情 報 保 護 學 會 誌
第18卷 第2號, 2008. 4

신뢰된 유비쿼터스 인증환경을 위한 u-인증 프레임워크

김 영 준*, 황 보 성*, 김 정 희*, 백 종 현**

요 약

유비쿼터스 환경에서는 IT서비스에 사람뿐만 아니라 기기 및 사물 등이 참여하고 다양한 인증수단이 사용된다. 하지만, u-IT서비스에 참여하는 개체에 대한 신뢰된 인증환경이 없다면 유비쿼터스 사회의 전체 신뢰도가 떨어지는 결과를 초래하게 된다. 본 논문에서는 유비쿼터스 환경의 신뢰된 인증 환경 조성을 위한 프레임워크로서 u-IT 서비스에 인증서비스를 도입하기 위한 절차와 u-IT 서비스 위험평가 방법 및 인증수단 선택기준 등의 보안요구사항을 제시한다.

Ⅰ. 서 론

최근 정보통신 및 네트워크 기술의 급속한 발전으로 사람뿐만 아니라 기기 및 사물 등이 IT 서비스에 참여하는 유비쿼터스 사회가 도래하고, 공인인증서, ID/Password, 바이오정보 등 다양한 인증수단의 이용 요구도 증가하고 있다.

u-City로 대표되는 u-IT 서비스는 그 특성상 개체간 정보가 자유롭게 이동하고, 서비스간 융·복합이 빈번하게 발생한다. 따라서, u-IT 서비스에 참여하는 개체에 대한 신뢰된 인증 환경 부재시, 유비쿼터스 사회의 전체 신뢰도가 저해되는 결과를 초래하게 되어, u-IT 서비스에 대한 신뢰된 인증서비스 도입절차 및 이용기준의 필요성이 높아지고 있다.

본 논문에서는 사람뿐만 아니라 기기 및 사물 등이 참여하고 다양한 인증수단이 이용되는 유비쿼터스 환경의 신뢰된 인증환경 조성을 위해, u-IT 서비스에 인증서비스를 도입하기 위한 절차와 이용기준을 제시한다. 인증서비스 도입절차와 이용기준에는 u-인증서비스 모델 및 u-인증서비스 도입절차, u-IT 서비스 위험평가 방법 및 인증수단 선택기준, 위험수준별 인증수단 이용기준 등이 포함된다.

본 논문의 구성은 다음과 같다. 1장과 2장에서 서론과 인증 프레임워크 관련 국외 사례들을 소개하고, 3장에서 6장까지 u-인증 프레임워크를 제시한다. 마지막으로 7장에서 결론과 앞으로의 연구계획에 대하여 논의한다.

Ⅱ. 국외 동향

여기에서는 미국, 일본, 유럽 등 주요 국가들의 인증 프레임워크 관련 현황을 소개한다.

2.1 미국 전자인증(e-Authentication) 현황

미국은 정책기반 마련을 위해 정부 전반에 사용할 수 있는 전자인증(e-authentication)[1] 위험 및 보증레벨을 수립하였다.

보증레벨[2]은 제시된 신원의 적법성에 대한 확신에 따라 총 4가지의 레벨로 정의되며, 전자정부서비스에 대한 위험평가를 실시하여 적절한 신원 보증레벨[3]을 선택하도록 하였다.

또한, 전자인증 위험평가를 위한 방법론인 e-RA를 수립하여 정부기관 등이 자신의 서비스에 적합한 인증 요구사항을 식별하고, 이를 통해 적절한 보증레벨을 선택할 수 있도록 하기위한 e-RA 툴[4]을 제공하였으며, 크리덴셜(credential)[5]과 크리덴셜서비스제공자를 평가하기 위해서 기술적 보증레벨과 크리덴셜 평가프레임워크(Credential Assessment Framework)[5]를 수립하여

* 한국정보보호진흥원 IT기반보호단 전자인증팀 연구원 ({dream, hbs2593, kimjh}@kisa.or.kr)
** 한국정보보호진흥원 IT기반보호단 전자인증팀 팀장 (jhbaek@kisa.or.kr)

〔표 1〕 신원보증레벨

Level 1	Level 2	Level 3	Level 4
Little or no confidence in asserted identity (e g. self identified user/password)	*Some confidence in* asserted identity (e.g. PIN/Password)	*High confidence in* asserted identity (e g. digital cert)	*Very high* confidence in the asserted identity (e.g. Smart Card)

〔표 2〕 보증레벨별 최대 잠재 위험

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

크리덴셜서비스제공자에 대해 크리덴셜 발급 절차, 네트워크 및 시스템 보안, 시스템 전체에 대한 위험관리 등에 대해 현장심사를 하도록 하였다.

2.2 일본 차세대 전자인증 프로젝트 현황

일본은 차세대 인증 적용시 관련되는 참여자를 식별하고 크리덴셜 발급과 관련하여 필요한 시나리오 개발을 위해 전자인증 업무모델 체계를 수립하였으며, 다양한 사용자 인증수단을 도입한 서비스 제공자간 상호연동을 보장하는 기술과 인증수단 선택시 참조할 수 있는 인증정책 가이드라인(Authentication Policy Guideline)을 개발하여 인증프레임워크, 보증레벨, 보증레벨 결정을 위한 절차, 운영 및 기술기준에 대하여 참조할 수 있게 하였다.

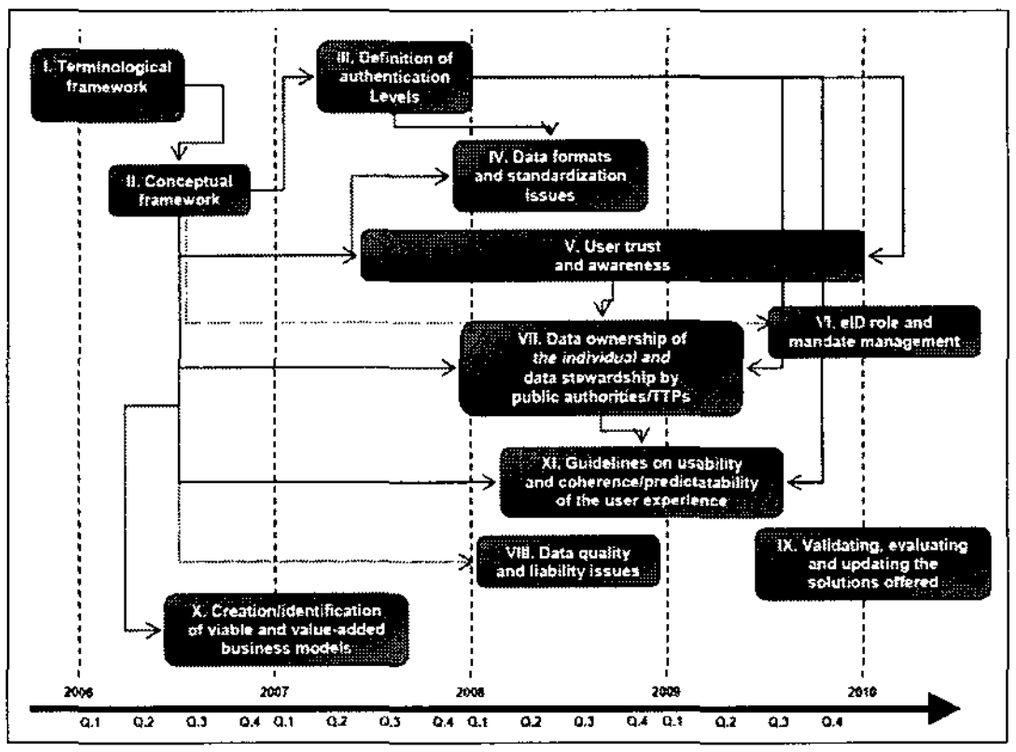
차세대 전자인증 업무모델은 사용자, 서비스제공자, 포털서비스제공자, 크리덴셜서비스제공자, 평가기관, 이용활성화 추진기관으로 구성된 비즈니스모델 체계와 의료/건강, 금융, 디지털콘텐츠, 전자상거래의 4가지 업무영역에 대해 수립하였다.

인증정책 가이드라인은 인증프레임워크, 보증레벨, 보증레벨 결정을 위한 절차, 운영 및 기술기준으로 구성되어 있으며, 인증정책은 인증프레임워크에 참여하게 되는 참여자와 관련하여 등록, 크리덴셜 관리, 토큰관련, 인증프로토콜 등의 규정으로 구성되어 있고, 보증레벨은 해당 플랫폼에서 보장되는 크리덴셜에 대한 신뢰정도를 의미하는데 Minimal, Low, Substantial, High의 총4가지로 분류된다. 서비스제공자가 필요한 보증레벨은 해당 서비스에서 인증에러가 발생 시 생길 수 있는 잠재적인 영향평가를 통해 선택되며, 인증과정에서 일어나는 절차를 등록, 크리덴셜관리, 토큰, 인증프로토콜 등 총 4가지 분류하고 각각의 처리 절차에서 필요한 사항을 기준으로 규정하였다.

2.3 유럽위원회의 전자신원(eID) 로드맵 현황

유럽의 대다수 국가는 스마트카드 기반의 PKI, 바이오정보 등을 이용한 인증인프라 구축을 위해 전자신원(eID) 정책을 수립하여 시행 또는 준비 중이며, EU의 유럽위원회는 각국이 구축·운영 중인 eID를 국경에 관계없이 다양한 서비스에 이용할 수 있도록 '범유럽권 전자신원(eID)로드맵'을 수립하여 추진하고 있다.

공통되고 일관성 있는 eID 용어프레임워크, eID에 대한 이용자 신뢰도 및 인식 제고, 개인 프라이버시를 고려한 개인데이터소유권 검토가 eID의 근본 요건이며, eID 규격 등을 포함하는 개념(Conceptual) 프레임워크, 인증수준 정의, eID 데이터형식 및 표준화, eID를 이용한 역할 및 권한 관리, eID 관련 법적 문제 등이 eID 인프라 요건에 해당되고, eID 유용성 요건으로는 eID 이용 비즈니스 모델 검증, eID 이용을 위한 공공과 민간부문 협력, EU규정을 통한 국가 eID에 대한 상호인정 등이 있다.



〔그림 1〕 전자신원(eID)로드맵 세부절차

Ⅲ. u-인증서비스 모델

3.1 u-인증서비스 구성개체

u-인증서비스의 구성개체는 인증대상, 등록기관, u-

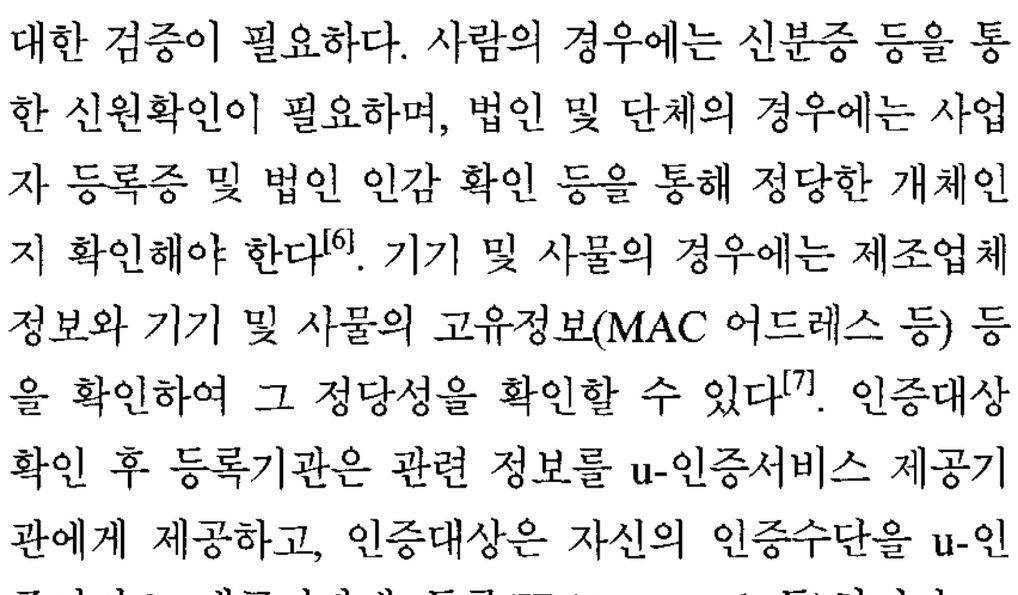
인증서비스 제공기관, 신뢰당사자, 검증기관, u-인증서비스 관리기관 등으로 구성되며, 이들 개체들은 별개의 개체로 각각 연관관계를 가질 수도 있으며, 하나의 개체가 여러 개체의 역할을 수행할 수도 있다.

3.2 u-인증서비스 모델

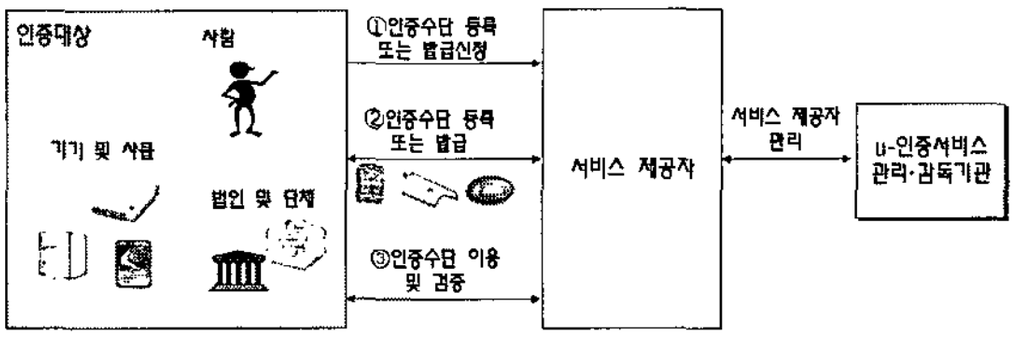
u-인증서비스 모델은 인증수단별 특징 및 서비스 이용환경 등에 따라 다양한 모델이 존재할 수 있다. [그림 2]는 u-인증서비스의 기본모델을 나타낸다. u-인증서비스를 제공하고자 하는 기관은 u-인증서비스 관리·감독기관으로부터 지정요건을 평가받아 u-인증서비스 제공기관으로 지정받은 후 u-인증서비스를 제공한다. 인증대상이 u-인증서비스 제공기관에게 인증수단을 발급받아 이용하는 과정은, 자신의 인증수단을 등록하거나 발급받는 「인증수단 등록 및 발급단계」와 실제 인증수단을 이용해 서비스 제공자에 접근해 서비스를 이용하는 「인증수단 이용단계」로 구분된다.

「인증수단 등록 및 발급단계」에서 등록기관은 인증수단을 발급받고자 하는 인증대상이 정당한 개체인지에 대한 검증이 필요하다. 사람의 경우에는 신분증 등을 통한 신원확인이 필요하며, 법인 및 단체의 경우에는 사업자 등록증 및 법인 인감 확인 등을 통해 정당한 개체인지 확인해야 한다[6]. 기기 및 사물의 경우에는 제조업체 정보와 기기 및 사물의 고유정보(MAC 어드레스 등) 등을 확인하여 그 정당성을 확인할 수 있다[7]. 인증대상 확인 후 등록기관은 관련 정보를 u-인증서비스 제공기관에게 제공하고, 인증대상은 자신의 인증수단을 u-인증서비스 제공기관에 등록(ID/Password 등)하거나 u-인증서비스 제공기관으로부터 인증수단을 발급(공인인증서 등)받을 수 있다.

「인증수단 등록 및 발급단계」 종료 후, 인증대상은 u-



〔그림 2〕 u-인증서비스 기본모델



〔그림 3〕 u-인증서비스 모델 I

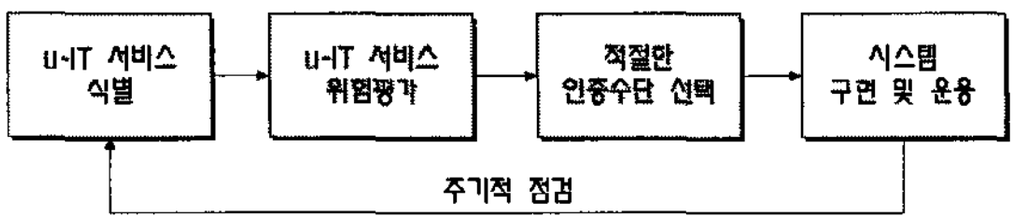
인증서비스 제공기관으로부터 신뢰된 인증수단을 이용해 IT 서비스에 접근한다. 검증기관은 인증대상이 제출한 인증수단을 검증하고 그 결과를 신뢰당사자에게 제공함으로써 인증대상의 진정성을 확인하고 신뢰당사자는 이를 기반으로 인증대상에서 서비스 접근을 허용한다.

인증수단 및 서비스 제공자의 특징에 따라 다양한 u-인증서비스 모델이 존재할 수 있다. [그림 3]은 서비스 제공자가 인증수단을 발급하는 u-인증서비스 제공기관과 신뢰당사자의 역할을 병행하는 모델을 나타낸다. 일반적인 ID/Password와 같이, 자신의 서비스를 이용하는 인증대상에게 인증수단(ID/Password)을 발급한 후 인증대상이 해당 서비스에 접근할 경우 자신에 보유한 인증수단(ID/Password) 정보를 이용해 인증대상의 진위를 확인하는 모델이다. 이러한 모델 또한 서비스 제공자가 u-인증서비스 관리·감독기관으로부터 지정을 받거나 또는 u-인증서비스 관리·감독기관이 제시하는 기준을 준용함을 증빙하는 별도의 절차를 통해 u-인증서비스의 안전성을 확보할 수 있다.

Ⅳ. u-IT 서비스의 인증시스템 적용절차

본 장에서는 현재 운영 중이거나 신규로 도입되는 IT 서비스에 적절한 인증시스템을 선택·적용하는 절차를 제시한다. 성공적인 인증시스템 도입을 위해서는 해당 IT 서비스에 대한 정확한 분석을 기반으로 어떤 수준의 인증시스템을 도입할지를 결정해야 한다. [그림 4]는 IT 서비스의 인증시스템 적용 절차를 나타낸다.

IT 서비스 제공자는 인증시스템이 적용되는 기본적인 서비스 범위를 식별하고 이에 대해 인증 관점에서 위험평가를 수행한다. IT 서비스의 위험평가 범위 식별



〔그림 4〕 IT서비스의 인증시스템 적용 절차

시 그 범위를 최소화하는 것이 이상적이지만, 기본적인 서비스 단위 또는 하나의 인증수단이 통용되는 범위를 위험평가의 최소 범위로 한정할 수 있다.

IT 서비스의 위험평가 범위 식별시 그 범위를 최소화하는 것이 이상적이지만, 기본적인 서비스 단위 또는 하나의 인증수단이 통용되는 범위를 위험평가의 최소 범위로 한정할 수 있다. 위험평가 범위를 식별한 후, 해당 서비스 범위 내에서 송·수신되는 트랜잭션과 트랜잭션 상의 주요정보를 식별해야 한다. 주요정보를 식별해야 하는 이유는 인증수단이 적용되지 않았을 경우, 비인가자 또는 비인가 기기·사물의 불법적인 서비스 접근에 의해 해당 정보가 유출 및 위·변조되기 때문이다. 주요정보가 식별되면 인증수단이 적용되지 않았을 경우를 가정하여 위협을 식별하고 위협 시나리오를 작성한다. 인증수단이 적용되지 않았을 경우의 위협은 비인가자 또는 비인가 기기·사물의 불법적인 서비스 접근이 된다. 불법적인 서비스 접근을 통한 일반적인 위협의 형태는 비인가자 또는 비인가 기기·사물을 통한 주요정보 유출 혹은 위·변조이고, 위협 시나리오는 일반적인 위협 형태를 기반하여 작성한다.

인증 관점에서의 IT 서비스 위험평가 절차는 [그림 5]와 같다. 위험평가를 통해 해당 서비스의 위험수준이 결정되며, 위험수준은 해당 서비스에 어떤 수준의 인증시스템을 도입할 지를 결정하는 기준이 된다.

IT 서비스의 위험수준은 [표 3]과 같이 4가지로 등급화 되며, 이에 따라 인증시스템의 요구사항도 틀려진다. 위험평가를 통해 IT 서비스의 위험수준이 결정되면, 위험수준의 요구사항을 만족하는 적절한 인증수단(ID/Password, 공인인증서 등)을 선택하여 인증시스템을 구축한다. 위험수준이 높은 IT 서비스의 경우 보안성이 높은 인증수단이 적용되어야 하고 위험수준이 낮은 IT

IT 서비스 식별 및 위협분석	① 위험평가 대상이 되는 IT 서비스의 범위 식별 ② 트랜잭션 및 주요정보 식별 ③ 인증수단이 적용되지 않았을 경우에 대한 위협 식별
⇓	
위협의 발생가능성 (Likelihood) 산정	① 발생가능성(Likelihood) 세부 산정기준 정립 ② 위협의 발생가능성 산정
⇓	
위협의 피해규모 (Impact) 산정	① 피해규모(Impact) 세부 산정기준 정립 ② 위협에 따른 피해규모 산정
⇓	
위험수준 결정	① 피해규모와 발생가능성에 기반한 위험수치 산정 ② 위험수치에 따른 최종 위험수준 결정

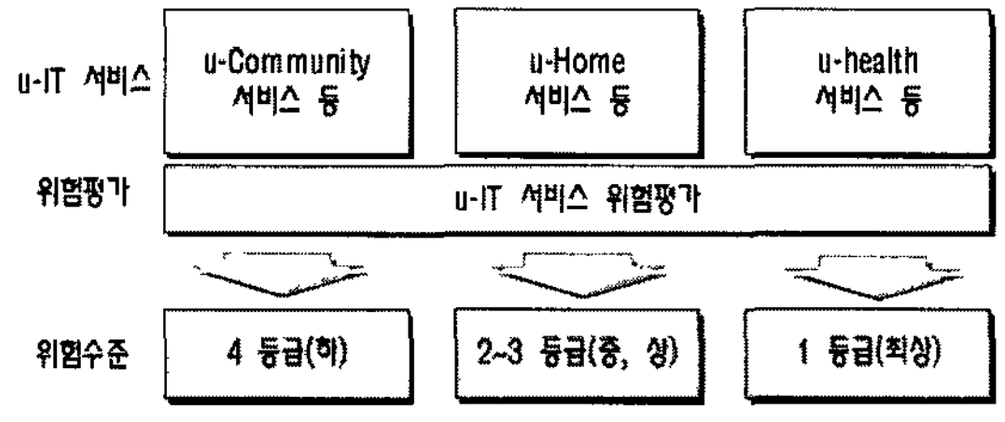
〔그림 5〕 IT 서비스 위험평가 절차

〔표 3〕 IT 서비스의 위험수준 등급

위험 수준	설명
1등급 [최상(Extreme)]	인증시스템의 아주 높은(Very High) 확신 및 신뢰 요구
2등급 [상(High)]	인증시스템의 높은(High) 확신 및 신뢰 요구
3등급 [중(Medium)]	인증시스템의 약간의(Some) 확신 및 신뢰 요구
4등급 [하(Low)]	인증시스템의 아주 미미한(Little or No) 확신 및 신뢰 요구

〔표 4〕 u-IT 서비스 위험수준 등급화

발생가능성 / 피해규모	낮음	보통	높음
낮음	4등급(하)	3 등급(중)	2 등급(상)
보통	3 등급(중)	2 등급(상)	1 등급(최상)
높음	2 등급(상)	1 등급(최상)	1 등급(최상)



〔그림 6〕 위험평가에 따른 위험수준 결정

서비스의 경우에는 상대적으로 보안성이 낮은 인증수단이 이용될 수 있다. 마지막으로, 인증시스템 구축 후 요구사항에 만족하는 시스템이 구축되었는지 점검하고 향후, 주기적인 재평가를 통해 보완할 사항을 점검해 나간다.

Ⅴ. u-IT 서비스 위험평가 방법

본 장에서는 IT 서비스 제공자가 적절한 인증수단을 선택하여 IT 서비스를 구축·운영할 수 있도록 해당 IT 서비스에 대한 위험평가 방법을 제시한다. 위험평가는 인증 관점에서 수행되며, 위협의 발생가능성(Likelihood) 및 발생시 피해규모(Impact)를 고려하여 최종 위험수준을 결정한다.

5.1 위협의 발생가능성(Likelihood) 산정 단계

IT 서비스의 위험평가를 위해 서비스 범위 및 위협이

〔표 5〕 위협의 발생가능성 산정기준

구분	높음	보통	낮음
발생 가능성	비인가자(기기·사물 포함)가 주요정보를 획득할 동기가 충분하고, 비인가자의 접근이 용이한 서비스 환경	비인가자(기기·사물 포함)가 주요정보를 획득할 동기가 충분하고, 비인가자가 접근이 용이하지 않는 서비스 환경	비인가자(기기·사물 포함)가 주요정보를 획득할 동기가 불충분하고, 비인가자가 접근이 용이한 서비스 환경

식별되면 해당 위협이 실제로 발생할 가능성을 산정한다. 발생가능성 정도는 침해 동기(Motivation), 서비스 환경(Environment)을 고려하여 [표 5]와 같이 3가지 등급(높음, 보통, 낮음)으로 정의한다.

위험평가자는 해당 서비스의 침해 동기 및 서비스 환경을 종합 고려하여 발생가능성 등급을 판단해야 한다. 침해 동기는 노출 및 위·변조 대상이 되는 주요정보의 중요도 등가 기준이 될 수 있으며, 서비스 환경은 네트워크 이용 환경, 물리적 통제 등 대체 통제 수단의 존재 여부, 불법적 침해를 위해 요구되는 기술적 수준 등이 구분기준으로 이용될 수 있다.

5.2 위협의 피해규모(Impact) 산정 단계

위협의 발생가능성을 산정한 후, 실제 위협이 발생한 경우를 가정하여 피해형태와 피해규모를 산정해야 한다. [표 6]과 같이 피해형태는 "신뢰 및 명성의 훼손" 등 5가지로 분류하고, 각 피해형태에 따른 피해규모는 3가지 등급(높음, 보통, 낮음)으로 정의한다.

〔표 6〕 피해형태에 따른 피해규모 산정기준

구분	높음	보통	낮음
신뢰 및 명성의 훼손	심각하고 장기적인 신뢰/명성의 추락	심각하고 단기적인 신뢰/명성 추락	제한되고 단기적인 신뢰/명성 추락
재무적 손실	복구하기 힘들고 재앙수준의 재정손실	중요하면서 복구하기 힘든 재정 손실	중요하지 않고 비교적 복구하기 쉬운 재정 손실
생산성 및 성과 저하	주요기능, 수행기간과 범위 등에 대한 심각한 저하	주요기능, 수행기간과 범위 등에 대한 현저한 저하	주요기능 수행기간과 범위 등에 대한 저하
건강 및 안전 침해	중상이나 사망	의료치료가 필요한 부상	의료치료가 필요없는 경미한 부상
법규의 위반	형 집행에 결정적 영향을 줄 수 있는 위반	형 집행에 영향을 미칠 수 있는 위반	형 집행에 영향이 없는 위반

피해규모의 산정기준 정립 후, 위험평가자와 서비스 제공자는 식별된 위협이 발생한 경우를 가정하여 피해규모를 산정한다.

5.3 위험수준 결정 단계

IT 서비스의 위험수준은 피해규모와 발생가능성을 고려하여 4가지 등급(최상, 상, 중, 하)으로 결정된다. 위험평가자는 [표 7]과 같이 산정된 피해규모의 등급과 발생가능성의 등급을 곱하여 IT 서비스의 위험수치를 산정한다. 위험수치의 산정결과는 계량화된 정수가 된다.

위험수치가 계산되면 IT 서비스의 최종 위험수준을 [표 8]에 따라 평가한다. 위험평가의 최종결과는 위험수준의 정도(최상, 상, 중, 하)가 되며 향후, 해당 위험수준에 따라 적절한 인증수단을 선택하여야 한다.

〔표 7〕 IT 서비스 위험수치 산정

	피해규모	높음	보통	낮음
발생 가능성	점수 / 가중치	100	50	10
높음	1	100×1=100	50×1=50	10× 1=10
보통	0.5	100×0.5=50	50×0.5=25	10×0.5=5
낮음	0.1	100×0.1=10	50×0.5=5	10×0.1=1

※ 피해규모 점수 및 발생가능성 가중치는 위험평가자 및 서비스 제공자에 의해 조정 가능

〔표 8〕 IT 서비스 위험수치 산정

위험수치	위험수준	비고
76점~100점	최상 (Extreme)	1등급의 인증수단 적용 필요
51점~75점	상 (High)	2등급이상의 인증수단 적용 필요
26점~50점	중 (medium)	3등급이상의 인증수단 적용 필요
1점~25점	하 (Low)	4등급이상의 인증수단 적용 필요

※ 위험수치는 위험평가자 및 서비스 제공자에 의해 조정 가능

Ⅵ. 인증수단 선택 및 이용기준

6.1 인증수단 선택

유비쿼터스 환경에서는 패스워드, OTP, 공인인증서, 바이오정보, 등 다양한 인증수단을 사람, 기기·사물이 이용할 수 있다. 일반적으로 이러한 인증수단은 사용자가 아는 것, 소지한 것, 사용자 자체인 것 등의 유형으로 구분되어지며 해당 유형에 따라 인증수단을 [표 9]와 같이 구분할 수 있다.

패스워드 등 다양한 인증수단들은 하나의 인증수단으로 이용될 뿐만 아니라 서로 다른 유형의 인증수단이 혼용되어 함께 이용될 수 있으며, 이를 Multi-factor 인증이라 한다.

〔표 9〕 인증수단의 유형

유 형	예 시
사용자가 아는 것 (You Know)	패스워드, 개인식별번호(PIN) 등
사용자가 소지한 것 (You Have)	공인인증서, OTP 등
사용자 자체인 것 (You Are)	지문, 얼굴, 정맥 등 바이오정보

다가오는 유비쿼터스 환경에서는 다양한 참여개체 및 서비스 특성으로 인해 패스워드, 소프트토큰(공인인증서), OTP, 하드토큰(PKI+HSM), 바이오정보 등의 수많은 인증수단이 도입되어 이용될 것으로 예상된다.

인증수단은 고유 특성에 따라 인증과정에서 발생 가능한 공격에 대해 가지는 취약점이 달라질 수 있다. 따라서 사용하고자 하는 인증수단의 특징과 운영방식을 이해하고 해당 수단의 취약점을 보완하여 사용하여야 한다. 다양한 형태의 공격을 모두 막아낼 수 있는 인증수단은 존재하지 않는다. 다만, 인증수단이 이용되는 환경에서 해당 수단이 가지는 취약성을 보완하기 위한 보안요구사항을 식별하고 이를 만족시키기 위한 필요 조치가 취해 질 때 비로소 인증수단을 안전하게 이용할 수 있게 된다.

6.2 인증수단 선택기준

인증수단을 적용하고자 하는 서비스는 본 논문 제5장에 기술된 u-IT 서비스 위험평가를 거쳐 해당 서비스의 위험이 최상, 상, 중, 하 총 4단계 중 하나로 식별될 수 있다. 각 위험 수준별로 필요한 인증수준과 인증수단 요구사항은 [표 10]과 같다.

〔표 10〕 위험수준별 인증수단 선택기준

위험수준	필요한 인증수준		인증수단 선택기준
	보증등급	설명	
최상 (Extreme)	1등급	이용될 인증수단은 아주 높은 확신 및 신뢰를 줄 수 있어야 함	- HSM 이용 - Multi-factor - 직접대면 발급 - 추측 불가능
상 (High)	2등급	이용될 인증수단은 높은 확신 및 신뢰를 줄 수 있어야 함	- Multi-factor - 직접대면 발급 - 추측 불가능
중 (Medium)	3등급	이용될 인증수단은 약간의 확신 및 신뢰를 줄 수 있어야 함	- 추측 어려움
하 (Low)	4등급	이용될 인증수단은 아주 미미한 확신 및 신뢰를 줄 수 있어야 함	- 추측 가능

위험수준별 인증수단 선택기준은 인증수단 추측 가능성 정도, 인증수단 발급을 위한 신원확인 방법의 신뢰성, Multi-factor 이용 여부, HSM(Hardware Security Module) 이용 여부 등으로 구분되어 질 수 있다.

위험수준이 중(Medium) 또는 하(Low)의 경우, 인증수단 추측이 상대적으로 용이한 패스워드도 이용될 수 있으나, 위험수준이 높은 최상(Extreme)과 상(High)에서는 이용될 수 없다. 또한, 위험수준이 최상(Extreme) 또는 상(High)일 경우, 서로 다른 유형의 인증수단을 함께 사용(Multi-factor)해야 하며, 최상(Extreme)의 서비스에서는 해당 인증수단을 안전한 하드토큰인 보안모듈(HSM)을 통해 관리할 것을 권고한다.

[표 10]에 제시된 인증수단 선택기준은 다양한 인증수단이 가지는 특징, 인증시스템 이용환경 및 별도의 보안성 향상 대책 등에 따라 그 기준과 예는 달라질 수 있다.

6.3 인증수단 이용기준

u-IT 서비스 환경에서는 다양한 인증수단이 이용될 수 있다. 본 논문에서는 그 중에서 많이 이용되고 있는 패스워드, 공인인증서와 같은 인증수단을 안전하게 이용하기 위한 기본적인 이용기준의 예를 제시한다.

인증수단 이용기준은 각 인증수단의 일반적인 이용 형태에 기반하고 있으며, 다양한 이용환경과 강화된 보안대책 등에 따라 인증수단별 이용기준 및 그에 따른 등급은 달라질 수 있다.

6.3.1 패스워드

① 신원확인

패스워드는 온라인 신원확인을 통해 발급된다. 패스워드가 가지는 보안요구사항의 수준에 따라 인증수준이 달라지며 본 논문에서는 3등급과 4등급으로 구분되어 설명된다. 패스워드 발급을 위한 온라인 신원확인 시 등급별로 확인되어야 하는 신원확인 정보는 [표 11]과 같다.

3등급 패스워드의 경우 신원확인 정보에 대하여 이메일 발급기관, 신용카드 사, 관리자가 속한 회사 등을 통해 검증이 필요하며, 신원확인 정보와 관련된 기록과 등록정보는 패스워드 인증기관이 일정 기간 보관하여야 한다. 또한, 3등급 패스워드의 경우, 패스워드 인증기관과 신원정보 검증기관간 정보통신망을 통해 전달되는 신원확인 정보는 전자서명 및 암호화되어야 하며, 패스워드 신청자와 패스워드 인증기관간 정보통신망을 통해 전달되는 신원확인 정보 또한 암호화되어야 한다.

〔표 11〕 패스워드 발급을 위한 신원확인 정보

인증대상 \ 인증수준	3등급	4등급
사람	· 이메일 · 신용카드 정보 등	· 이메일
기기 · 사물	· 기기 등 관리자 이메일 · 시리얼번호, MAC 어드레스 등의 기기 식별정보 · 관리자임을 증빙할 수 있는 서류	· 기기 등 관리자 이메일 · 시리얼번호, MAC 어드레스 등의 기기 식별정보

② 생성·등록

패스워드 생성 시 [표 12]와 같은 패스워드 구성을 만족해야 한다.

3등급 패스워드의 경우, 패스워드 생성 후 이를 패스워드 인증기관에 등록을 위해 전송 시 암호화하여 전송해야 한다. 또한 패스워드 등록 시 신원확인 정보 중 하나를 다시 확인하는 등 패스워드에 대한 정당한 신청자

〔표 12〕 패스워드 구성

인증대상 \ 인증수준		3등급	4등급
사람, 기기 · 사물	문자 종류	알파벳 대 · 소문자, 특수기호, 숫자 등	
	문자 구성 및 길이	· 3가지 종류 이상의 문자구성으로 8자리 이상의 길이 · 2가지 종류 이상의 문자구성으로 10자리 이상의 길이	· 3가지 종류 이상의 문자구성으로 6자리 이상 · 2가지 종류 이상의 문자구성으로 8자리 이상의 길이
	특정 정보 이용 및 패턴 조건	· 한글, 영어 등의 사전적 단어를 포함하지 않음 · ID와 연관성이 있는 단어구성을 포함하지 않음 · 널리 알려진 단어를 포함하지 않거나 예측이 어렵도록 가공한 패스워드 이용 ※ 널리 알려진 단어 : 컴퓨터 용어, 기업 등의 특정명칭을 가공하지 않고 그대로 사용하는 경우 · 제3자가 쉽게 알 수 있는 개인정보를 포함하지 않음 ※ 개인정보 : 가족이름, 생일, 주소, 휴대전화번호 등 · 이전 패스워드와 연관성이 있는 단어구성을 포함하지 않음	

인지를 확인하여야 한다.

③ 관리

패스워드 인증기관 등 사용자의 패스워드를 관리하는 기관은 사용자의 패스워드와 이에 관련된 주요 데이터를 모두 암호화하여 저장하여야 한다. 사용자의 경우 자신의 패스워드는 암기하여 사용하는 것이 원칙이며, 기기·사물은 메모리 등에 암호화하여 저장하여야 한다.

패스워드 소유자는 자신의 패스워드가 제3자에게 노출되었을 경우 즉시 새로운 패스워드로 변경하여야 한다. 패스워드 인증기관은 언제든지 사용자가 자신의 패스워드를 변경할 수 있도록 패스워드 변경기능을 제공하여야 한다. 또한 사용자로부터 패스워드 변경 요청이 있을 경우 사용자 신원확인이 완료 된 후 패스워드 변경을 처리하여야 한다.

등록된 패스워드는 주기적으로 패스워드 소유자에 의해 변경되어야 하며, 그 주기는 3등급의 경우 6개월 이하, 4등급의 경우 12개월 이하로 권고한다.

④ 이용·검증

패스워드 소유자가 3등급 패스워드를 통해 패스워드 이용기관으로부터 인증 받고자 하는 경우, 양 당사자간 정보통신망을 통해 전달되는 정보는 암호화되어야 한다. 또한, 패스워드 인증기관으로부터 해당 패스워드에 대한 검증정보가 패스워드 이용기관으로 전달되는 경우, 해당 정보통신망을 통해 전달되는 검증정보는 암호화 및 전자서명 되어야 한다.

패스워드 인증기관으로부터 전달된 패스워드 검증정보는 패스워드 이용환경을 고려하여 검증정보에 대한 유효기간이 설정되어야 한다. 또한, 패스워드 이용기관은 패스워드 소유자가 패스워드를 이용하여 로그인하고 일정 시간이 경과된 경우 자동 로그아웃 등의 기능을 제공하여야 하며, 사용자가 패스워드를 3회 이상 오류 입력시 별도의 절차를 통해 해당 패스워드를 이용할 수 있도록 해야 한다.

6.3.2 공인인증서

① 신원확인

공인인증서가 가지는 보안요구사항의 수준에 따라 인증수준이 달라지며 본 논문에서는 1등급과 2등급으로 구분되어 설명된다. 공인인증기관은 공인인증서 신청자를 직접 대면하여 신원확인 후 공인인증서를 발급한다. 공인인증기관은 인증기관을 대신하여 공인인증서 신청자에 대한 신원확인업무를 수행하는 인증서 등록대행기관을 둘 수 있다. 공인인증기관 또는 인증서 등록대행기관이 공인인증서 신청자에 대한 신원확인 시 확인하여야 하는 정보는 [표 13]과 같다. 신원확인증표의 경우, 전자서명법 시행규칙 제13조의3이 규정을, 신원확인 방법 및 기준의 경우 제13조의2 규정에 따른다. 기기·사물에 대한 공인인증서 발급 시 시리얼번호, MAC 어드레스 등 기기사물에 대한 식별정보와 기기관리자에 대한 추가적인 정보가 요구된다.

공인인증기관은 공인인증서 신청자가 제시한 신원정보의 정당성을 확인하기 위해 제3의 신원정보 검증기관을 통해 신청자의 신원정보를 검증할 수 있다. 예를 들어 주민등록증의 진위 여부 확인을 위해서 행정기관에 문의하여 신청자가 제시한 증표의 발급일자 등을 확인할 수 있다. 또한 기기관리자에 대한 진정성 확인을 위해서 소속 회사 또는 기관에 기기 관리자에 대한 신원을 확인할 수 있다. 공인인증기관은 신원정보 검증을 위

〔표 13〕 공인인증서 발급을 위한 신원확인 정보

인증수준 / 인증대상	1등급	2등급
사람 (개인)	· 신원확인증표에 기재된 성명, 주민번호, 사진 · 신용카드, 은행계좌를 이용한 성명, 생년월일, 주소 등	· 신원확인증표에 기재된 성명, 주민번호, 사진 ※ 금융실명법에 의한 온라인신원확인 가능
기기 · 사물	· 관리자의 신원확인증표에 기재된 성명, 주민번호, 사진 · 관리자임을 증빙할 수 있는 서류 · 시리얼번호, MAC 어드레스 등의 기기 식별정보 · 관리자의 신용카드, 은행계좌를 이용한 성명, 생년월일, 주소 등	· 관리자의 신원확인증표에 기재된 성명, 주민번호, 사진 · 관리자임을 증빙할 수 있는 서류 · 시리얼번호, MAC 어드레스 등의 기기 식별정보

해 신원정보 검증기관과 송수신 시 송수신 상대방을 인증하여야 하며, 정보통신망을 통해 전달되는 송수신 정보를 암호화 및 전자서명하여야 한다.

공인인증서는 10년 이상 보관하여야 하고 공인인증서를 이용한 전자거래에 대하여 보관기간에 대한 요구사항이 있을 경우, 공인인증서의 신원정보 관련기록은 그 기간 동안 보관되어야 한다.

② 생성·발급

공인인증서 신청자가 공인인증서 발급 신청 시 공인인증기관과 공인인증서 신청자간 정보통신망을 통해 송·수신되는 데이터는 암호화 되어야 한다. 공인인증기관은 공인인증서 신청자가 인증서 등록대행기관을 통해 신원확인 받은 정당한 신청자인지에 대해 확인하여야 한다.

공인인증기관은 공인인증서 신청자의 전자서명생성키가 해당 신청자에게 속한다는 사실을 확인하여야 한다. 공인인증기관은 전자서명키 길이를 1등급 공인인증서의 경우 2048비트 이상, 2등급 공인인증서의 경우 1024비트 이상으로 하여 공인인증서를 발급하여야 하며 기기·사물의 경우 인증서 내에 시리얼번호, MAC 어드레스 등 기기·사물에 대한 식별정보가 포함되어야 한다.

공인인증기관은 공인인증서 유효기간을 1등급 공인

인증서의 경우 1년 이상, 2등급 공인인증서의 경우 1년 이하로 설정하여 공인인증서를 발급하여야 한다.

③ 관리

공인인증기관은 공인인증서 가입자가 자신의 전자서명키, 전자서명 비밀번호 등 공인인증서 관련 데이터를 안전하게 보관할 수 있도록 암호화 기능 등을 제공하여야 한다. 1등급 공인인증서의 경우 HSM으로 2등급 공인인증서의 경우 하드디스크, 이동식디스크 등을 통해 공인인증서를 저장·이용할 수 있다. 공인인증서 가입자는 공인인증서 이용 시 필요한 전자서명 비밀번호를 주기적으로 변경하여야 한다. 본 논문에서는 그 주기를 1등급의 경우 6개월 이하로 제시한다.

④ 이용·검증

공인인증서 가입자가 공인인증서를 통해 전자거래기관으로부터 인증 받고자 하는 경우, 해당 정보통신망을 통해 전달되는 정보는 암호화 되어야 한다. 또한, 공인인증기관으로부터 해당 가입자의 공인인증서에 대한 검증정보가 전자거래기관으로 전달되는 경우 해당 정보통신망을 통해 전달되는 검증정보는 암호화 되어야 하고 검증결과에 대해 부인방지기능을 제공하여야 한다.

전자거래기관이 공인인증기관으로부터 전달받은 공인인증서 검증정보가 [표 14]의 유효기간 내에서 신뢰되도록 유의하여야 한다.

〔표 14〕 공인인증서 검증정보 유효기간

인증수준 / 인증대상	1등급	2등급
사람 및 기기·사물	공인인증기관으로부터 검증정보가 전달된 시간	공인인증기관이 발급한 CRL 유효기간 내

Ⅶ. 결 론

본 논문에서는 유비쿼터스 환경에서 신뢰된 인증 환경 조성을 위한 u-인증 프레임워크로서 u-인증서비스 모델 및 도입절차, u-IT 서비스 위험평가 방법 및 위험수준별 인증수단 요구사항, 그리고 인증수단 선택 및 이용기준 등을 제시하였다.

향후 이러한 u-인증서비스 도입절차와 인증수단 선택 및 이용기준을 기반으로 유비쿼터스 환경의 각 인증수단 별 보안요구사항을 제시할 것이고, 이러한 연구를 통해 u-City로 대변되는 유비쿼터스 사회의 신뢰된 인증환경 조성이 가능하게 될 것이다.

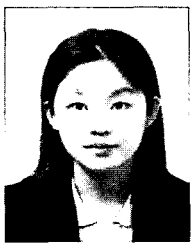
참고문헌

[1] http://www.cio.gov/eauthentication/index.cfm
[2] http://eap.projectliberty.org/docs/EAP_Temoshok_2-12-04.ppt
[3] http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
[4] http://www.cio.gov/eauthentication/documents/eRAv15 guide.pdf
[5] http://www.cio.gov/eauthentication/credential_suite.cfm
[6] 전자서명법 시행규칙, 제13조의2(신원확인의 기준 및 방법)
[7] http://www.verisign.com/products-services/security-services/pki/pki-application/cable-modem-services/cable-modem-authentication/page_001468.html

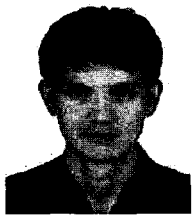
〈著者紹介〉

김 영 준 (Young-Jun Kim)
2002년 2월 : 고려대학교 컴퓨터학과 석사
2004년 10월~2005년 5월 : (주)엔텔스 기술연구소
2005년 8월~2006년 6월 : 미국 NC State Univ., Computer Science Dept., 박사과정
2006년 12월~현재 : 한국정보보호진흥원 전자인증팀 주임연구원
<관심분야> 정보보호, PKI

황 보 성 (Bo-Sung Hwang)
2001년 2월 : 순천향대학교 전산학과 석사
2001년 1월~현재 : 한국정보보호진흥원 전자인증팀 선임연구원
<관심분야>정보보호, PKI



김 정 희 (Jung-Hee, Kim)
1997년 2월 : 중앙대학교 산업정보학과 졸업
1999년 2월 : 중앙대학교 산업정보학과 석사
1999년 1월~8월 : 한국정보보호센터 연구원
1999년 9월 ~ 2001년 8월 : (주)쌍용정보통신 사원
2001년 9월~현재 : 한국정보보호진흥원 전자인증팀 선임연구원
<관심분야> PKI, RFID 정보보호, 시스템개발방법론



백 종 현 (Baek, Jonghyun)
1996년 2월 : 순천향대학교 전자공학과 졸업
1998년 2월 : 순천향대학교 전자공학과 석사
2001년 4월~현재 : 한국정보보호진흥원 전자인증팀장
<관심분야> 정보보호, PKI