 세션키 k_2로 v_2를 복호화($D_{k2}(v_2)$)하여 z를 얻고, $z\cdot H_2(b)^{-1} \bmod N$을 연산하여 σ를 얻는

다. 따라서, 사용자는 인증 도메인의 RSA 서명과 $H_1(m)=\sigma^e \bmod \cdot N$을 비교하여 검증한다. 그리고, 사용자는 검증이 실패하면 현재 세션을 종료하고, 검증이 성공하면 <m, σ>로 구성된 TAC를 얻은 후 세션을 종료한다.

[0067] 상기 단계(step) 2-1과 2-2를 여러 번 반복하여 사용자는 여러 개의 TAC를 발급받을 수 있고, 발급받은 TAC를 이용하여 서비스 제공자가 제공하는 서비스를 익명으로 이용할 수 있다.

[0068] 한편, 사용자가 익명성을 남용한다면, 서비스 제공자는 사용자 계정 또는 콘텐트의 폐기(revocation)를 인증 도메인(10)에 요청할 수 있고, 해당 사용자가 익명성을 남용한 증거와 함께 TAC에서 얻은 PN을 콘텐트 인증 관리자(30)에게 제출하여 해당 사용자의 실명을 찾을 수 있다. 이러한 과정을 폐기(revocation)와 실명추적 또는 간단히 추적(trace)이라고 부르는데, 추적 및 폐기(trace and revocation) 방법은 다음과 같다.

[0069] (1) Step 3-1 (CV ⇒ IV : ω)

[0070] 콘텐트 인증 관리자(30)는 PN에 대한 MAC을 계산하고, 이 MAC 값을 이용하여 해당 추적 기록(trace transcript) $T_2=<\omega, M_{kCV}(PN), \varepsilon_{pkCV}(c_2^*, m)>$를 찾아낸다. 그리고, 콘텐트 인증 관리자(30)는 계정 검증 관리자(20)에게 추적(trace) 혹은 폐기(revocation)를 요청하기 위해서 안전한 채널을 이용하여 ω를 전송한다.

[0071] ω를 받은 계정 검증 관리자는 ω를 이용하여 자신이 가진 추적 기록에서 해당 $T_1=<\omega, M_{kIV}(UN), \varepsilon_{pkIV}(c_1^*, \Theta)>$을 찾는다. 계정 검증 관리자(20)는 $\varepsilon_{pkIV}(c_1^*, \Theta)$을 복호화하여 Θ를 얻고, 이로부터 UN을 알게 된다. 그러면, 콘텐트 인증 관리자와 계정 검증 관리자는 해당 사용자의 서명 $<c_1^*, c_2^*>$으로부터 사용자의 <UN,PN>을 추적할 수 있다.

[0072] 또한, 특정 UN을 사용하는 사용자가 가진 모든 TAC를 폐기하고자 한다면 다음의 단계 3-2를 이용하면 된다.

[0073] (2) Step 3-2 (IV ⇒ CV : $<\omega_1, \omega_n>$)

[0074] 계정 검증 관리자(20)는 UN에 대한 MAC을 계산하고, 이를 이용하여 모든 추적 기록 $T_{1i}=<\omega_i, M_{kIV}(UN), \varepsilon_{pkIV}(c_{1i}^*, \Theta)>$를 찾아낸다. 찾아낸 기록(transcripts)으로부터 얻은 $<\omega_1, \cdots, \omega_n>$을 안전한 채널을 이용하여 콘텐트 인증 관리자(30)로 전송하면, 콘텐트 인증 관리자(30)는 ω_i, $1 \le i \le n$에 해당하는 모든 기록 $T_{2i}=<\omega_i, M_{kCV}(PN_i), \varepsilon_{pkCV}(c_{2i}^*, m_i)>$를 찾아낸다. 또한, 콘텐트 인증 관리자(30)는 추적 기록에서 $\varepsilon_{pkCV}(c_{2i}^*, m_i)$, $1 \le i \le n$을 모두 복호화하여 PNs를 찾아내고, 계정 검증 관리자(20)와 콘텐트 인증 관리자(30)는 $<UN, PN_1 \cdots PN_n>$에 해당하는 사용자를 추적할 수 있고, 따라서 해당 TAC들을 폐기할 수 있다.

[0075] 본 실시예에 따르면, 블라인딩 팩터 b를 해쉬한 후에 e 멱승을 함($u=H_1(m) \cdot H_2(b)^e$)으로써, 콘텐트 인증 관리자(30)와 계정 검증 관리자(20)의 공조로 사용자가 피해를 보지 않도록 할 수 있다.

[0076] 위에서 설명한 실시예에 있어서, TAC를 발급받고, TAC를 이용하는 사용자의 실명을 찾아내고, 사용자가 익명성을 오용 또는 남용할 경우 해당 사용자의 TAC를 폐기하는 방법을 좀 더 확장할 수 있다.

[0077] 즉, 또 다른 실시예에서는 TAC의 생성시 split-RSA 서명을 이용하지 않고 TAC를 증명(certify)하기 위해서 또 다른 서명구조 시그마(Σ)를 이용할 수 있다. 그 경우, $\Sigma=S_{skCD}(m)$이고, $<pk_{CD}, sk_{CD}>$를 이용하여 서명을 수행한다. 또한, split-RSA 서명을 이용하지 않기 때문에, 콘텐트 인증 관리자(30)는 인증서를 완성하기 전에 m의 내용을 컨트롤할 수 있다. 따라서, 인증 도메인의 정책에 따라서 m에 다양한 필드를 추가할 수 있는 장점이 있다.

[0078] 예컨대, 인증 도메인의 정책 β에 따라서 변경된 m은 $m \leftarrow <m, \beta>$으로 표현할 수 있다. 이와 같은 방법을 이용하는 TAC 생성 프로토콜을 앞의 방법을 이용하여 TAC를 생성하는 프로토콜 TAC-RSA에 대해서 TAC-MAC이라 기술한다.

[0079] 도 3은 본 발명의 또 다른 일 실시예에 따른 TAC-MAC 생성 방법을 설명하기 위한 도면이다.

[0080] 도 3을 참조하면, TAC-MAC에서는 TAC-RSA 프로토콜에서 b를 해쉬하여 이용하는 대신 $u \leftarrow M_b(m)$으로 표현되는 MAC-and-sign 방식을 이용한다. 이때, 임의 사용자의 서명 $\sigma'=S_{UN}(m')$에 대해서, 계정 검증 관리자(IV, 20)와 콘텐트 인증 관리자(CV, 30)가 공모를 하더라도 임의의 TAC 내용인 m과 추적 기록 T_1, T_2에 대해서 $m'=M_b(m)$을

만족하는 b를 찾을 수 없으므로 사용자에게 피해를 줄 수 없다.

[0081] 전술한 실시예들에 따르면, 계정 검증 관리자(IV)와 콘텐트 인증 관리자(CV)를 통해 개인의 신분을 드러내지 않고, 온라인 환경에서 인증을 받고, 서비스를 이용할 수 있는 인증구조 및 추적 가능한 익명 인증서(traceable anonymous certificate; TAC)의 발급 및 관리, 사용자의 실명 추적을 할 수 있다.

[0082] 다시 말해서, 기존의 실명을 사용하는 인증서나 아이디 및 패스워드 방식을 이용하여 온라인 서비스를 이용하면 개인의 신분이 드러나기 때문에 프라이버시 침해의 요인이 될 수 있고, 또한 온라인 서비스 제공자의 개인정보 수집 및 관리상의 부주의로 인한 개인정보 유출은 심각한 사회적 문제가 될 수 있다. 하지만, 본 발명에 따르면, 서비스 제공자가 개인정보를 수집할 필요가 없으므로 개인정보 유출의 문제가 발생하지 않고, 개인의 신분이 드러나지 않는 TAC를 이용하여 온라인 서비스 이용시 인증을 받게 되므로 프라이버시를 보호할 수 있다.

[0083] 이상에서와 같이 상세한 설명과 도면을 통해 본 발명의 최적 실시예를 개시하였다. 용어들은 단지 본 발명을 설명하기 위한 목적에서 사용된 것이며, 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 본 명세서로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면의 간단한 설명

[0084] 도 1은 본 발명의 일 실시예에 따른 익명성 보장을 위한 TAC 발급 기관에 대한 개략적인 구성도이다.

[0085] 도 2는 본 발명의 일 실시예에 따른 TAC 생성 방법을 설명하기 위한 도면이다.

[0086] 도 3은 본 발명의 또 다른 일 실시예에 따른 TAC-MAC 생성 방법을 설명하기 위한 도면이다.

[0087] < 도면의 주요 부분에 대한 부호의 설명 >

[0088] 2: 사용자(user)

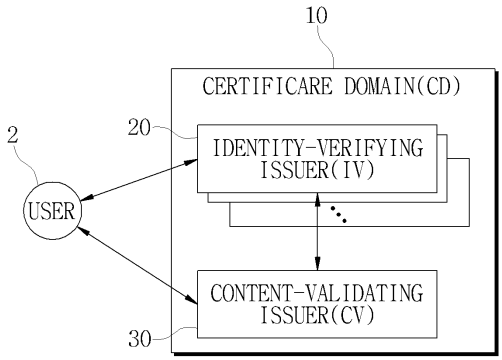
[0089] 10: 인증 도메인(certificate domain; CD)

[0090] 20: 계정 검증 관리자(identity-verifying issuer; IV)

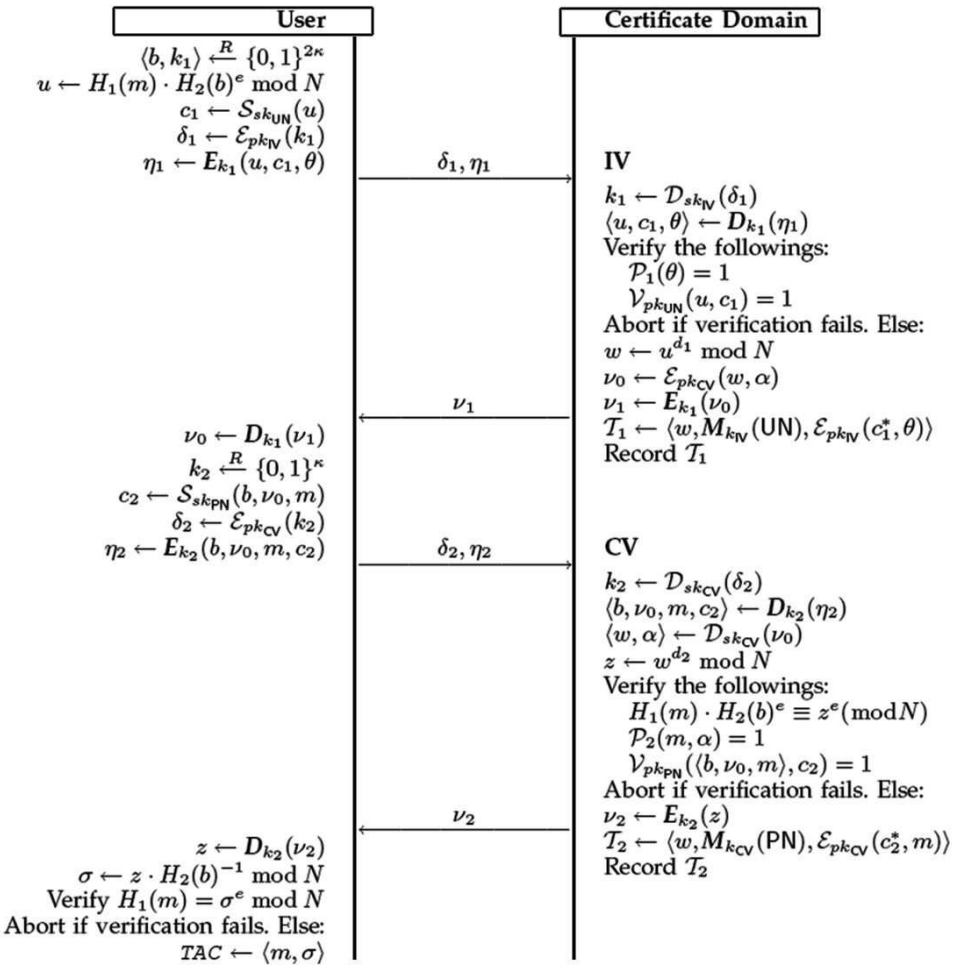
[0091] 30: 콘텐트 인증 관리자(content-validating issuer; CV)

도면

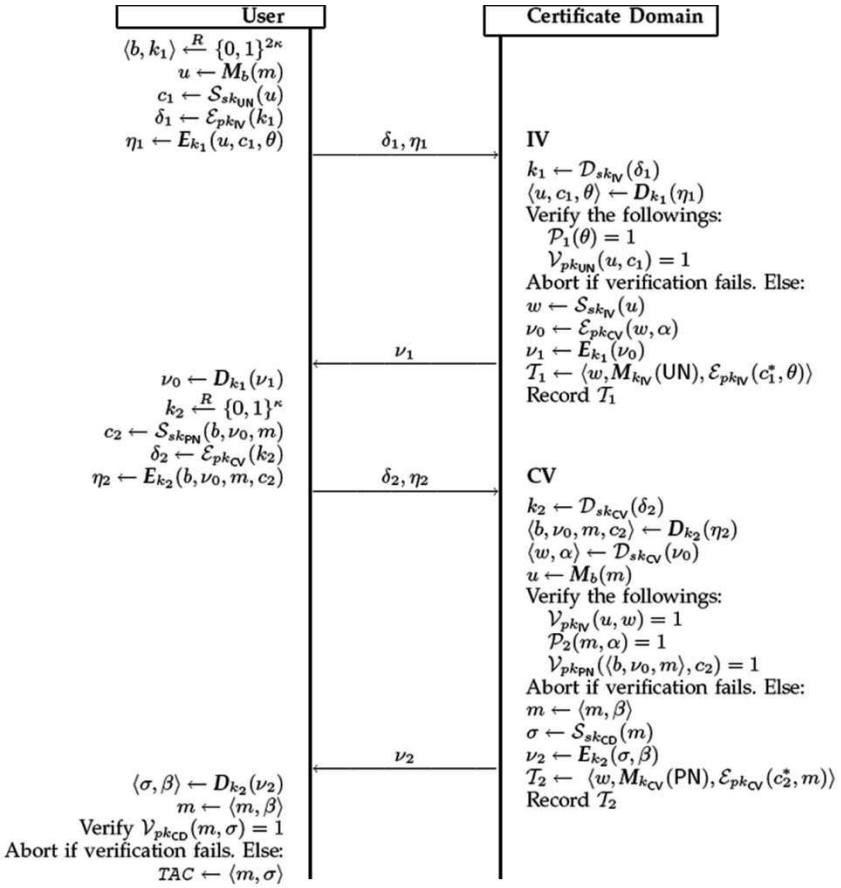
도면1



도면2


User
Certificate Domain
$\langle b, k_1 \rangle \xleftarrow{R} \{0,1\}^{2\kappa}$
$u \leftarrow H_1(m) \cdot H_2(b)^e \bmod N$
$c_1 \leftarrow \mathcal{S}_{sk_{\mathsf{UN}}}(u)$
$\delta_1 \leftarrow \mathcal{E}_{pk_{\mathsf{IV}}}(k_1)$
$\eta_1 \leftarrow \boldsymbol{E}_{k_1}(u, c_1, \theta)$
δ_1, η_1
IV
$k_1 \leftarrow \mathcal{D}_{sk_{\mathsf{IV}}}(\delta_1)$
$\langle u, c_1, \theta \rangle \leftarrow \boldsymbol{D}_{k_1}(\eta_1)$
Verify the followings:
$\mathcal{P}_1(\theta) = 1$
$\mathcal{V}_{pk_{\mathsf{UN}}}(u, c_1) = 1$
Abort if verification fails. Else:
$w \leftarrow u^{d_1} \bmod N$
$\nu_0 \leftarrow \mathcal{E}_{pk_{\mathsf{CV}}}(w, \alpha)$
$\nu_1 \leftarrow \boldsymbol{E}_{k_1}(\nu_0)$
$\mathcal{T}_1 \leftarrow \langle w, \boldsymbol{M}_{k_{\mathsf{IV}}}(\mathsf{UN}), \mathcal{E}_{pk_{\mathsf{IV}}}(c_1^*, \theta) \rangle$
Record $\mathcal{T}_1$
ν_1
$\nu_0 \leftarrow \boldsymbol{D}_{k_1}(\nu_1)$
$k_2 \xleftarrow{R} \{0,1\}^{\kappa}$
$c_2 \leftarrow \mathcal{S}_{sk_{\mathsf{PN}}}(b, \nu_0, m)$
$\delta_2 \leftarrow \mathcal{E}_{pk_{\mathsf{CV}}}(k_2)$
$\eta_2 \leftarrow \boldsymbol{E}_{k_2}(b, \nu_0, m, c_2)$
δ_2, η_2
CV
$k_2 \leftarrow \mathcal{D}_{sk_{\mathsf{CV}}}(\delta_2)$
$\langle b, \nu_0, m, c_2 \rangle \leftarrow \boldsymbol{D}_{k_2}(\eta_2)$
$\langle w, \alpha \rangle \leftarrow \mathcal{D}_{sk_{\mathsf{CV}}}(\nu_0)$
$z \leftarrow w^{d_2} \bmod N$
Verify the followings:
$H_1(m) \cdot H_2(b)^e \equiv z^e (\mathrm{mod} N)$
$\mathcal{P}_2(m, \alpha) = 1$
$\mathcal{V}_{pk_{\mathsf{PN}}}(\langle b, \nu_0, m \rangle, c_2) = 1$
Abort if verification fails. Else:
$\nu_2 \leftarrow \boldsymbol{E}_{k_2}(z)$
$\mathcal{T}_2 \leftarrow \langle w, \boldsymbol{M}_{k_{\mathsf{CV}}}(\mathsf{PN}), \mathcal{E}_{pk_{\mathsf{CV}}}(c_2^*, m) \rangle$
Record $\mathcal{T}_2$
ν_2
$z \leftarrow \boldsymbol{D}_{k_2}(\nu_2)$
$\sigma \leftarrow z \cdot H_2(b)^{-1} \bmod N$
Verify $H_1(m) = \sigma^e \bmod N$
Abort if verification fails. Else:
$TAC \leftarrow \langle m, \sigma \rangle$

도면3


User
Certificate Domain
$\langle b, k_1 \rangle \xleftarrow{R} \{0,1\}^{2\kappa}$
$u \leftarrow M_b(m)$
$c_1 \leftarrow \mathcal{S}_{sk_{UN}}(u)$
$\delta_1 \leftarrow \mathcal{E}_{pk_{IV}}(k_1)$
$\eta_1 \leftarrow E_{k_1}(u, c_1, \theta)$
δ_1, η_1
IV
$k_1 \leftarrow \mathcal{D}_{sk_{IV}}(\delta_1)$
$\langle u, c_1, \theta \rangle \leftarrow D_{k_1}(\eta_1)$
Verify the followings:
$\mathcal{P}_1(\theta) = 1$
$\mathcal{V}_{pk_{UN}}(u, c_1) = 1$
Abort if verification fails. Else:
$w \leftarrow \mathcal{S}_{sk_{IV}}(u)$
$\nu_0 \leftarrow \mathcal{E}_{pk_{CV}}(w, \alpha)$
$\nu_1 \leftarrow E_{k_1}(\nu_0)$
$\mathcal{T}_1 \leftarrow \langle w, M_{k_{IV}}(\mathsf{UN}), \mathcal{E}_{pk_{IV}}(c_1^*, \theta) \rangle$
Record $\mathcal{T}_1$
ν_1
$\nu_0 \leftarrow D_{k_1}(\nu_1)$
$k_2 \xleftarrow{R} \{0,1\}^{\kappa}$
$c_2 \leftarrow \mathcal{S}_{sk_{PN}}(b, \nu_0, m)$
$\delta_2 \leftarrow \mathcal{E}_{pk_{CV}}(k_2)$
$\eta_2 \leftarrow E_{k_2}(b, \nu_0, m, c_2)$
δ_2, η_2
CV
$k_2 \leftarrow \mathcal{D}_{sk_{CV}}(\delta_2)$
$\langle b, \nu_0, m, c_2 \rangle \leftarrow D_{k_2}(\eta_2)$
$\langle w, \alpha \rangle \leftarrow \mathcal{D}_{sk_{CV}}(\nu_0)$
$u \leftarrow M_b(m)$
Verify the followings:
$\mathcal{V}_{pk_{IV}}(u, w) = 1$
$\mathcal{P}_2(m, \alpha) = 1$
$\mathcal{V}_{pk_{PN}}(\langle b, \nu_0, m \rangle, c_2) = 1$
Abort if verification fails. Else:
$m \leftarrow \langle m, \beta \rangle$
$\sigma \leftarrow \mathcal{S}_{sk_{CD}}(m)$
$\nu_2 \leftarrow E_{k_2}(\sigma, \beta)$
$\mathcal{T}_2 \leftarrow \langle w, M_{k_{CV}}(\mathsf{PN}), \mathcal{E}_{pk_{CV}}(c_2^*, m) \rangle$
Record $\mathcal{T}_2$
ν_2
$\langle \sigma, \beta \rangle \leftarrow D_{k_2}(\nu_2)$
$m \leftarrow \langle m, \beta \rangle$
Verify $\mathcal{V}_{pk_{CD}}(m, \sigma) = 1$
Abort if verification fails. Else:
$TAC \leftarrow \langle m, \sigma \rangle$