미래인터넷 서비스와 User-Centric Identity Management

2008.8.27

진승헌(jinsh@etri.re.kr)

디지털ID보안연구팀
정보보호연구본부

ETRI 한국전자통신연구원
Electronics and Telecommunications Research Institute

들어가면서…

LIGHT READING insider
TARGETED ANALYSIS OF THE TELECOM INDUSTRY

http://www.lightreading.com/insider/document.asp?doc_id=127858

통신사 vs. 포털

새로운 환경에서 누가 승자가 될 것인가?

Telcos Face a Web 2.0 Identity Crisis

Dawn Bushaus | Analyst, Light Reading |

Like it or not, telecom network operators are on a collision course with a group of competitors that pose long-term challenges extending beyond conventional services such as voice, data, and video. Companies that are approaching next-gen services from a non-telecom (i.e. Web 2.0) framework are angling to disintermediate network operators, relegating them to supplying bandwidth and little more.

As the latest edition of *Light Reading Insider* details, identity management (IdM) will be a key enabler of that transparent, all-encompassing user experience. In a nutshell, IdM is an integrated system of business processes, policies, and technology that lets an organization control user access to online applications or services while protecting the user's privacy and the organization's resources. In other words, an IdM system can be the gatekeeper to the entire user experience.

Providing an integrated IdM experience isn't going to be easy, and it isn't going to be cheap. But as the latest *Insider* points out, next-gen competitors such as Google (Nasdaq: GOOG) are deploying Web 2.0 technologies to achieve robust IdM. If network operators cede IdM leadership to these competitors, they will lose an important mechanism for customer retention – as well as potentially significant revenue.

Forward-looking operators see the threat and are acting on it. TA Orange Co. Ltd. , the wireless arm of France Telecom SA (NYSE: FTE), is among a handful of European and Asian network operators that are implementing IdM technology and learning to become identity providers – companies that can, in effect, vouch for a user's identity in transactions with Web-based service providers. Orange may not really know yet how it's going to make money as an identity provider, but the company is certain that IdM will help it deliver services that can reduce customer churn.

There's no clear-cut path to IdM supremacy, but network operators aren't in position to wait until that roadmap is in place. "The biggest fear that telcos have is to become pipe providers," notes Guillaume Garnier de Falletans, a project manager working on identity management at Orange. "To maximize profit, we definitely have to provide more and more services to our customers. We need to manage their identities if we want to keep them loyal."

미래 인터넷 서비스 요구사항

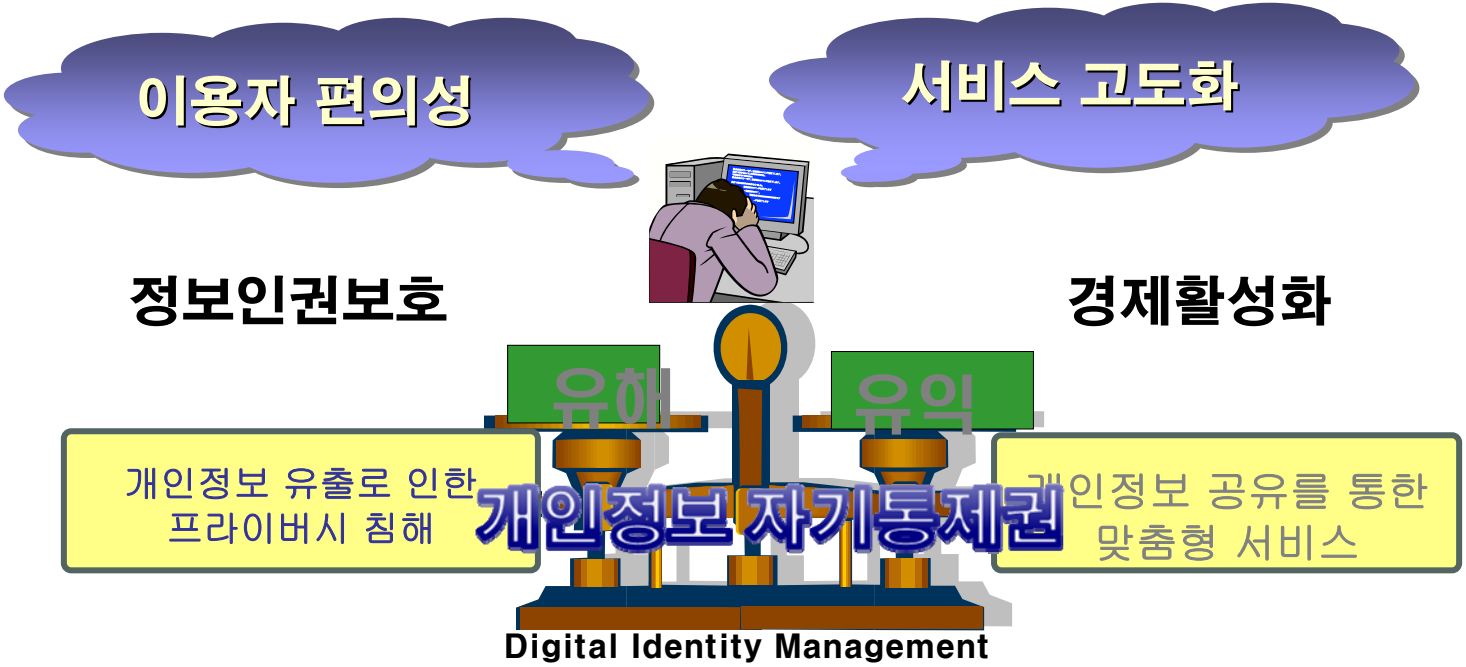
- ‘나’를 중심으로 (I-Centric)
- 상황을 인지하고 (Situation Aware)
- 선호도를 고려하여 (Considering user’s preference)
- 필요에 따라 능동적으로 서비스를 제공받으며 (Proactive Service Provisioning)
- 어떤 상황에서도 서비스의 연속성을 보장 (Seamless Service)

개인화서비스 vs. 프라이버시 보호 선택의 문제인가?

출처 : 김상기(ETRI), “미래인터넷에서의 서비스요구사항”

사회적 이슈와 IdM의 필요성

*. 아이핀 도입을 의무화에 대한 한국인터넷기업협회 반발 [출처 : 디지털타임즈 '08.5.27]

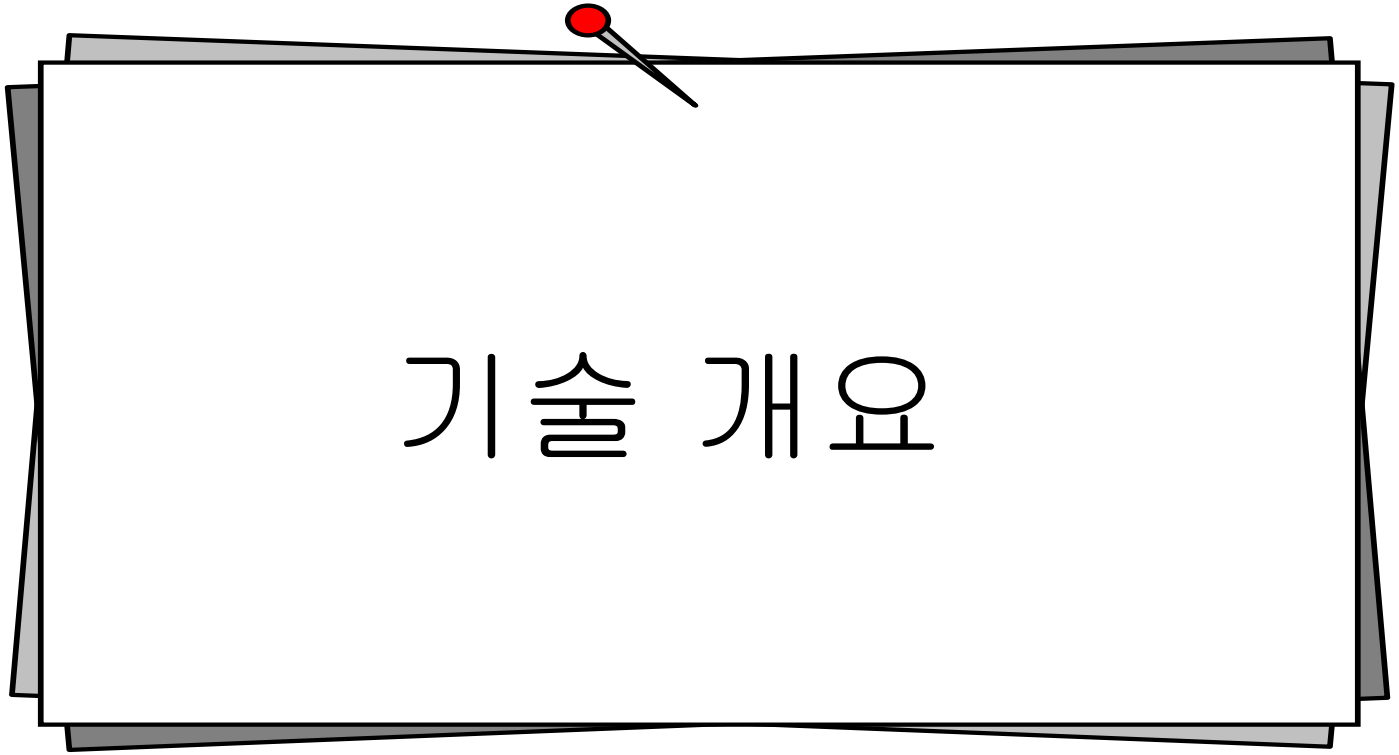


*. 온/오프라인에서 개인정보(주민번호 포함)를 요구하는 관행 개선에 대한 검토 필요
*. 공급자 중심이 아닌 수요자/서비스 중심의 검토가 필요함

차세대 네트워크의 발달과 차별화된 서비스에 대한 사용자의 요구에
개인화된 서비스의 중요성이 증가함에 따라 이와 같은 이슈는 더욱 증가 할 것임

일방적인 선택의 문제가 아니며, 균형잡힌 접근이 필요함

목 차



기술 개요

Identity 개념

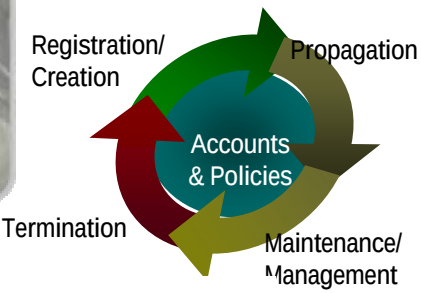
Identity

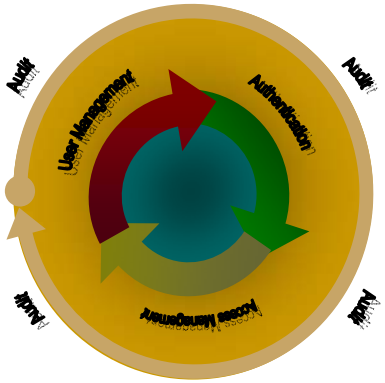
- 엔터티(Entity)가 묘사되거나 인지되거나 또는 알게되는 속성들 (ITU-T)
- 지역, 기업, 국가, 글로벌 같은 지정된 콘텍스트 내에서 객체를 유일하게 식별할 수 있는 기본 개념(OpenGroup)
- 누군가를 특정할 수 있는 주장(Claims)들의 집합(Microsoft)
- 개인정보라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명 · 주민등록번호등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.[공공기관의개인정보보호에관한법률 제2조2항]

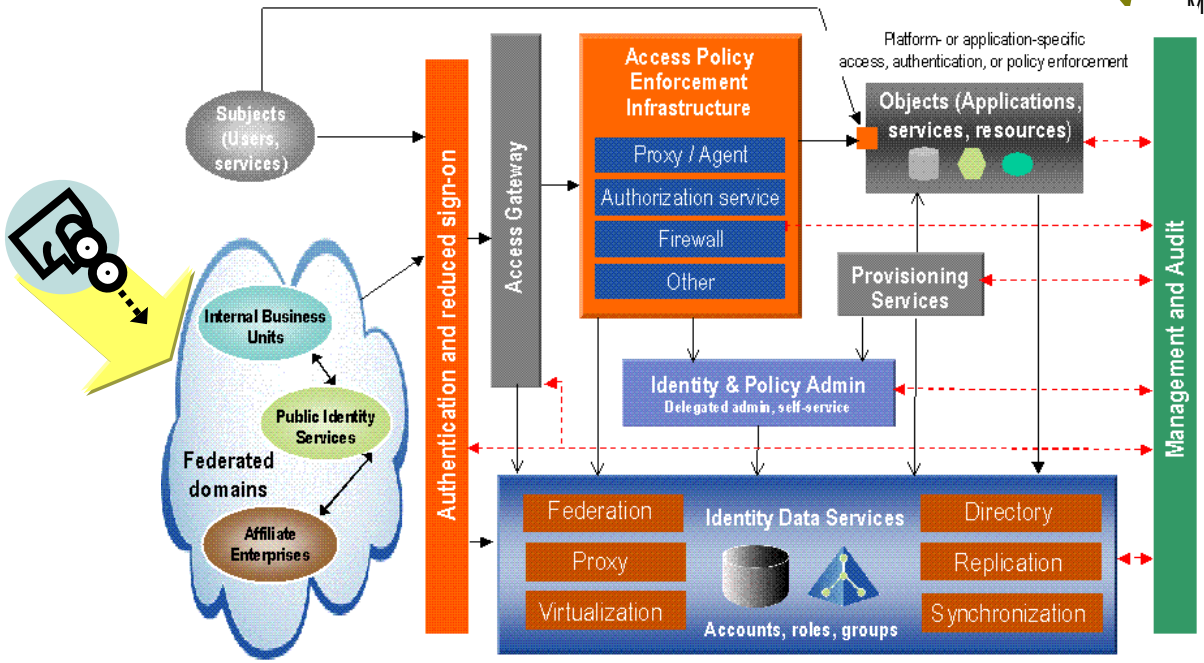
Identity Management 개념

Identity Management

- Identity의 생성, 이용, 폐기를 위한 생명주기 관리 및 인증, 인가, 감사를 위한 기반구조





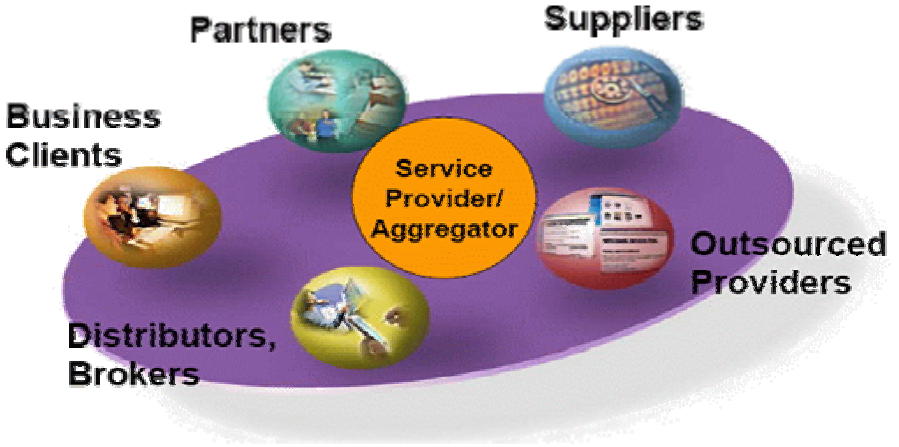


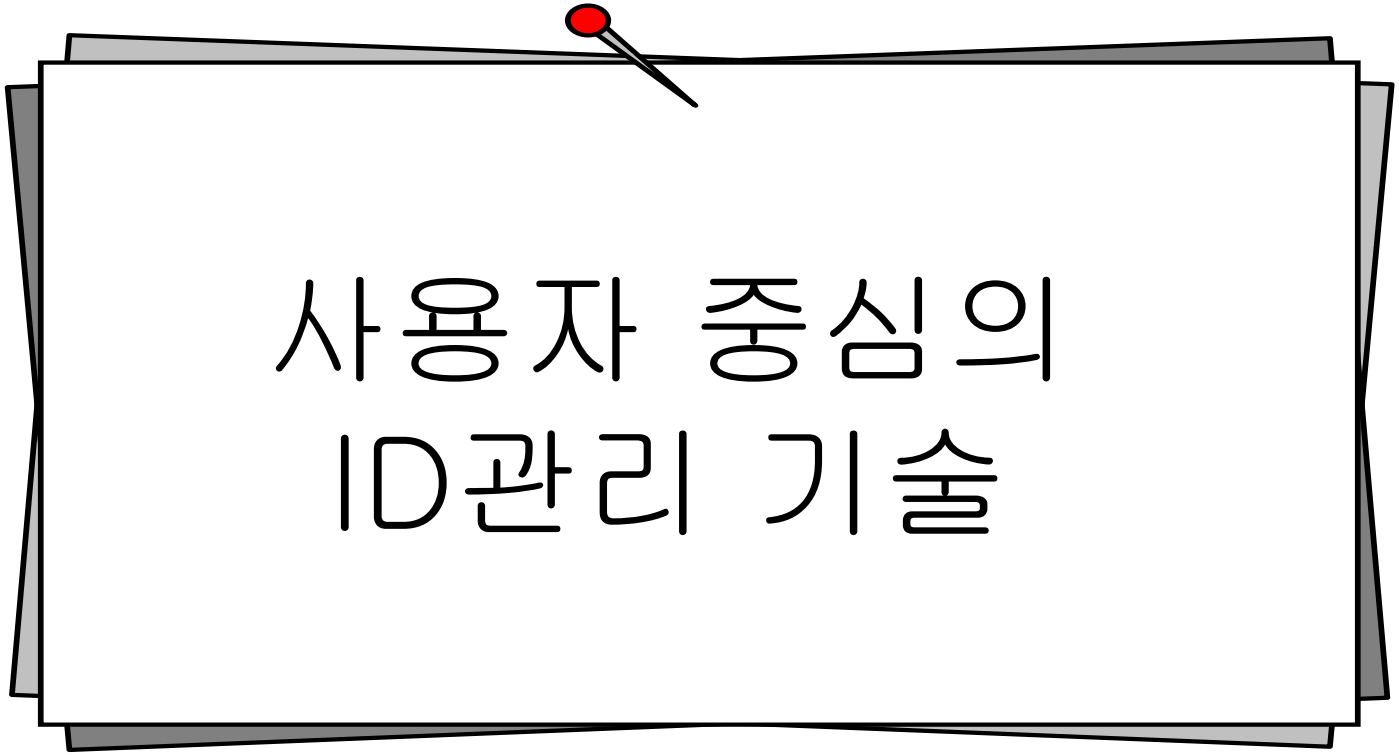
Architecture Template for IDM

출처 : Burton Group 2006

IdM(Identity Management)의 목적

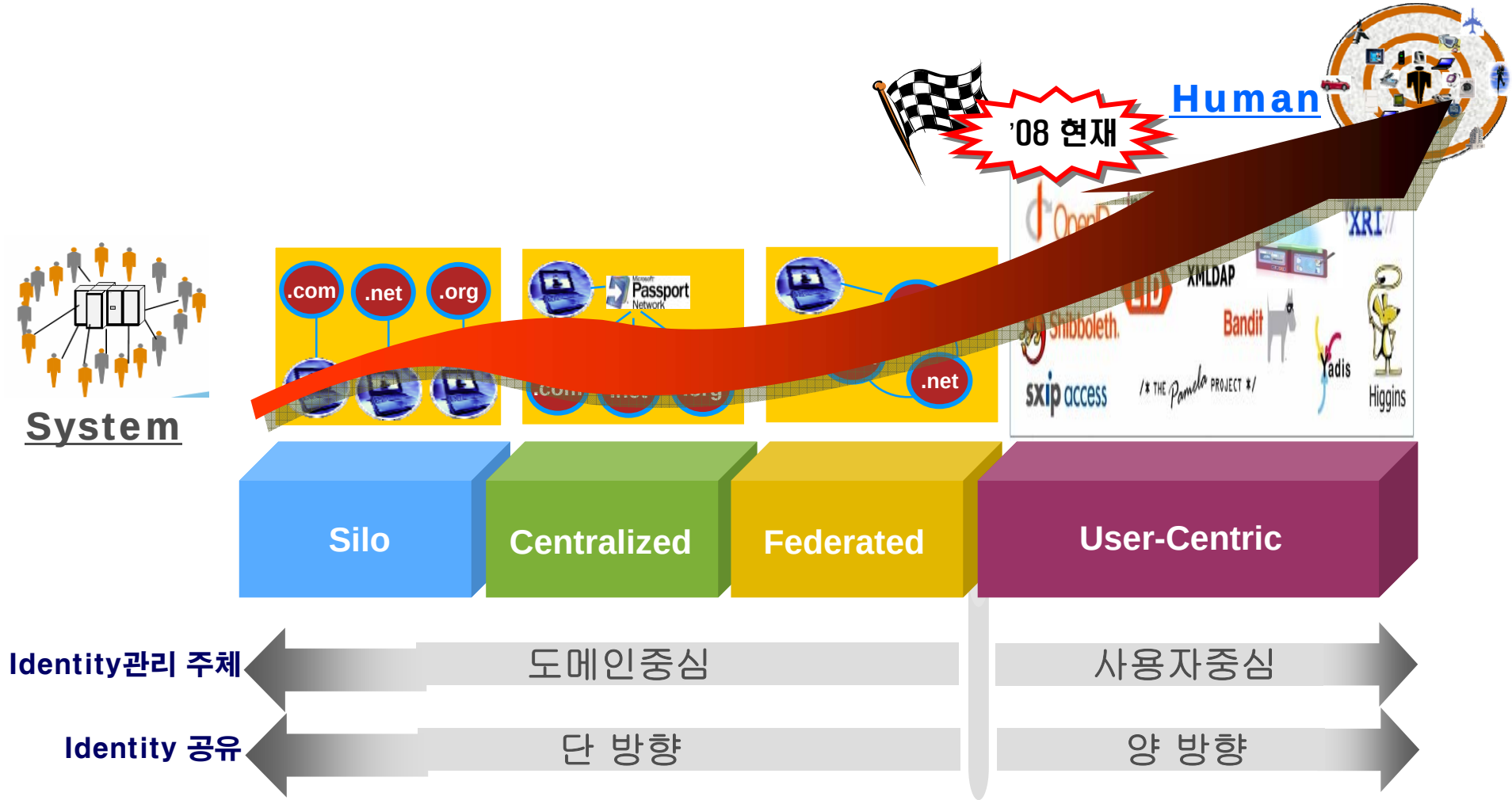
- **인터넷 서비스 증가에 따른 개인 보유 ID 수의 증가 : 이용 불편 개선**
  - 우리나라 네티즌들 평균 27개 사이트에 가입, 7.5개의 ID 보유 [전자신문, '05.2.23]
- **조직내 ID관리 요구 증가 및 비즈니스 관계 다변화 : 효율&생산성 증대**
  - SSO 및 EAM&IAM 수요 증가, 인트라넷 -> 인터넷 [DigitalIDWorld Newsletter,'05.3.31]
- **개인정보 기반의 맞춤형 서비스 요구 증가 : 신규 IT 서비스 창출 및 개인정보보호 증대**
  - 웹2.0 기반의 신규 서비스 창출을 위해서는 프라이버시 보호가 필수적임[ZDNet, '06.12]





사용자 중심의 ID관리 기술

IdM 의 진화



사용자 中心 : 자신이 원하는 시간과 장소에 자신의 목적에 맞는 서비스를 쉽고 안전하게 받을 수 있음
(사용자는 What만 관심을 갖고 How는 신경쓰지 않도록)

User-Centric Identity 개념

출처 : OASIS, The Core Concept of Identity 2.0

User consent

- User always can allow or deny whether information about them is released or not (reactive consent management)

User control

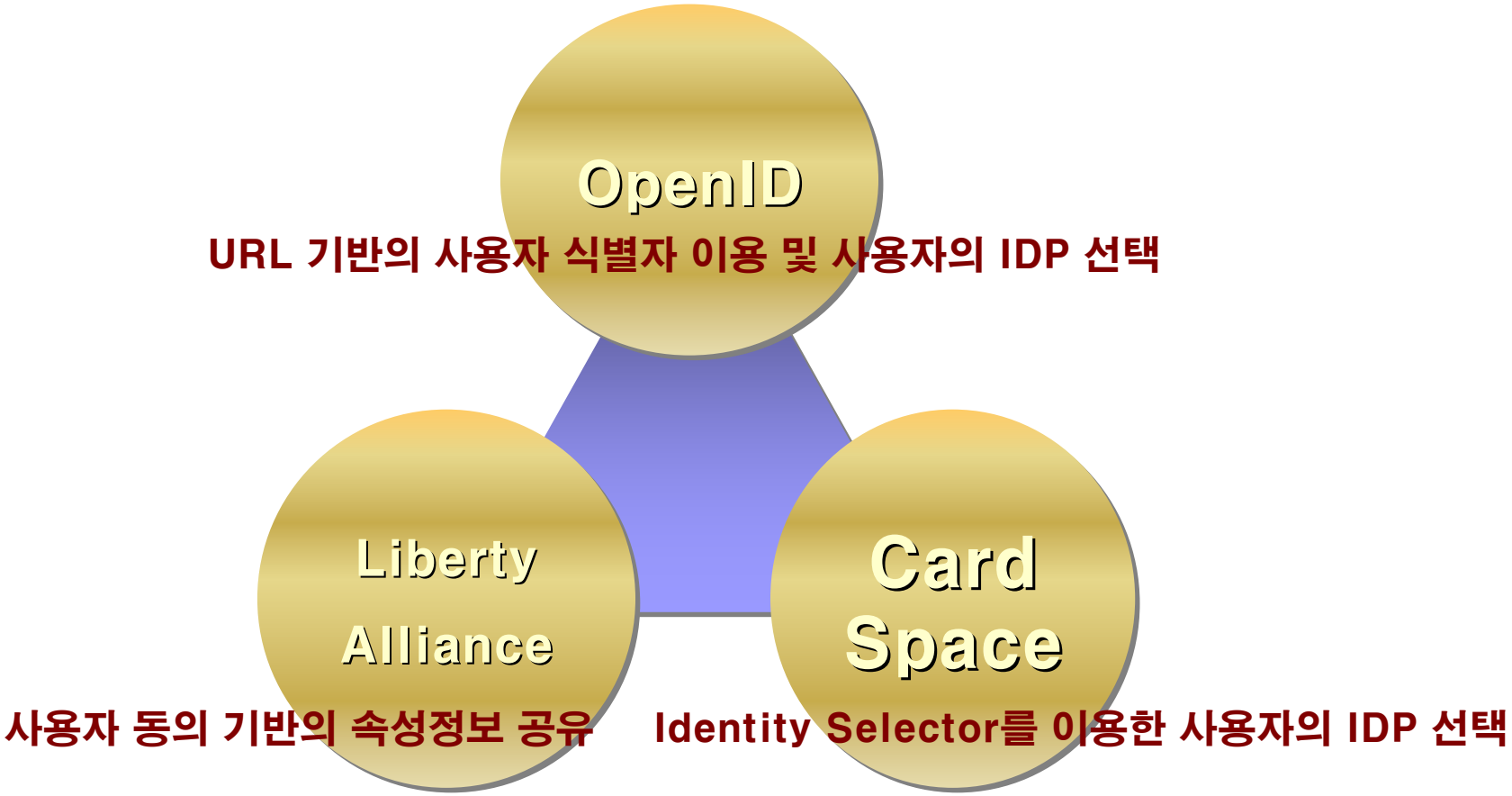
- User has ability to policy-control all exchanges of identity information (proactive consent management)
- User delegates decisions to identity agents controlled through policy

User-centered

- Core subset of the previous two as ‘People in the protocol’
- User is actively involved in information disclosure policy decisions at run time

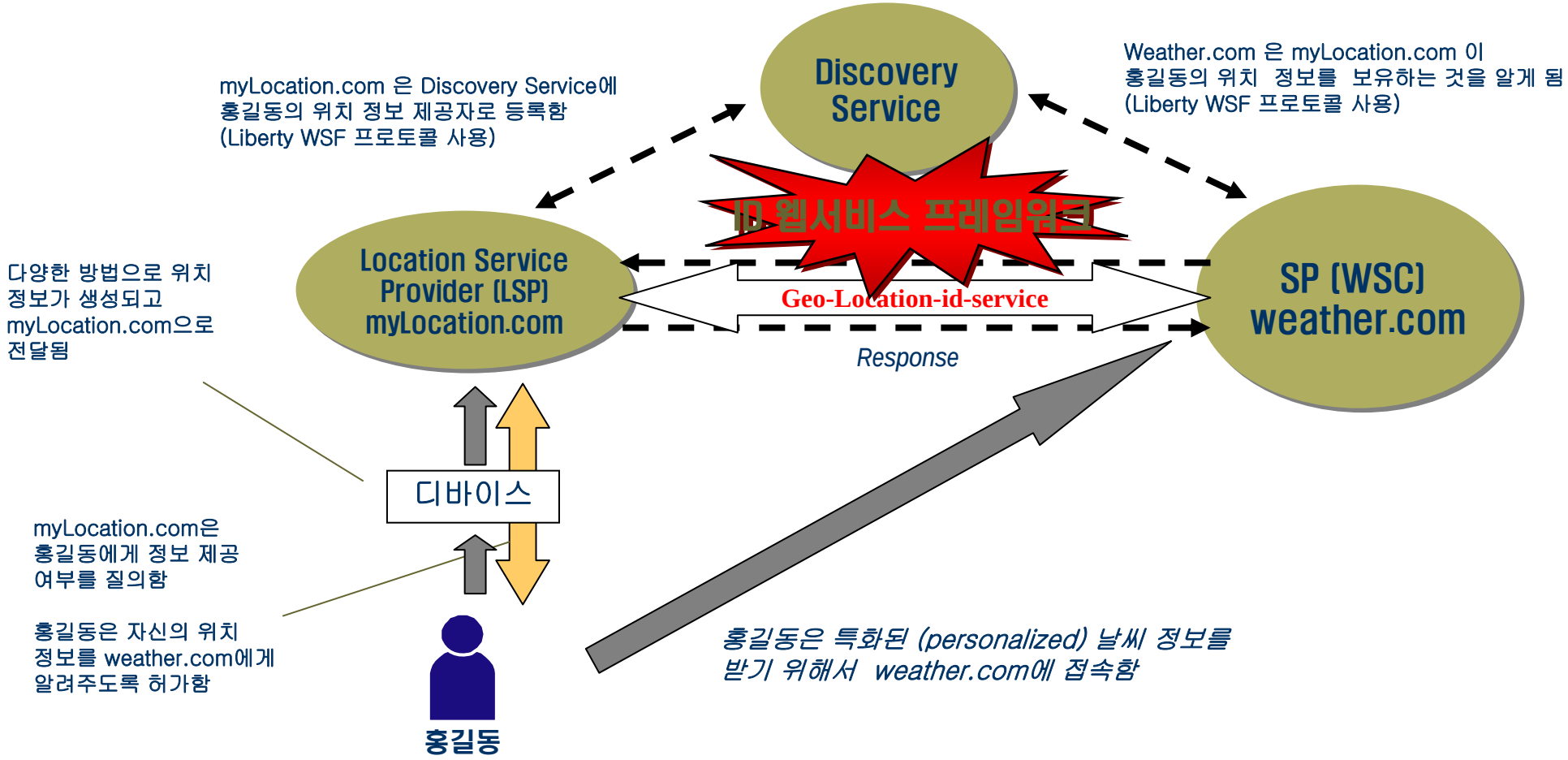
주요 사용자 중심의 IdM 기술

각 기술들의 사용자중심의 특성들



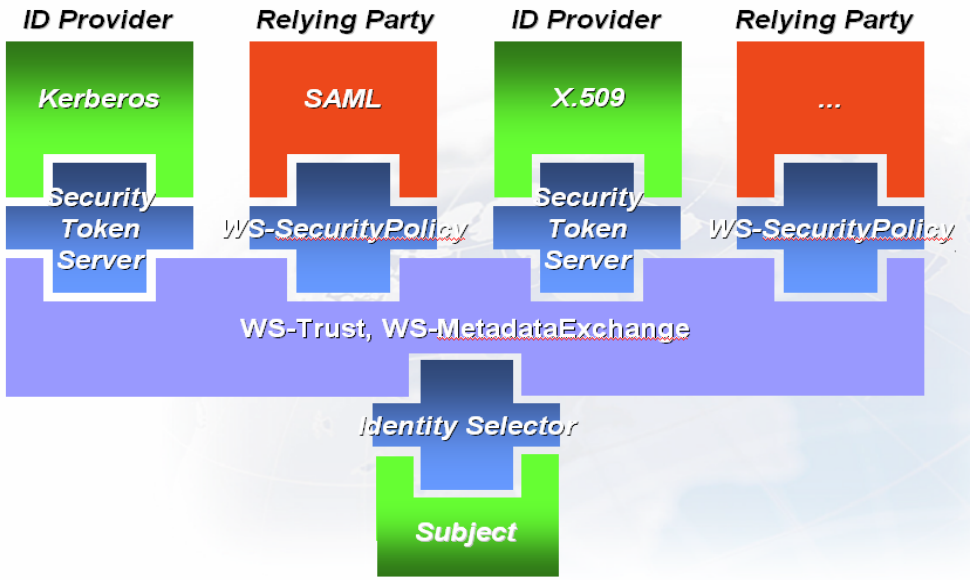
Liberty Alliance (ID-WSF)

Permission-based Attributes Sharing



Microsoft CardSpace

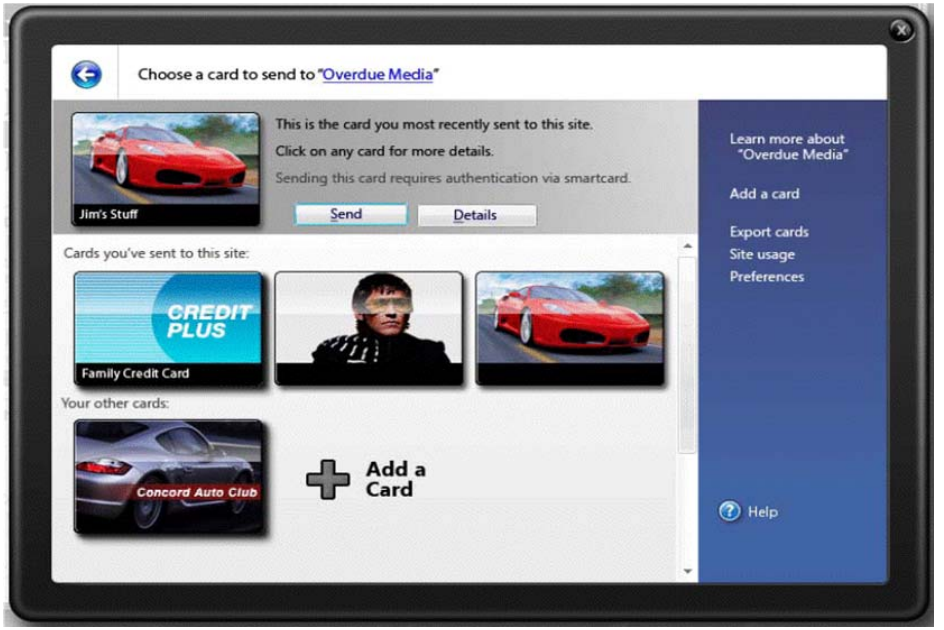
Microsoft



Identity Metasystem Architecture

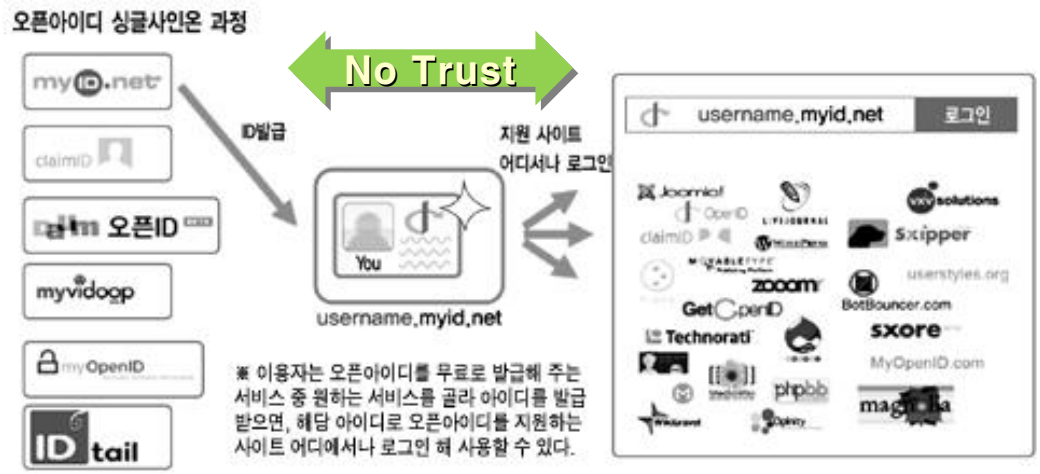
Kim Carmeron – 운영과 기술의 다양한 제공
I&AM Architect, Microsoft Corp.

CardSpace – Vista 채택



OpenID

URL 기반의 사용자 중심 Identity를 위한 분산형 공개 표준 기술



출처 : 디지털타임즈 2008.1

야후, 「OpenID」 지원 발표

Caroline McCarthy (CNET News.com) 2008/01/21 원문보기

야후가 17일(미국시간) 공

'오픈ID 2.0' 지원을 밝혔다.

용성 흐름이 빨라지는 가운데 중요한

오픈ID 재단에 구글, MS, 야후 등 참여

Caroline McCarthy (CNET News.com) 2008/02/11 원문보기

SAVE 폰트

추진하는 미국의 오픈

일(미국시간) 구글,

관계자가 이사회의 첫 기업 일

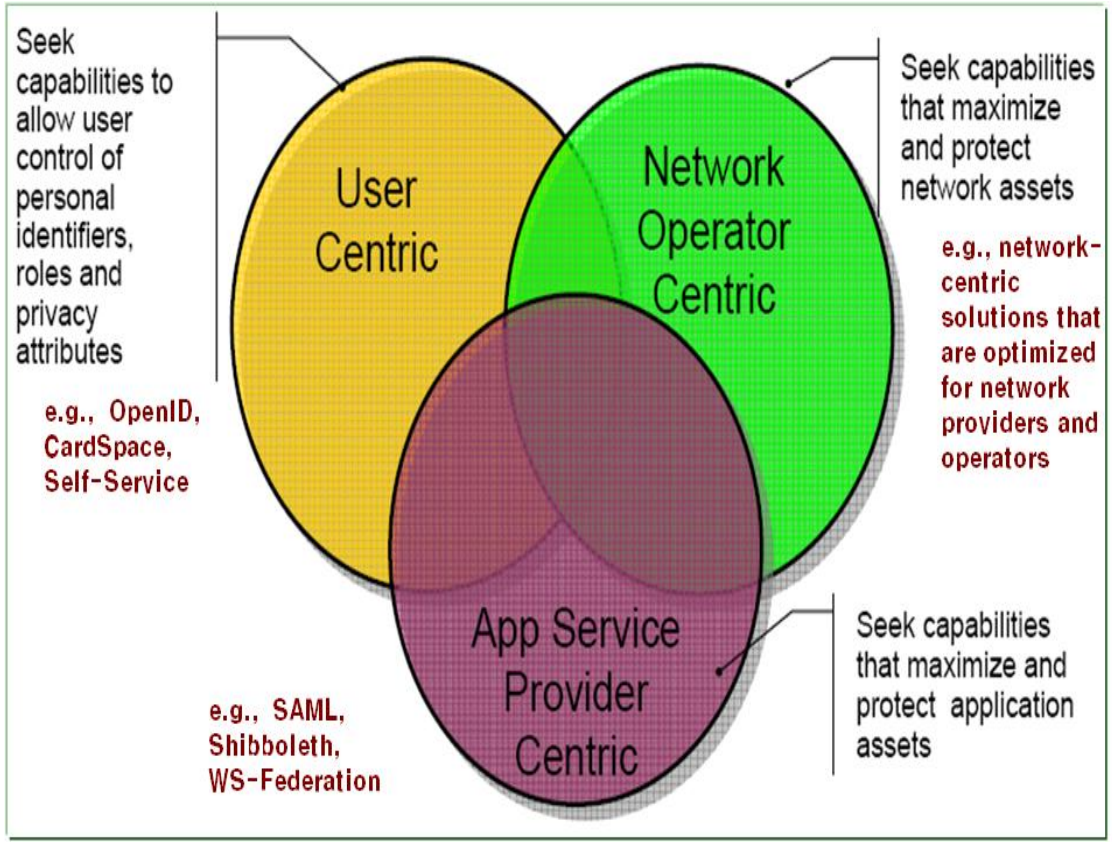
원이 되었다고 발표했다.

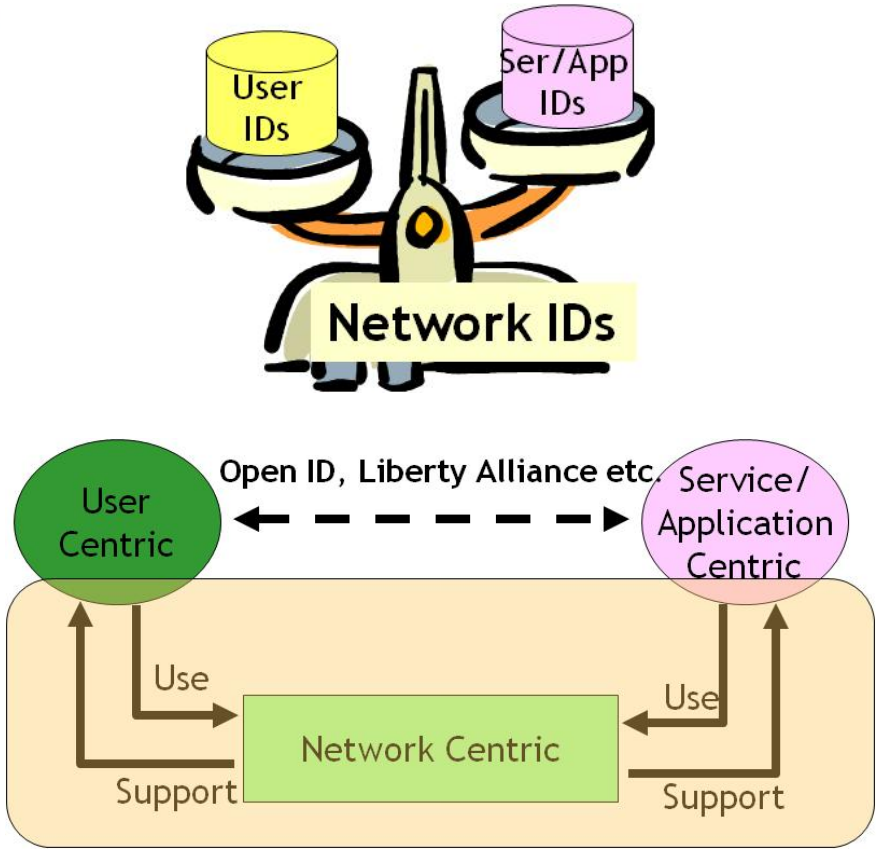
신뢰??

OP & RP??

표준화 동향(국외: ITU-T SG17 IdM FG)

Current View of IdM Landscape





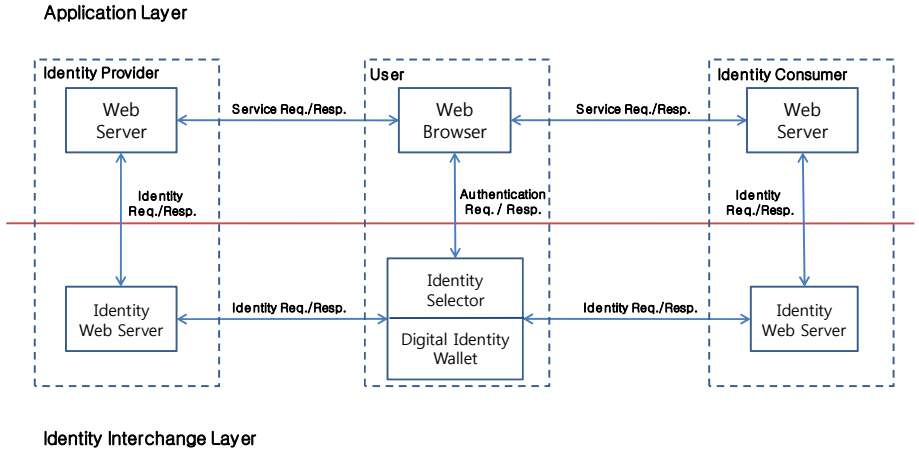
출처 : Report on Identity Management Use Cases and Gap Analysis, ITU-T FG IdM

표준화 동향(국외: ITU-T SG17 Q.6)

Question6/17 – Cyber security

- Proposal of first draft Recommendation on X.idif: User Control Enhanced Digital Identity Interchange Framework
  - 2007년 12월 ITU-T SG17 Q6에 제안하여 TD로 채택
  - 기고문의 주요내용은 자기통제 강화형 디지털ID 공유 기술에서 ID 공유 프레임워크를 정의하여 독립적으로 사용자 ID를 공유할 수 있는 방안을 제시한 것임
  - IBM의 Michael McIntosh는 향후 X.idif의 표준개발에 지속적으로 공동 참여하기 위해 Co-Editor로 임명됨

Report on Question 6/17



User Control Enhanced Digital Identity Interchange Framework

IdM related issues

- X.idif
  - Q6 reviewed and discussed two following documents ;
    "Proposal of first draft Recommendation on X.idif: User Control Enhanced Digital Identity Interchange Framework (C253R1)"
    and "Using WS-Trust and Information Card Technology to Satisfy the Requirements of the User Control Enhanced Digital Identify Interchange Framework (from the ftp area)
  - Q6 agreed to produce the draft text of X.idif with the two documents by the next meeting, and assigned Michael McIntosh (IBM Research) as a new co-editor. Current editors: Sangrae Cho (ETRI) and Mike McIntosh (IBM). Current draft Recommendation is in TD 2920R1.
- X.idmreq
  - Editors' version was discussed. Accepted text from the meeting was issued as a draft Recommendation in TD 2881R1.
- X.idm-dm
  - Editors' version was discussed. Accepted text from the meeting was issued as a draft Recommendation in TD 2886R2.

표준화 동향(국내:TTA TC5 PG502)

개인정보보호 및 ID관리 프로젝트그룹 활동영역('08.02 ~)

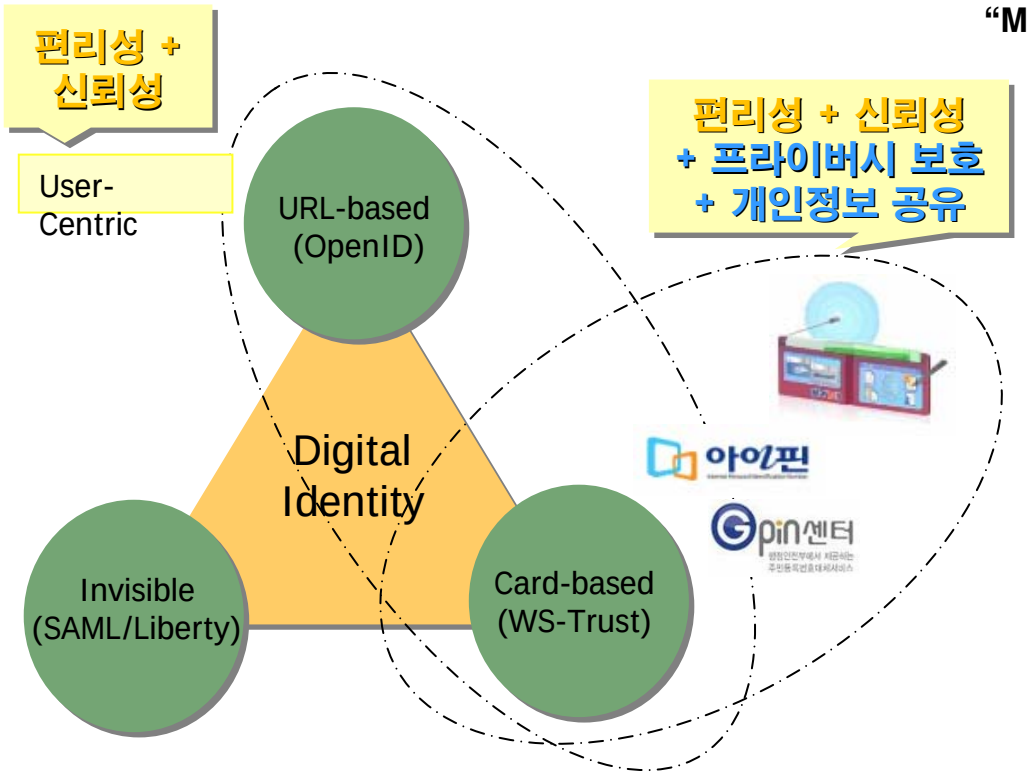
- 개인정보보호를 위한 가이드라인 표준 개발
- 주민등록번호 대체 보호수단(i-PIN) 관련 표준 개발
- ID관리(사용자 중심 ID관리, 응용중심 ID관리, 네트워크중심 ID관리 등) 관련 표준 개발

'08년도 과제 추진 계획

No.	국문 과제명	관련 국제표준	국제표준 준용		국/영문	추진계획 (일정)
			준용여부	준용률		
1	ID 정보의 식별, 디스커버리, 의미, 형식, 공유 프로토콜 및 공통 프레임워크 기술 개발	ITU-T FG-IdM Report	O	30%	국/영문	2008.01~ 2009.12
2	개인정보정책 설정 . 협상 규격 및 개인정보 생명주기별 프라이버시 관리모델 표준 개정	W3C P3P	-	-	국문	2007.01~ 2008.12
3	주민번호대체 기술 및 네트워크 중심 ID 관리 기술 표준 개발	-	-	-	국문	2008.01~ 2009.12

The Identity Landscape

“사용자 중심의 ID 관리 기술에 대한 관심 증가와 기술간의 협업 시도 증가”



The Identity Landscape 2006 **재구성**

Johannes Ernst, CEO of NetMesh

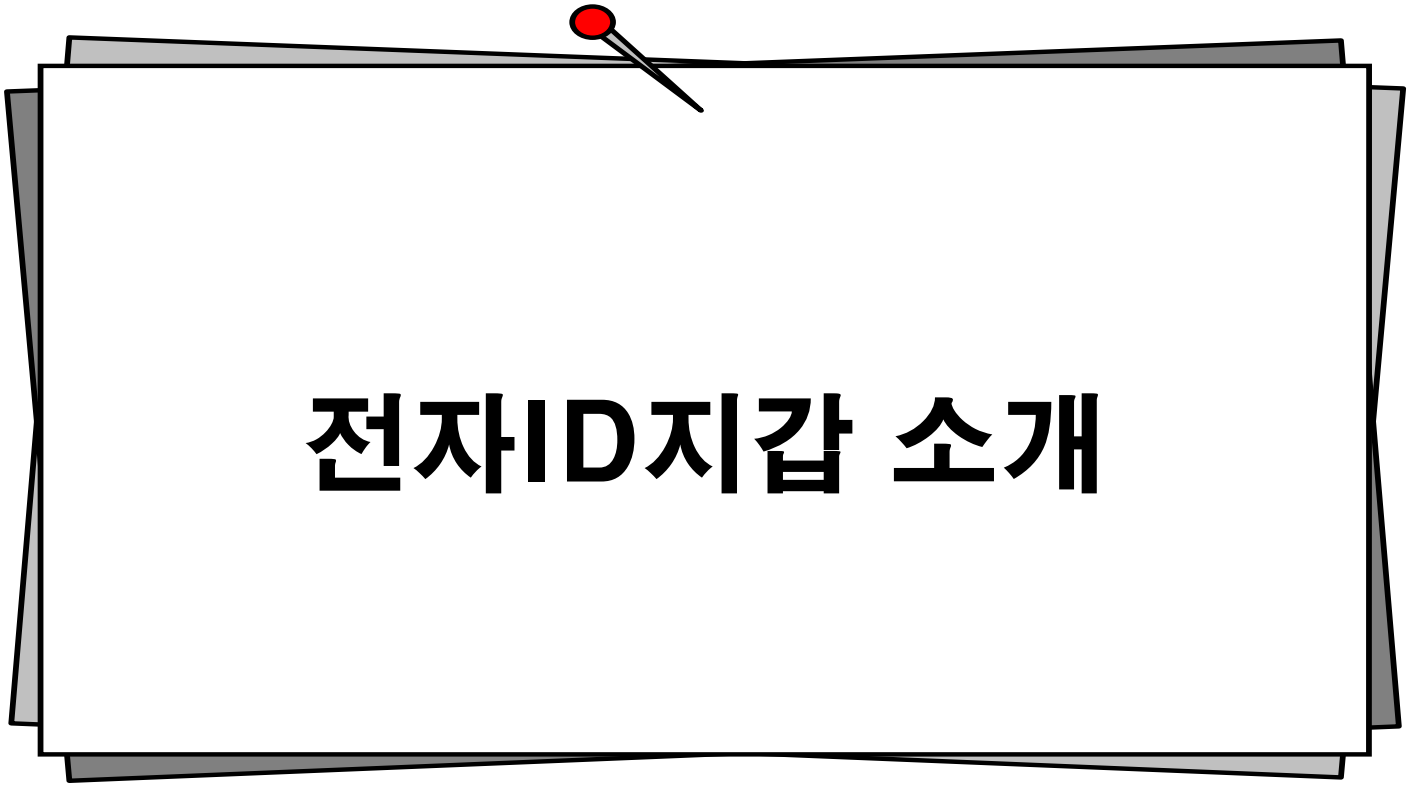
디지털ID**보안연구팀**, ETRI

“MS, 차세대 인증기술 '오픈ID'를 껴안다.”
CardSpace에서 Open ID 지원, Open ID에서 CardSpace의 InfoCard 지원을 위한 상호운용성 확보 계획 발표(‘07.02)

Microsoft OpenID

“ETRI, MS와 ‘전자ID지갑’ 연구 협력”
프라이버시 보호 및 개인정보 공유를 위한 차세대 ID관리 기술의 공동연구 개발 계획을 발표
(‘07.05)

IT R&D Global Leader ETRI Microsoft

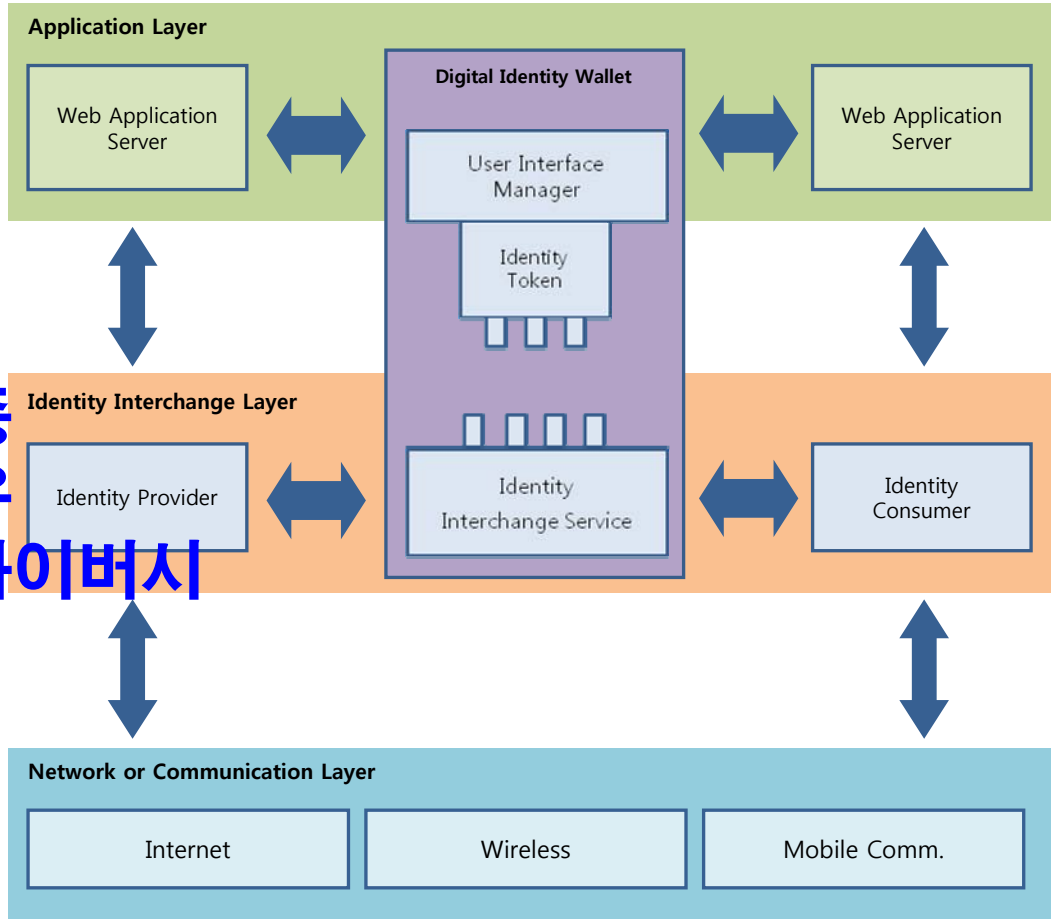


전자ID지갑 소개

배경 : 사용자는 무엇을 원하는지?

- 웹사이트 가입시 개인정보를 매번 입력하는 것이 귀찮아요.
- 특히, 주민번호를 입력하는게 걱정되요.
- 서비스 이용시에 로그인하는 것이 번거로운데, 휴대폰으로 모바일 인터넷을 이용할 때는 더 힘든 것 같아요.
- PC방과 같이 공용PC에서 ID/PWD 입력하는게 걱정되요.
- 내가 접속하고 있는 사이트가 위장 사이트일까 걱정되요.
- 내가 어느 사이트에 가입되어 있는지 기억하기 힘들어요.
- 이사해서 주소가 바뀌었는데, 사이트마다 변경하기가 어려워요.
- A 사이트에 저장된 나의 정보를 B 사이트에 새로 생긴 서비스로 가져가면 좋겠는데, 그럴 수 없어요.

제안배경 : Identity Layer의 필요



인증
공유
프라이버시

Report on Question 6/17

IdM related issues

- X.idif
  - Q6 reviewed and discussed two following documents :
    "Proposal of first draft Recommendation on X.idif: User Control Enhanced Digital Identity Interchange Framework (C253R1)"
    and "Using WS-Trust and Information Card Technology to Satisfy the Requirements of the User Control Enhanced Digital Identify Interchange Framework (from the ftp area)
  - Q6 agreed to produce the draft text of X.idif with the two documents by the next meeting, and assigned Michael McIntosh (IBM Research) as a new co-editor. Current editors: Sangrae Cho (ETRI) and Mike McIntosh (IBM). Current draft Recommendation is in TD 2920R1.
- X.idmreq
  - Editors' version was discussed. Accepted text from the meeting was issued as a draft Recommendation in TD 2881R1.
- X.idm-dm
  - Editors' version was discussed. Accepted text from the meeting was issued as a draft Recommendation in TD 2886R2.

ITU-T SG17 Q.6 X.idif

Editor : ETRI, Co-Editor : IBM, Author : Microsoft

개념 및 정의

전자ID지갑이란 ?

•일상생활에서 사용하는 지갑처럼 인터넷 상에서 사용되는 사이버 지갑

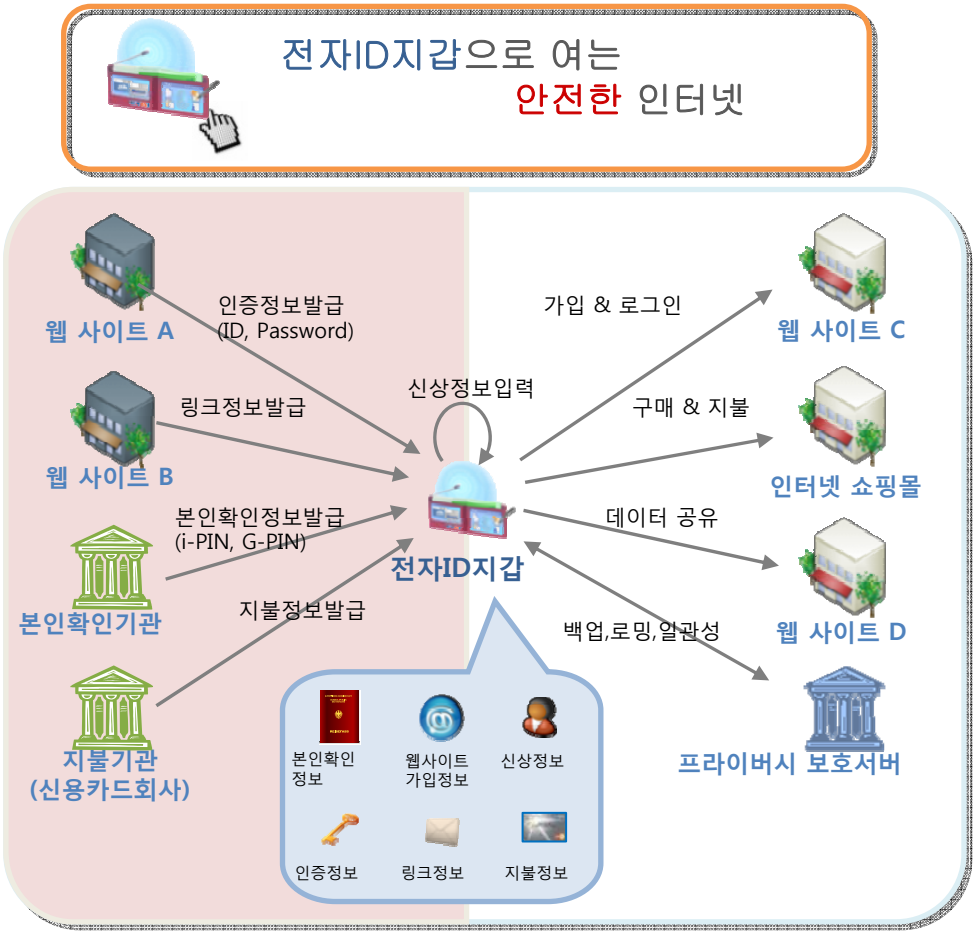
•사용자의 개인정보(주소, 전화번호 등), 인증정보(로그인 아이디, 비밀번호 등), 지불정보(신용카드 등) 같은 Identity 정보를 보관하는 저장소

•Identity 정보를 USB 메모리, 휴대폰과 같은 이동 저장매체에 안전하게 저장하거나 프라이버시 보호서버에 정보 관리를 위탁할 수 있는 시스템

•개인정보의 제공 여부를 사용자가 직접 제어하여 개인정보의 유출 또는 오남용을 방지할 수 있는 시스템

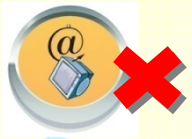
전자ID지갑의 주요기능

•사이트 가입 및 인증
•Identity 공유 및 인증 연동
•사용자 프라이버시 보호
•모바일 Identity 관리

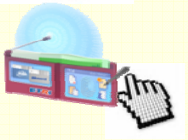


전자ID지갑 서비스

사이트 가입 서비스



피싱 사이트 확인



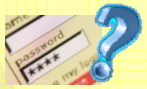
클릭만으로 사이트 가입

가입된 사이트 목록 관리

본인확인 및 인증 서비스

주민번호 대체 본인확인

다양한 인증 수단 연동



원 클릭! 모바일 인증

그 외 응용 서비스

신용·포인트 카드 사용 및 조회

웹 연동 홈 장치에서의 인증

사이버 세계와의 ID 연계

공유 및 동기화 서비스

사이트 간 안전한 정보 공유

변경된 개인정보 자동 동기화

개인정보보호형 맞춤형 서비스
(Personalized Mesh-up Service)

전자ID지갑기반의 인증 연동 기술

IT 인프라 강국에 만족할 것인가?

아니면 진정한 IT 강국이 될 것인가?

경청해 주셔서 감사합니다.