모바일 전자 ID 지갑에 적합한 신뢰 관리 및 개인 정보보호 방안

(Trust Management and Privacy Protection for Mobile Digital ID Wallets)

장 공 수 † 윤 주 승 †† 이 항 석 †† 정 한 울 ††
(Gong-Soo Jang) (Ju-Seung Yun) (Hang-Suk Lee) (Han-Wul Jung)

박 용 수 ††† 최 대 선 †††† 진 승 헌 ††††
(Young-Su Park) (Dea-Sun Choi) (Seung-Hun Jin)

요 약 각종 전자인증 및 개인정보를 언제 어디서나 저장·이용 가능한 모바일 전자 ID지갑이 2008년 ETRI에서 개발되었다. 전자 ID지갑을 사용함에 있어 효과적인 사용자 개인정보 프라이버시 제어 방법과 인증정보, 개인정보, 크레덴셜 관리는 개인 정보보호 측면에서 매우 중요한 문제이며, 전자 ID지갑을 사용하기 위한 환경에서 사람과의 온/오프라인에서의 신뢰, 웹사이트의 피싱확인 및 회원가입, 무인 단말기와의 신뢰를 통한 개인정보의 제공 등 다양한 환경에서의 적용 가능한 신뢰관리 및 개인정보를 보호해줄 수 있는 방법이 필요하다.

본 논문에서는 모바일 전자 ID지갑에 적합한 신뢰 관리 및 개인 정보보호를 위한 삼중 신뢰 평가 방법을 제안한다. 다양하고 복잡한 모바일 ID지갑 사용환경에서 단순히 PKI 인증서 또는, 명성(Reputation)만으로는 개인정보의 관리 및 보호를 할 수 없다. 이러한 복합적인 상황에서 개인정보의 관리 및 보호를 위해서 PKI와 Reputation(명성) 그리고 정보 제공을 위한 상태(조건, Conditon)를 모두 고려해야 하며, 이 3가지(PKI, Reputation, Condition)를 판단하여 모바일 ID지갑환경에서 개인의 정보를 관리하고 보호할 수 있는 Triangular Trust Rating(삼중 신뢰 평가) 방법을 고안하였다. 우리는 프로토타입을 구현하고, 모바일 전자 ID지갑에 적용되는 다양한 시나리오에서 삼중 신뢰 평가 방법을 적용시켜 보았다. 그 결과, 제안 방법이 다양한 환경, 다양한 시나리오에서 적용될 수 있음을 보였다.

키워드 : 모바일 전자 ID 지갑, 개인정보보호, 신뢰관리

Abstract In 2008, ETRI developed a new mobile digital ID wallet, in which anyone can store personal information and PKI credential. When the wallet is used, privacy protection is one of the most important problems and personal information should be protected under various usage scenarios such as exchanging sensitive information in on/off-line environments, joining as a new member in the web site, etc.

· 본 연구는 지식경제부 및 한국산업기술진흥원의 국제공동기술개발사업의 일환으로 수행하였으며[2007-S-601-03, 자기통제 강화형 전자ID지갑 시스템 개발], 2007년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임[KRF-2007-313-D00760]

† 학생회원 : 한양대학교 정보통신대학
micro77@hanyang.ac.kr
†† 비 회 원 : 한양대학교 정보통신대학
yjuseung@gmail.com
hangston@nate.com
darknespiru@lycos.co.kr
††† 종신회원 : 한양대학교 정보통신대학 교수
yongsu@hanyang.ac.kr
(Corresponding author임)
†††† 비 회 원 : 한국전자통신연구원
sunchoi@etri.re.kr
jinsh@etri.re.kr

논문접수 : 2009년 2월 5일
심사완료 : 2009년 5월 27일

정보과학회논문지: 정보통신 제36권 제4호(2009.8)

In this paper, we propose a triangular trust management scheme that can effectively manage trustness, and also protect sensitive personal information. This scheme relies on three techniques: PKI, reputation and condition (situation context). We implemented prototype of our scheme, and tested it under various scenarios, which showed that the proposed scheme can effectively be used for diverse cases.

Key words : mobile Digital ID Wallets, personal information protection, trust management

1. 서 론

현재의 인터넷 환경은 사이트마다 각기 다른 인증방법과 개인정보 입력방법으로 인해 피싱(phishing) 공격 등에 의한 개인정보 유출이 심각하여 편의성과 보안성 측면에서 취약함을 보인다. 실제, 옥션의 해킹 사례와 같이 해킹으로 인한 개인의 모든 정보가 노출된 것처럼 중앙집중식 ID 관리와 인증정보, 개인정보, 크레덴셜 관리의 문제점이 발생하게 된다. 또한, 서비스 제공을 위해 필요 이상의 개인정보를 요구하고, 사이트 가입시에 포괄적인 약관동의만으로 개인정보 통제에 대한 모든 권리가 사이트로 이양되어 개인정보에 대한 사용자의 자기 통제권이 부재하게 된다는 문제점이 있다[1].

기존의 ID관리 기술을 적용시 사용자의 입장에서는 사용자들은 여전히 여러 사이트에서 발급된 많은 크리덴셜들을 관리해야 하는 불편한 경험을 느껴야 하고 사이트마다 프라이버시 정책이 상이하고 사용자가 그러한 정책의 이해와 인식이 제한되고 있고, 사용자 자신이 자기정보가 어떻게 유통되고 이용되는지에 대한 통제권 보장이 불가한 상황이며, 사업자들의 입장에서는 각각의 도메인마다 보안 및 프라이버시정책이 서로 상이, 서비스 통합하는데 많은 시간과 비용이 과다하게 소요되고 공유하려는 도메인이 많은 경우 복잡성이 기하급수적으로 증가, ID정보 공유의 문제점 발생하게 될 것이고, 사업자들마다 존재하는 서비스들을 연계하기 위해서는 공통의 ID 식별과 표현양식이 필요하나, 이러한 필요성을 충족시켜 줄만한 장치가 미구축되어 있다는 문제점이 발생하게 된다[1].

이런 문제를 해결하기 위하여 2009년 1월 ETRI에서는 전자인증 정보 및 개인정보를 언제 어디서든 저장·이용할 수 있는 사이버상의 전자 ID지갑 기술을 개발하였다. 전자 ID지갑은 지정된 서버, 휴대전화, USB메모리 등 이동저장매체에 주민등록번호나 주소, ID, 비밀번호, 신용카드 번호 등을 안전하게 보관해 언제 어디서나 꺼내 쓸 수 있는 기술이다[2].

그러나, 전자 ID지갑을 사용하기 위해 전자 ID지갑을 가진 사람과의 온/오프라인에서의 신뢰, 웹사이트의 피싱확인 및 회원가입, 무인 단말기와의 신뢰를 통한 개인정보의 제공 등 다양한 환경에서의 적용가능한 신뢰관리 및 개인정보를 보호해줄 수 있는 방법이 필요하다.

본 논문에서는 Ubiquitous 분산 환경에서의 PKI와 Local Reputation과 Global Reputation을 조합한 Combination Reputation, 정보를 제공할 수 있는 상황(Condition)을 고려한 모바일 ID지갑에 적합한 신뢰관리 및 효과적인 사용자 개인정보 프라이버시 제어를 할 수 있는 Triangular Trust Rating을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 전자 ID지갑 환경 신뢰관계 이슈와 요구사항을 설명한다. 3장에서는 SPKI/SDSI[3]와 Reputation management system인 Eigentrust[4]와 Beta Reputation[5]을 설명한다. 4장에서는 PKI, Reputation, Condition을 고려한 Triangular Trust Rating을 설명하고, 5장에서는 실험결과와 프로토타입을 설명하고, 마지막 6장에서는 결론을 맺는다.

2. 모바일 전자 ID지갑 환경 신뢰관계 이슈 / 요구사항

본 장에서는 모바일 ID지갑의 개념과 사용환경 및 신뢰관리 시스템 설계시 요구사항을 기술한다.

모바일 전자ID지갑은 일상생활에서 사용하는 지갑처럼 인터넷 상에서 사용되는 사이버 지갑이다. 전자ID지갑은 사용자는 자신의 주소, 전화번호 등과 같은 개인정보, 로그인 아이디, 비밀번호 등과 같은 인증정보와 신용카드 등과 같은 지불정보들로 구성된 Identity 정보를 보관한다. 사용자가 인터넷 웹 사이트에서 서비스를 받으면서 웹 사이트가 사용자 인증, 개인정보, 결제정보 등을 요구하면, 자신의 전자ID지갑에서 필요한 정보를 확인하여 웹 사이트에 제공하는 방식으로 운용된다. 이와 같이 전자ID지갑은 사용자 ID 정보 흐름 중간에 위치하여, 사용자가 직접 ID 정보의 흐름을 통제할 수 있도록 하였으며, 모든 정보를 Card 형태로 표현하여 사용자에게 일관성 있고 편리한 인터페이스를 제공하는 사용자 중심 ID 관리 시스템이다[2].

모바일 ID 지갑이 사용되는 환경의 예는 다음과 같이 요약될 수 있다.

1. 모바일 전자 ID지갑을 가지는 사람들 간의 정보 교환
2. 모바일 전자 ID지갑이 없는 사람과 모바일 전자 ID지갑을 가지는 사람과의 정보 교환
3. 모바일 전자 ID지갑을 소유한 사람과 장치 간의 정보 교환
4. 모바일 전자 ID지갑과 PC를 가지는 사람과 웹 사이트 사이의 정보 교환
   - 웹 사이트나 기타 서비스 방문(피싱 확인)

- 웹 사이트 회원 가입시 신뢰도 판단 및 개인정보 제공
- ID 지갑을 이용한 전자상거래

5. 모바일 ID지갑을 가지는 사람끼리의 사이버 공간에서의 정보 교환

또한, 모바일 ID지갑을 사용하는 환경에서 필요한 신뢰관리 시스템을 설계시 요구사항을 도출하였으며, 이는 다음과 같다.

1. 간편한 initial trust 확립
2. 믿을 수 있는 신뢰 등급 관리
3. 간편하고 직관적인 신뢰 관계 표현
4. 명성 및 신뢰 변화 발전 방안 수립
5. 신뢰도 및 위임장에 따른 효과적인 권한 부여
6. 신뢰도에 따른 체계적인 개인정보 제공 여부 방법 수립
7. 온/오프라인을 어우르는 신뢰 관리 체계 수립

3. 관련연구

본 장에서는 제안 기법이 사용하는 SPKI/SDSI와 Reputation Management System인 Eigentrust와 Beta Reputation에 관하여 기술한다.

3.1 SPKI/SDSI

웹 환경에서 인증서비스를 제공해주는 기존의 X. 509 공개키 기반구조는 권한이나 이름을 하나의 인증서에 나타내야 하므로 둘 중에 하나라도 변경 상황이 있을 경우 인증서를 새로 갱신해야 하는 불완전성을 지니고 있다. 뿐만 아니라 루트에서 시작하는 계층적 구조의 전역이름을 이용하고 있어 사용자가 소속되어 있는 회사나 부서의 이동에 따른 전역이름의 변경이 자주 일어날 수 있고, 루트가 어느 국가에 소속되어야 하는가 등에 따른 국제적인 이해관계에 얽힐 수 있는 복잡성을 내재하고 있다. 이런 문제점을 해결하기 위해 공개키 기반 구조를 단순화 시키고 유연하게 보완한 SPKI/SDSI가 연구되고 있다.

The Simple Distributed Security Infrastructure (SDSI)는 1996년 MIT에서 디자인 되었으며, 주된 목표는 보안, 확장성, 분산 컴퓨팅 시스템의 보안 인프라 구축을 촉진하는 것이다. 같은 시간 때에 칼 엔리슨은 간단하고, 유연한 인증 모델이 설계되었다. 그것의 이름은 Simple Public-Key Infrastructure(SPKI)이다. 이렇게 각각 연구되기 시작한 SPKI와 SDSI는 1998년에 SPKI/SDSI라는 명칭으로 통합되었다.

SPKI/SDSI는 평등주위 디자인을 가진다. 공급자들의 공개키는 인증 기관에 위치한다. 각 공급자는 다른 공급자와 같은 기준으로 인증서를 발급할 수 있다. SPKI/SDSI는 분배방식으로 만들 수 있고 신뢰할 수 있는 루트도 필요가 없다. SPKI/SDSI는 이름 인증서와 권한 인증서를 제공한다. 이름 인증서는 인증서 발행자의 지역 이름공간의 지역이름을 정의하고 권한 인증서는 인증서 발행자가 인증서의 주체에게 특별한 권한을 인정한다[3].

3.2 Eigentrust

Eigentrust 알고리즘은 2003년 Stanford 대학의 Sepandar D Kamvar가 "The Eigen Trust Algorithm for Reputation Management in P2P Networks"[4] 논문에서 P2P환경의 Globlal Reputation을 제공하기 위해 제안하였다.

Eigentrust에서는 표준화된 Local trust value를 가지는데 local trust value를 구하기 위해서는 s_{ij}를 구해야 한다. s_{ij}는 peer i이 peer j에게 받은 데이터를 평가한 값으로 peer i가 peer j에게 데이터를 받게 되고 받은 데이터가 긍정(Positive)이면 1이고, 부정(Negative)이면 -1로 평가하여 s_{ij}가 구해진다. 이 구해진 s_{ij}를 가지고 아래 식을 이용하여 표준화된 Local trust value가 구해진다.

$$c_{ij} = \frac{\max(s_{ij},0)}{\sum_j \max(s_{ij},0)} \quad (1)$$

Local trust value c_{ij}는 0과 1사이의 값을 가진다. Local trust value는 나와 이웃한 peer에 대해서만 평가한 값이고 이웃에 이웃의 trust value를 알기 위해서는 나와 이웃의 Local trust value와 이웃과 이웃의 이웃의 Local trust value를 곱하여 계산한다.

자신을 peer i라고 하고 이웃을 peer j, 이웃의 이웃을 peer k라고 하면 다음 식으로 구해진다.

$$t_{ik} = \sum_j c_{ij} c_{jk} \quad (2)$$

위 식을 행렬로 표현하면 식과 같고 이것은 $\vec{t_i} = C^T \vec{c_i}$에 포함되는 행렬이 된다.

$$= \begin{bmatrix} c_{i1} & c_{i2} & \cdots & c_{ij} \end{bmatrix} \begin{bmatrix} c_{1k} \\ c_{2k} \\ \vdots \\ c_{jk} \end{bmatrix} \quad (3)$$

여기서 Markov Process의 정의에 의해 C^T값이 무수히 곱해지면 $\vec{t_i}$는 peer i에 대해서 일정한 값을 가지게 된다. 기본적인 EigenTrust 알고리즘은 다음과 같다. pj는 한번도 데이터를 주고받지 않았을 때 초기 trust 값으로 모든 peer 수 분에 1의 값으로 정의한다.

분산된 환경에서 EigenTrust 알고리즘을 적용하여 자신의 global trust를 아래 식을 이용하여 계산할 수 있다.

$$t_i^{(k+1)} = (1-a)(c_{1i}t_1^{(k)} + \cdots + c_{ni}t_n^{(k)}) + ap_i \quad (4)$$

Peer i는 자신을 평가한 모든 peer들에게서 local trust value와 global trust를 이용하여 자신의 global trust 값을 계산한다.

3.3 Beta Reputation

Beta Reputation은 2002년 Audun Jøsang이 "The Beta Reputation System"[5]에서 전자상거래 환경에서의 Local Reputation을 제공하기 위하여 제안했다.

Beta Reputation[5]은 Bayesian Reputation System의 Binomial Reputation, Mutinomial Reputation[6], Continous Ratings in Discrete Bayesian Reputation [7]중 positive(good) 또는 negative(bad)와 같은 두 값으로만 평가하는 Binomial Reputation System의 한 종류이다.

Beta Reputation System은 feedback의 조합과 reputation rating을 이끌어 내기 위해 Beta 확률 밀도 함수 이용을 기반으로 한 Reputation System Engine으로서, 분산 환경(Decentralised), 중앙집중 환경(Centralised)에서 적용이 가능하며, 간단한 확률통계를 이용하여 쉽고, 유연하게 Reputation을 계산할 수 있는 장점이 있다.

Beta Reputation system에서Binary event의 확률분포를 표현할 수 있는 Beta 확률 밀도 함수를 사용하여 Feedback의 조합과 reputation rating을 표현을 위해 수학적 원리를 제공한다. Binary event의 귀납적 확률은 Beta 분포로 나타낼 수 있으며 Beta 분포 f(p|α, β)는 감마함수 Γ를 사용하여 아래와 같이 표현할 수 있다.

$$f(p|\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}p^{(\alpha-1)}(1-p)^{(\beta-1)}$$

※ $0\le p\le 1,\ 0<\alpha,\ 0<\beta$ (5)

Beat 분포의 확률 기대값은 다음과 같다.

$$E(p)=\alpha/(\alpha+\beta) \quad (6)$$

※ α=r+1, β=s+1 (0≤r,s), r:만족한 거래의 횟수, s:불만족한 거래의 횟수

X가 T를 평가한 만족한 횟수(r)와 불만족하는 횟수(s)라 하면 Reputation 함수는 아래와 같다.

$$\psi(p|r_T^X, s_T^X)=\frac{\Gamma(r_T^X+s_T^X+2)}{\Gamma(r_T^X+1)\Gamma(s_T^X+1)}p^{r_T^X}(1-p)^{s_T^X} \quad (7)$$

$$where\ 0\le p\le 1, 0\le r_T^X, 0\le s_T^X$$

Beta Reputation의 기대값(Local Reputation)은 아래와 같이 표현할 수 있다.

$$E(\psi(p|r_T^X, s_T^X))=(r_T^X+1)/(r_T^X+s_T^X+2) \quad (8)$$

4. 모바일 전자 ID 지갑에 적합한 신뢰 관리 및 개인 정보 보호 방안

본 장에서는 모바일 ID지갑 사용환경에서의 개인정보의 신뢰등급의 분류와 적용기법 및 모바일 ID지갑에 적합한 신뢰관리를 위한 Triangular Trust Rating을 설계한 내용을 기술한다.

4.1 모바일 ID 지갑 환경에서의 적용기법 및 신뢰등급

4.1.1 개인정보의 신뢰등급

4.1.1.1 개인정보의 분류

모바일 ID지갑환경에서 개인의 정보의 수준을 5단계로 분류할 수 있으며, 각 단계는 개인 비밀정보 - 개인 신상정보 - 개인 일반정보 - 익명성 정보로 분류할 수 있고, 각각의 정보들에 관한 설명은 다음과 같다.

- 개인 비밀정보: 정보 노출 시 개인 신상에 심대한 피해가 발생할 수 있는 정보
  예) 개인 패스워드, 재산현황, 신용정보, 신용카드 번호 등
- 개인 신상정보: 정보 노출 시 개인 신상에 피해가 발생할 수 있는 정보
  예) 주민등록번호, 운전면허번호, 학/이력, 여권번호 등
- 개인 일반정보: 정보 노출 시 개인 사생활에 피해를 보는 정보
  예) 집 전화번호 / 핸드폰 번호, 이름, 회사명, 전자명함정보
- 개인 익명성: 정보가 노출되어도 개인의 익명성 보장되는 정보
  예) ID, 닉네임, 사적인 E-mail, Blog등

4.1.1.2 개인정보와 신뢰등급

한국정보보호 진흥원에서는 개인정보의수명(壽命) 혹은 주기(週期)에 관한 관리가 필요하여 표 2와 같이 5등급의 개인정보 유형을 분류하였다[8].

본 논문에서는 한국정보보호 진흥원에서 발간한 2002년 개인정보보호 백서의 개인정보 5등급을 바탕으로 개인정보의 노출에 의해 발생할 수 있는 위험(Risk)에 따라 9개의 신뢰등급으로 구체화 및 세분화하였으며, 신뢰등급에 따른 개인정보와 정보의 수준을 살펴보면 표 3과 같다.

Level이 높을수록 중요한 개인 정보가 포함되어 있고, Level이 낮을수록 민감하지 않은 개인정보를 포함한다.

4.1.2 모바일 ID지갑환경에서의 적용기법

모바일 전자 ID지갑 사용환경에 따라 적용기법을 다르게 적용할 수 있다. 웹사이트의 피싱확인 및 상거래를 위해서는 Global Trust인 Eigentrust로 계산하며, 모바일 ID지갑이 없는 Offline상에서 만난 사람과는 Beta Reputation을 계산하며, 모바일 ID지갑을 가진 사람과 On/Offline에서 Eigentrust와 Beta Reputation을 기반

표 1 Bayesian Reputation System 종류

Binomial Reputation System	positive(good) 또는 negative(bad)와 같은 두 값으로만 평가
Mutinomial Reputation System	mediocre-bad-average-good-excellent와 같은 여러 등급으로 평가
Continous Ratings in Discrete Bayesian Reputation	평가하는 사람들의 의견을 더 잘 반영할 수 있는 "average-to-good"와 같이 평가

표 2 2002년 개인정보보호 백서의 개인정보 등급

등급	개인정보의 유형
1급 개인정보	신조·의료·성생활·인종·혈통·범죄·국가안보와관련된비밀정보등
2급 개인정보	교육·고용·금융신용·주민번호·자격증명·지문·혈액형·D N A·출입국정보등
3급 개인정보	개인이제출한정보, 프로파일된개인정보, 법령에의한수집정보등
4급 개인정보	기관의견해, 타인의견해, 정부기관의응답, 공개가능한통신문등
5급 개인정보	연구목적, 통계목적, 학술자료등의집합적으로활용되는정보등

표 3 개인정보 수준에 따른 신뢰등급 구분

신뢰등급	개인 정보	정보의 수준
Level 9	개인 패스워드	개인 비밀정보
Level 8	재산현황(부동산, 주식수), 신용정보, 병력	
Level 7	은행 계좌번호, 주식 계좌번호, 신용카드번호	
Level 6	주민등록번호, 여권번호, 학번, 운전면허번호	개인 신상정보
Level 5	학/이력, 가족관계, 자격증취득현황, 영어점수	
Level 4	집 전화번호/집주소, 핸드폰 번호	개인 일반정보
Level 3	이름, 회사명, 전자명함정보	
Level 2	Blog, 미니홈피(홈페이지), 가입한 동호회	익명성 정보
Level 1	사적인 E-mail	
Level 0	ID, 닉네임	

표 4 모바일 ID지갑 사용환경에 따른 신뢰관리 적용기법

구분	IDW↔Web서버		IDW↔IDW (On/Offline)	IDW↔Machine	IDW↔Human (Offline)
환경	은행업무	피싱확인 회원가입 상거래	개인정보교환 (명함, 전화번호)	장치인증, 개인정보 및 인증정보 제공	개인정보교환
적용방식	공개키	공개키 Reputation	공개키 Reputation	공개키 / 패스워드	만남에 의한 신뢰 Reputation
적용기법	공인인증서 (PKI)	공인인증서 (SPKI/SDSI) Eigentrust	공인인증서 (SPKI/SDSI), Beta Eigentrust	공인인증서 (SPKI/SDSI)	Beta

으로한 Combination Reputation으로 계산을 한다. 또한 현재까지 우리나라는 대부분 모든 기관과 웹사이트에서 PKI 공인인증서를 사용하고 있으므로 SPKI/SDSI 대신 공인인증서로 사용할 수 있으며, 차후 공개키 기반 구조를 단순화시키고 유연하게 보완하기 위해 SPKI/SDSI를 사용할 수 있다. 본 논문에서는 SPKI/SDSI 대신 공인인증서를 적용하였으며, 논문에서 PKI 등급은 verisign, entrust 등과 같은 웹사이트를 인증하는 1단계 인증서와 은행/증권회사 등에서 사용하는 2단계 범용 인증서로 구분하였다.

4.2 Triangular Trust Level Rating

다양하고 복잡한 모바일 ID지갑 사용환경에서 단순히 PKI 인증서 또는, 명성(Reputation) 만으로는 개인정보의 관리 및 보호를 할 수 없다. 이러한 복합적인 상황에서 개인정보의 관리 및 보호를 위해서 PKI와 Reputation(명성) 그리고 정보 제공을 위한 상태(조건, Condition)를 모두 고려해야 한다. 이 3가지(PKI, Reputation, Condition)를 판단하여 모바일 ID지갑환경에서 개인의 정보를 관리하고 보호할 수 있는 Triangular Trust Rating(삼중 신뢰 평가) 방법을 사용한다. Triangular Trust Rating은 유연하고 다양한 PKI인증을 할 수 있는 공인인증서(SPKI/SDSI)를 기반으로, Global Reputation(명성)을 표현할 수 있는 Eigentrust와 자신과의 직접적 트랜잭션을 통해 Local Reputation을 표현할 수 있는 Beta Reputation, 그리고 개인의 정보제공상태(Condition)도 고려한다.

4.2.1 모바일 ID 지갑의 신뢰관리 프레임워크

모바일 ID지갑의 개인 정보관리 프레임워크는 크게 PKI를 평가하는 공인인증서(SPKI/SDS)와 명성(Reputation)을 평가하는 Eigentrust(Global Reputatio 평가)와 Beta Reputation(Local Reputation 평가), Condition(개인정보의 제공 상태), 신뢰등급(인증서, Reputation)에 따라 개인정보를 분류한 Privacy Protection of Individual Information으로 구성되어 있으며, 이러한 PKI, Reputation Score, Condition에 따른 신뢰등급(Trust Level)을 매핑해주고, Framework의 환경설정 기능을 해주는 Trust Management Framework으로 구성된다.

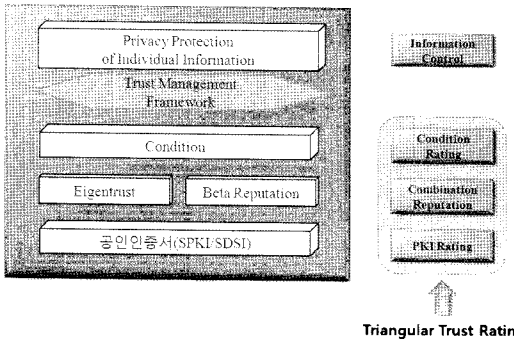


그림 1 모바일 ID지갑의 신뢰관리 프레임워크

4.2.2 Triangular Trust Rating

Triangular Trust Rating의 신뢰평가(Trust Rating)와 신뢰등급(Trust Level)은 다음과 같이 4가지로 계산될 수 있다.

① PKI + Reputation + Condition
② PKI+Condition
③ Reputation+Condition
④ Condition

첫번째로 PKI의 Trust 평가는 PKI의 Level에 따른 신뢰등급평가(Trust Level Rating)은 PKI가 없는 경우에는 Trust Level 0의 개인정보를 제공하고, PKI가 Level 1 인증서인 경우 Trust Level 2이하의 개인정보를 제공를, PKI가 Level2 인증서인 경우 Trust Level 3이하의 개인정보를 제공을 제공한다. PKI의 Level 인증서는 Trust Management Framework에서 설정가능하며, 예를 들면 PKI Level 1 인증서를 Verisign, entrust, 또는 PKI Level 2 인증서를 은행권 공인인증서, 범용인증서로 설정할 수 있다.

두번째로 Local Reputation과 Global Reputation을 조합한 Combination Reputation에서 Reputation(명성)은 자신과 직접적인 transaction 또는 자신이 알고 있는 대상을 통한 transaciton으로 발생한 Reputation을 Local Reputation, 평가하고자 하는 대상과 Transaction한 모든 Rating을 종합한 Reputation을 Global Reputation이라고 하며, 각각의 Reputation은 Beta Reputation과 Globa Reputation으로 계산할 수 있다. Reputation을 평가할 때 직접적인 transaction이 적을 경우 Global Trust를 더 높게 반영하고 자신이 상대방과의 많은 Transaction으로 계산된 Local Reputation을 Global Reputation보다 더 높게 반영해야 한다. 예를 들면 인터넷 쇼핑몰에서 많은 사람들이 높게 평가(Global)한 제품을 구입한 결과 만족스럽지 못했다(Local Trust). Global trust만을 믿고 살 수 없을 것이다.

Local Reputation과 Global Reputation의 Combination Rating은 다음과 같이 표현

$$Combination\ Reputation\ Score = \frac{(\sigma_0 - \sigma) B\ Reputation + \sigma \cdot Eigentrust}{\sigma_0} \quad (9)$$

※ σ_0 = 1번 Transaction 발생했을 때의 Beta Reputation의 표준편차

σ = Beta Reputation의 표준편차

상대방과 transaction이 많을수록 Eigentrust보다 Beta Reputation을 더 높게 반영하는 Combination Reputation 평가는 직접적인 트랜잭션이 없을 경우, 다른 사람들이 신뢰한 Reputation(Eigentrust)를 따르게 되며, 자신과 직접적인 트랜잭션이 많아질수록 Beta Reputation에 더 가중치를 부여할 수 있다.

그러나, 웹 사이트의 경우에는 Global Reputation (Eigentrust)만을 적용하며 Eigetrust 값은 디폴트로 0.5를 부여하며, Eigentrust값이 0이면 피싱 사이트로 간주하고, 1에 가까우면 매우 신뢰할 만한 사이트로 판단할 수 있다.

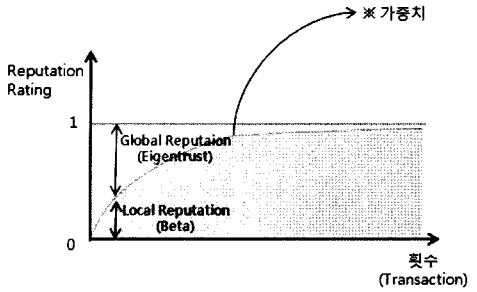


그림 2 트랜잭션 횟수에 따른 Global Reputation과 Local Reputation의 가중치

Offline Trust : Online Trust = 1: 0.3 (10)

만족(Positive)는 트랜잭션에 있어서 불만족(Negative)이 아닌 상태로 정의될 수 있다. 즉, 트랜잭션을 하면서 불만족(Negative)하지 않는다면 만족(Positive)이 되는 것이다. 예를 들면, 상대방과 대화를 하였는데 불쾌감이나 나쁜 감정을 느끼지 않았다면 그 상태는 만족(Positive)이며, 인터넷 웹사이트를 방문했는데 서비스를 정상적으로 받았거나, 정보를 제공받았다면 만족(Negative)상태이다.

불만족(Negative)은 신뢰관계에 있어서 만족(Positive)보다 더 큰 영향을 준다. 예를 들면, 웹 사이트에 방문했을 때 악성코드에 감염되었거나, Offline에서 상대방에게 안좋은 경험을 했다면, 신뢰가 급격히 감소하게 된다. 이와 같이 만족(Positive)와 불만족(Negative)이 신뢰에 영향을 미치는 영향을 수치적으로 비교하면 다음과 같이 부여할 수 있으며, 이 값은 모바일 ID갑에

서 언제나 수정이 가능하다.

Positive : Negative = 1: 10 (11)

Reputation Score에 의한 Trust Level은 다음과 같이 분류를 할 수 있다.

0 = Rep → Trust Level 0이하의 개인정보를 제공

0 < Rep <0.25 → Trust Level 1이하의 개인정보를 제공

0.25 ≤ Rep <0.50 → Trust Level 2이하의 개인정보를 제공

0.50 ≤ Rep <0.75 → Trust Level 3이하의 개인정보를 제공

0.75 ≤ Rep ≤ 1 → Trust Level 4이하의 개인정보를 제공 (12)

Reputation 평가에 의한 제공될 수 있는 정보는 Trust Level 4 이하의 정보만 제공할 수 있다. 즉, Reputation(명성)이 아주 좋다고 해서 "개인비밀정보, 개인신상정보"를 제공해 줄 수 없다.

세번째로 개인정보를 제공해야 하는 상황(Condition)에서 개인정보를 제공해야 하는 Condition은 표 5와 같이 분류할 수 있으며, 모바일 ID지갑에서는 디폴트값으로 Exchange(교환)로 설정한다.

표 5 개인정보의 제공 상황(Condition)과 예

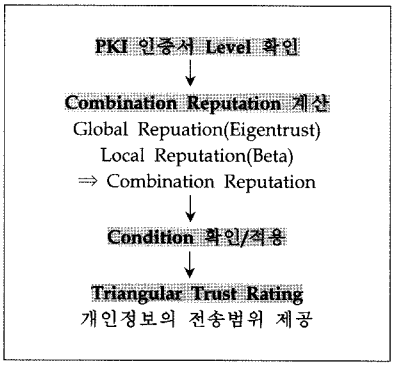
- Application(지원): 개인 정보가 필요에 의해 반드시 제공해야 하는 상황
  예: 입사지원, Toeic접수, 여권발급, 민원서류 발급, 진료(재정) 상담 등
- Exchange(교환): 상대방과의 개인정보 교류가 필요한 상황
  예: 전화번호 교환, 명함 교환,
- 공개(Public): 개인 정보를 일방적으로 제공해야 하는 상황
  예: ID, 닉네임 등

동일한 신뢰등급이라도 개인정보를 제공해야 하는 상황(Condition)에 따라 개인정보 제공의 범위(Trust Level)이 달라질 수 있다.

4.2.3 모바일 ID 지갑의 Triangular Trust Rating 과정

Triangular Trust Rating 과정은 먼저 PKI 인증서 Level을 확인하고, Global Reputation과 Local Reputation을 조합한 Combination Reputation을 계산하며, 자신의 정보를 제공해야하는 상황을 판단한 후, Triangular Trust Rating을 내린다. 이와 같은 절차를 살펴보면 표 6과 같다.

표 6 Triangluar Trust Rating 과정



4.2.4 Triangular Trust Rating Level

Triangular Trust Rating 결과에 따라 개인 정보 제공 범위를 결정하기 위해서는 표 7, 8, 9를 적용할 수 있다.

웹 사이트는 기본적으로 PKI 인증서 레벨1(Veri Sign, Entrust, ...)을 모바일 ID전자지갑에 제공하게 되고, 이를 기반으로 Reputation과 Condition을 고려하여

표 7 PKI 인증서가 없는 경우의 Reputation Score와 Condition에 따른 Level

SPKI/SDSI	Reputation Score	Conditon	Triangular Trust Level
x	Rep = 0	Application	Level 0 개인 정보제공
		Exchange	Level 0 개인 정보제공
		Public	Level 0 개인 정보제공
	0 < Rep <0.25	Application	Level 1이하 개인 정보제공
		Exchange	Level 1이하 개인 정보제공
		Public	Level 0이하 개인 정보제공
	0.25 ≤ Rep <0.50	Application	Level 2이하 개인 정보제공
		Exchange	Level 1이하 개인 정보제공
		Public	Level 1이하 개인 정보제공
	0.50 ≤ Rep <0.75	Application	Level 3이하 개인 정보제공
		Exchange	Level 2이하 개인 정보제공
		Public	Level 1이하 개인 정보제공
	0.75 ≤ Rep <1	Application	Level 4이하 개인 정보제공
		Exchange	Level 3이하 개인 정보제공
		Public	Level 2이하 개인 정보제공

표 8 PKI 인증서 Level 1이고 Reputation Score와 Condition에 따른 Level

SPKI/SDSI	Reputation Score	Conditon	Triangular Trust Level
인증서 레벨 1	Rep = 0	Application	Level 2이하 개인 정보제공
		Exchange	Level 2이하 개인 정보제공
		Public	Level 2이하 개인 정보제공
	0 < Rep <0.25	Application	Level 2이하 개인 정보제공
		Exchange	Level 2이하 개인 정보제공
		Public	Level 2이하 개인 정보제공
	0.25 ≤ Rep <0.50	Application	Level 3이하 개인 정보제공
		Exchange	Level 2이하 개인 정보제공
		Public	Level 2이하 개인 정보제공
	0.50 ≤ Rep <0.75	Application	Level 4이하 개인 정보제공
		Exchange	Level 3이하 개인 정보제공
		Public	Level 2이하 개인 정보제공
	0.75 ≤ Rep <1	Application	Level 5이하 개인 정보제공
		Exchange	Level 4이하 개인 정보제공
		Public	Level 2이하 개인 정보제공

표 9 PKI 인증서 Level 2이고 Reputation Score와 Condition에 따른 Level

SPKI/SDSI	Reputation Score	Conditon	Triangular Trust Level
PKI 레벨 2	Rep = 0	Application	Level 4이하 개인 정보제공
		Exchange	Level 4이하 개인 정보제공
		Public	Level 4이하 개인 정보제공
	0 < Rep <0.25	Application	Level 4이하 개인 정보제공
		Exchange	Level 4이하 개인 정보제공
		Public	Level 4이하 개인 정보제공
	0.25 ≤ Rep <0.50	Application	Level 4이하 개인 정보제공
		Exchange	Level 4이하 개인 정보제공
		Public	Level 4이하 개인 정보제공
	0.50 ≤ Rep <0.75	Application	Level 5이하 개인 정보제공
		Exchange	Level 4이하 개인 정보제공
		Public	Level 4이하 개인 정보제공
	0.75 ≤ Rep <1	Application	Level 6이하 개인 정보제공
		Exchange	Level 5이하 개인 정보제공
		Public	Level 4이하 개인 정보제공

Triangular Trust Level을 고려할 수 있다.

모바일 ID지갑끼리의 On/Off line에서는 위 Trigangular Trust Level을 적용하지만, 무인단말기간은 모바일 ID 지갑에 PKI 인증서 레벨 2(은행인증서, 범용 인증서)만을 제공하게 되고, Trigangular Trust Level 4이하의 정보를 제공할 수 있다. (무인단말기의 Reputation은 고려될 수 없음)

Bob, Tom, Jane의 Triangular Trust Level Rating이 아래와 같다고 가정하면, Triangular Trust Level Rating을 적용한 개인정보의 전송 수준은 표 10과 같다.

Bob, Tom, Jane의 개인정보 전송범위는 표 10과 같다.

5. 실험결과

본 장에서는 제안 기법인 Triangular Trust Rating을 적용한 프로토타입 구현 및 실험결과를 기술한다.

표 10 3명의 전자ID지갑 사용자의 Triangular Trust Level을 적용한 예

구 분	SPKI /SDSI	Combination Reputation Score	Conditon	Triangular Trust Level
Bob	Level 2	$0.75 \le Rep_{Bob} = 0.9 \le 1$	Application	Level 5이하 개인 정보제공
Tom	Level 1	$0.50 \le Rep_{Tom} = 0.5 < 0.75$	Exchange	Level 3이하 개인 정보제공
Jane	x	$0.25 \le Rep_{Jane} = 0.4 < 5$	Public	Level 3이하 개인 정보제공

5.1 프로토타입 구현

5.1.1 모바일 전자 ID지갑 신뢰관리

그림 3은 모바일 ID에 저장된 상대방의 개인정보를 볼 수 있고, on/off line에서 상대방과의 트랜잭션 이후 만족 / 불만족을 입력 및 상대방에게 제공 가능한 정보를 보여줄 수 있으며, 모바일 ID에 저장된 상대방을 입력하면 PKI레벨, Reputation, Transaction 등의 개인정보를 볼 수 있다.

자신의 제공 가능한 개인정보의 범위를 제공해준다. 그림 4는 이용하고자 하는 웹사이트의 정보를 보여주고, 웹사이트에 제공할 수 있는 정보를 보여줄 수 있다. 이때 웹사이트는 Global Reputation 값을 Reputation만을 적용한다. 그림 5는 상대방의 PKI, Combination Reputation, Transaction 정보 등을 출력 해 주며, 상대방

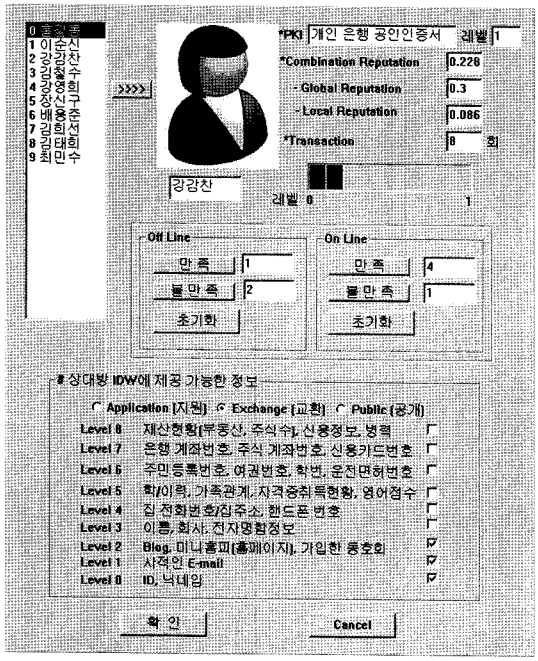


그림 3 모바일 ID지갑에서의 상대방의 인적관리

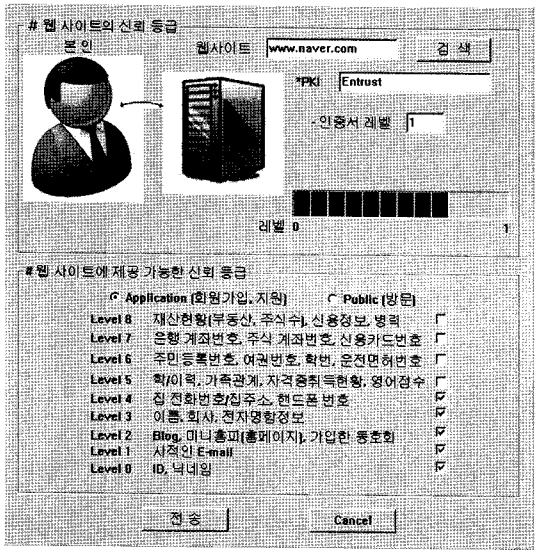


그림 4 모바일 ID지갑과 웹사이트간 신뢰관리

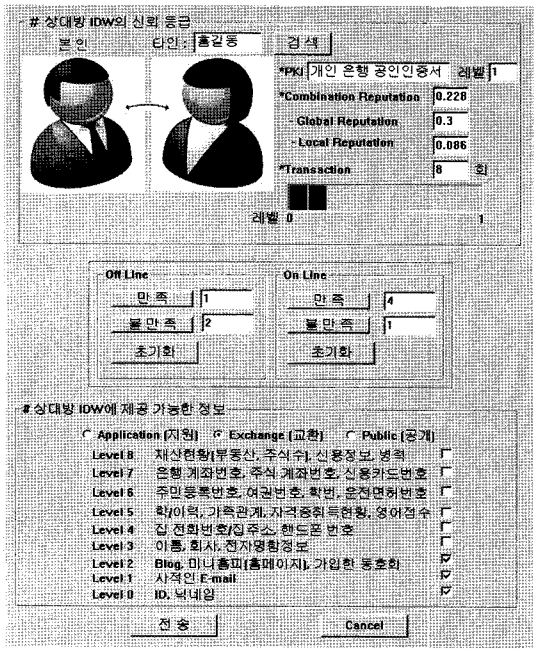


그림 5 모바일 ID지갑을 가진 상대방의 신뢰관리

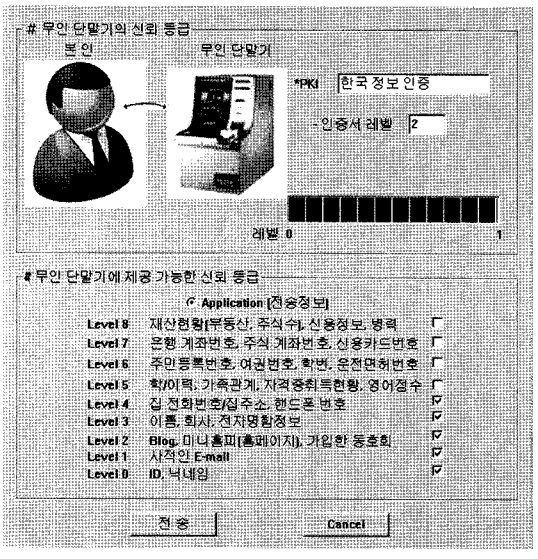


그림 6 모바일 ID지갑과 무인단말기간 신뢰관리

에게 제공 가능한 정보의 보여준다. 그림 6은 transaction할 무인 단말기의 정보와 무인 단말기에게 제공할 수 있는 개인정보를 보여주며, 무인단말기의 경우, 레벨 4의 이하의 정보를 제공할 수 있다.

5.2 Triangular Trust Level Rating 실험결과

본 절에서는 PKI, Eigentrust 및 Transaction에 따른 Triangluar Trust Rating을 적용한 실험결과를 기술한다.

5.2.1 PKI 인증서가 없고, Eigentrust, Beta에 의한 Trust Rating

PKI 인증서가 없는 경우 Eigentrust와 Beta Reputation을 기반으로 한 Combination Reputation Score에 의해 상대방에게 제공될 수 있는 정보는 Level 4이하의 정보를 제공할 수 있다. 직접적인 경험(트랜잭션=0)이 없는 경우에는 Global Reputation(Eigentrust) 값을 따르며, 트랜잭션(Positive)의 횟수가 늘어날수록 점점 상대방에게 제공할 수 있는 정보의 Level은 상승하나 Level 4를 초과하는 개인정보는 자동으로 전송할 수 없다.

5.2.2 PKI 인증서가 없고, Eigentrust, Beta에 의한 Trust Rating

인증서가 없고, 각각의 Egietrust값과 Transaction이 증가하며, 4번째 Transasction에 1번의 Negative값을 주었을 때 Trust Rating 결과는 위 표와 같다. 트랜잭션이 없을 경우에는 Eigentrust의 값으로 Trust Rating을 하며 트랜잭션이 많아질수록 Trust Rating은 Local Reputation(Beta Reputation)의 영향을 받게 된다. 4번째 트랜잭션에 1번의 negative가 입력되면, Negative가 Positive에 10배(Positive:Negative=1:10)이므로 Trust Rating은 급격이 하락하게 되고, 이후 Positive가 증가함에 따라 서서히 Trust Rating이 증가한다.

즉, 한번의 불만족(Negative)은 전체 신뢰를 낮추게 되고, 신뢰를 회복하기 위해서는 만족(Positive)의 횟수가 많아져야 한다. Global Reputation(Eigntrust)가 0.3인 상대방과는 최초 Level2이하의 정보(Blog, 미니홈피, 가입한 동호회, 사적인 E-mail, ID, 필명을 제공할 수 있

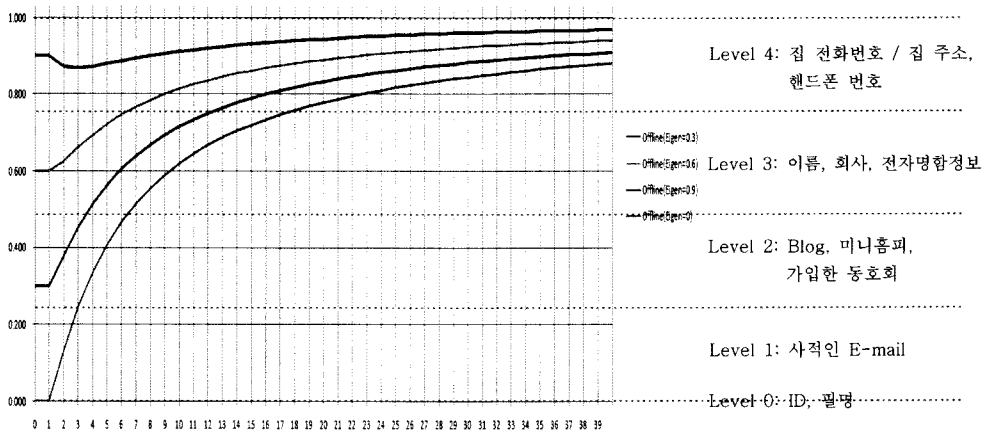


그림 7 Eigentrust 값이 0, 0.3, 06, 09이고, 지속적으로 Positive Transaction이 발생하는 경우

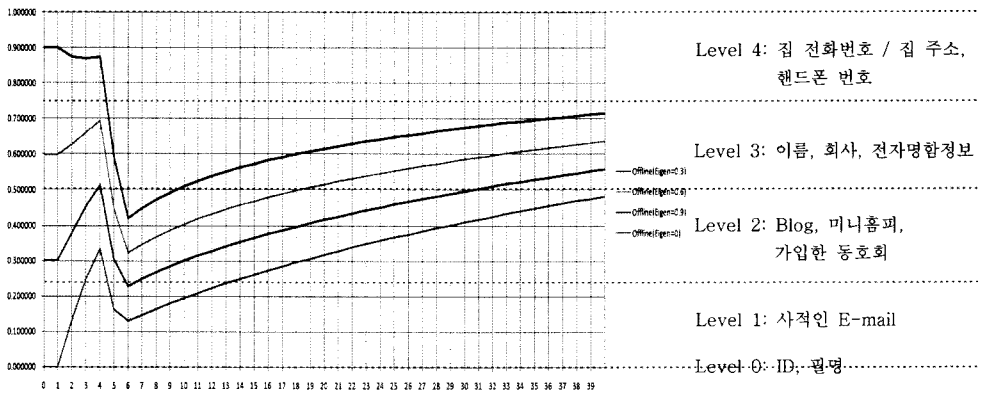


그림 8 Eigentrust 값이 0, 0.3, 06, 09이고, 4번째 Transaction에 Negative Transaction이 발생

고, 3번의 Positive를 transaction이 있으면 Level 3이하의 정보를 제공받을 수 있으나, 4번째 Ngative Transaction을 받게 되면 Level1이하의 정보만을 제공받게 된다.

5.2.3 PKI 인증서 레벨이 1이고, Eigentrust, Beta에 의한 Trust Rating

PKI인증서 Level 1을 가지고 온 상대방에게는 기본적으로 개인정보 Level 2이하의 정보를 제공할 수 있으며, Combination Reputation Score에 의해 제공될 수 있는 개인정보 Level은 향상될 수 있으나, Level 4를 초과하는 개인정보 Level은 자동으로 제공될 수 없고, 모바일 ID지갑을 소유한 사람이 수동으로 통제해야 한다. Reputation에 의해 개인 정보 제공범위가Level 3~Level 5사이로 정해진다.

5.2.4 PKI 인증서 레벨이 2이고, Eigentrust, Beta에 의한 Trust Rating

PKI인증서 Level 2을 가지고 온 상대방에게는 기본적으로 개인정보 Level 3이하의 정보를 제공할 수 있으며, Combination Reputation Score에 의해 제공될 수 있는 개인정보 Level은 향상될 수 있으나, Level 5를 초과하는 개인정보 Level은 자동으로 제공될 수 없고, 모바일 ID지갑을 소유한 사람이 수동으로 통제할 수 밖에 없다. Reputation에 의해 개인 정보 제공범위가 Level4~Level 6사이로 정해진다.

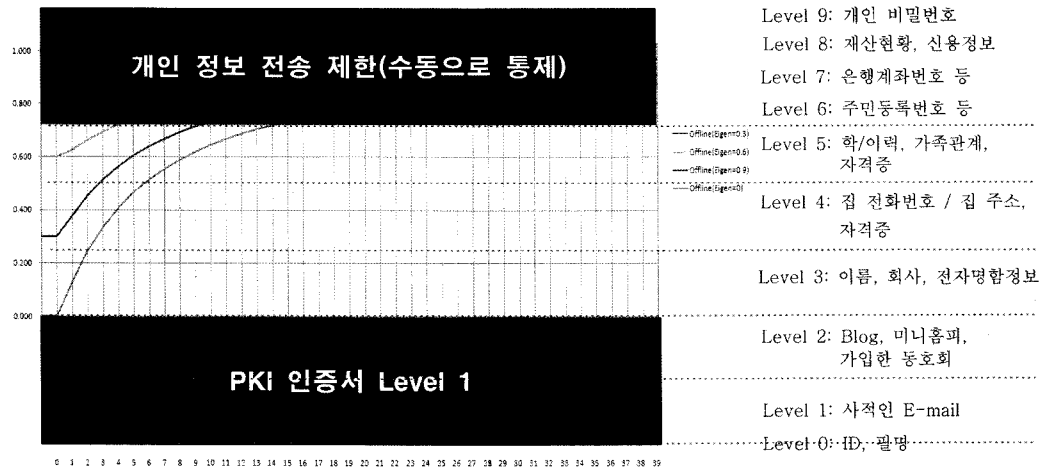


그림 9 Eigentrust 값이 0, 0.3, 06이고, PKI 인증서 Level 1인 경우

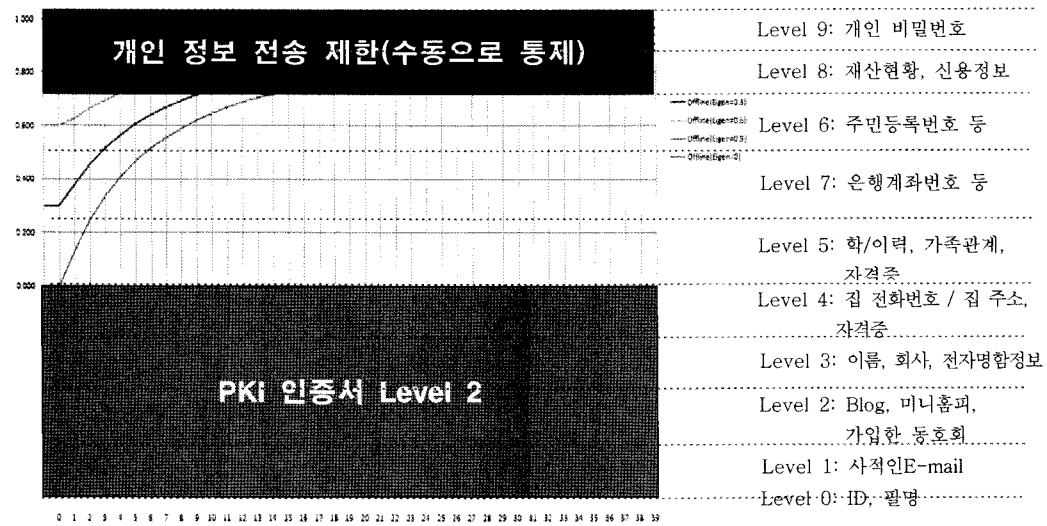


그림 10 Eigentrust 값이 0, 0.3, 06이고, PKI 인증서 Level 1인 경우

6. 결 론

본 논문에서 모바일 ID지갑에서 개인정보보호를 위한 모바일 ID지갑용 통합 신뢰관리 방안을 수립하였고 모바일 ID 지갑용 통합 신뢰관리를 위한 실험 결과 중앙집중식 개인정보의 효율적인 관리 문제와 분산형 환경에서 신뢰관계 구축을 수동으로 설정해야 하는 문제점을 해결하기 위해 모바일 ID지갑 환경에서 직관적인 관리 도구를 제공하여 쉽고 편리하게 사용자의 개인정보 프라이버시를 자동으로 제어할 수 있었다.

본 연구를 통해 Pervasive 환경에서 개인 익명성을 보장할 수 있고, 간편하고 자동적인 신뢰성 확립 방안 수립할 수 있으며, 웹 환경뿐만 아니라 사용자의 참여와 정보 공유가 더욱 중요해지는 웹 2.0 환경에 적합한 모바일 ID지갑의 신뢰 관리 및 개인 정보보호를 강화할 수 있는 방법을 제공할 수 있을 것으로 기대된다.

참 고 문 헌

[1] 진승헌, Digital Identy Management, 2007년 기술백서, 한국전자통신연구원, 2007.11.

[2] 조영섭, 진승헌, "사용자 중심 ID 관리 기능을 제공하는 전자 ID 지갑 시스템", *전자통신동향분석*, 제23권 제4호, 2008.08.

[3] D. E. Clarke. Spki/sdsi http server/certificate chain discovery in spki/sdsi. *Master' thesis, Massachusetts Institute of Technology - MIT*, September 2001.

[4] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, The eigentrust algorithm for reputation management in p2p networks, *Proceedings of the 12th International World Wide Web Conference*, May 20-24, 2004.

[5] Audun Josang and Roslan Ismail, The beta reputation system, In *Proceedings of the 15th Bled Electronic Commerce Conference*, Bled, Slovenia, June 2002.

[6] A. Jøsang and J. Haller, "Dirichlet Reputation Systems" (to appear), *Proceedings of the Second International Conference on Availability, Reliability and Security (ARES 2007)*, Vienna, April 2007.

[7] Audun Josang, Continuous Ratings in Discrete Bayesian Reputation Systems, *IFIP International Federation for Information Processing*, Trust Management II, 151-166, 2008.

[8] 2002년 개인정보보호 백서, 정보보호 진흥원, 2003.2.

장 공 수

2002년 단국대학교 전자공학(공학사). 2004년~2006년 1기갑여단 전산실장 2006년~2007년 3군사령부 C4I장교. 2008년~현재 한양대학교 전자컴퓨터통신공학 석사. 관심분야는 정보보호, NCW, 네트워크 보안

윤 주 승

2007년 대구대학교 통신공학(공학사) 2009년 한양대학교 전자컴퓨터통신공학 석사. 2009년~현재 한국정보보호진흥원 연구원. 관심분야는 정보보호, 침입탐지, 네트워크 보안

이 항 석

2009년 인천대학교 정보통신공학(공학사) 2009년~현재 한양대학교 전자컴퓨터통신공학 석사

정 한 울

2005년 성공회대학교 멀티미디어 시스템 공학(공학사). 2009년~현재 한양대학교 전자컴퓨터통신공학 석사. 관심분야는 정보보호, 시스템 보안

박 용 수

1996년 KAIST 전산학과(학사). 1998년 서울대학교 컴퓨터공학사(석사). 2003년 서울대학교 전기컴퓨터공학부(박사). 2003년~2004년 서울대학교 자동제어특화연구센터 박사후 연수연구원. 2005년~현재 한양대학교 정보통신대학 컴퓨터전공 조교수. 관심분야는 정보보호, 네트워크 보안, 암호학

최 대 선

1995년 동국대학교 전자계산학과 학사 1997년 포항공과대학교 전자계산학과 석사. 1998년 현대정보기술 연구소. 1999년~현재 한국전자통신연구원 정보보호연구단. 관심분야는 ID관리, 신뢰관리, P2P/MANET 보안

진 승 헌

1993년 숭실대학교 전자계산학과 학사 1995년 숭실대학교 대학원 전자계산학과 석사. 2004년 충남대학교 대학원 컴퓨터과학과 박사. 1999년~현재 한국전자통신연구원 정보보호연구본부 팀장/선임연구원. 관심분야는 Digital Identity Management, PKI, PMI, 인증인가, 개인정보보호