

FIDIS



★ Future of Identity in the Information Society

★ ★ ★ ★ ★
An FP6 Network of Excellence

Johann Wolfgang Goethe – University Frankfurt

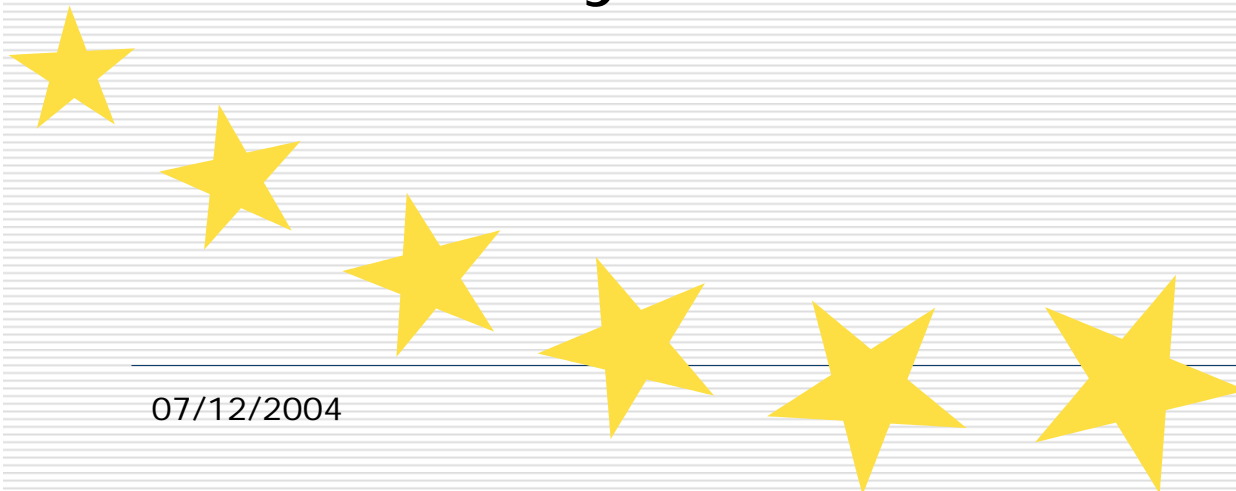
Kai Rannenbergh, Denis Royer
Goethe University Frankfurt
www.fidis.net



Agenda



- Why FIDIS?
- Who is FIDIS?
- FIDIS Aims & Scopes
- First Results
- Summary and Outlook



The initial challenge: “Identity” is changing



- IT puts more HighTech on ID cards
 - Biometrics to bind them closer to a human being
 - Chips to add services (such as a PKI)
- Profiles may make the „traditional“ ID concept obsolete
 - People are represented not by numbers or ID keys any more but by data sets.
 - Identities become “a fuzzy thing”.
- New IDs and ID management systems are coming up
 - Mobile communication (GSM) has introduced a globally interoperable „ID token“: the Subscriber Identity Module
 - Ebay lets people trade using Pseudonyms.
- Europe (the EU) consider joint ID and ID management systems
 - European countries have different traditions on identity card use
 - Compatibility of ID systems is not trivial



Why an EU FP 6 Network of Excellence?



- Consequences of “new” IDs are unclear
 - Privacy
 - Security
 - Forensics
 - ...

- “Change” Trends come from different fields and disciplines
 - Different disciplines see “Identity” in a different way

- Joint work will promote the European Information Society
 - Joint learning from “ID know-how” of different disciplines

⇒ **NoE FIDIS**: An international interdisciplinary **Network of Excellence on the Future of IDentity in the Information Society** (2004-04-01 – 2009-03-31)



Agenda



- Why FIDIS?
- Who is FIDIS?
- FIDIS Aims & Scopes
- First Results
- Summary and Outlook



FIDIS Participants



- Goethe University Frankfurt, D
- AXSionics AG, CH
- BUTE-UNESCO Information Society Research Institute, H
- Europäisches Microsoft Innovations Center GmbH, D
- European Institute of Business Administration, F
- Institut de recherche criminelle de la gendarmerie nationale, F
- Institute for Prospective Technological Studies, E
- International Business Machines Corporation, CH
- Karlstad University, S
- Katholieke Universiteit Leuven, B
- London School of Economics & Political Science, GB
- Masarykova universita v Brne, CZ
- National TU of Athens, GR
- Netherlands Forensic Institute, NL
- SIRRIX Security Technologies, D
- TU Berlin, D
- TU Dresden, D
- Tilburg University, NL
- Unabhängiges Landeszentrum für Datenschutz, D
- University of Freiburg, D
- University of Reading, GB
- VaF, Bratislava, SK
- Virtual Identity and Privacy Research Center, CH
- Vrije Universiteit Brussels, B



Agenda



- Why FIDIS?
- Who is FIDIS?
- FIDIS Aims & Scopes
- First Results
- Summary and Outlook



Vision



- Europe will develop a deeper understanding of how appropriate identification and ID management can progress the way to a fairer European information society.
- Exploration
 - of the relationship between identification and identity in a high tech environment and
 - implications for the workings of democracy and rule of law in the European 'Area of Freedom, Security and Justice' (Art. 29 Treaty of the European Union)



What can FIDIS offer (to Europe)?

What do we want to achieve within (the next) 5 years?



- Being a respected expert player (pool of experts) in the identity discussions
- A collection of Information
 - ID Management systems
 - ID regulation (legislation and case law)
 - How they are used
 - ...
- Expert publications (Deliverables)
- Influencing the scene
 - Research Institutions
 - Scientific Communities
 - Standardisation Bodies
 - Advanced decision makers



Joint Research Topics/Activities



- „Identity of Identity“
 - State of things, taxonomy
- Profiling
- Interoperability of IDs and ID management systems
- Forensic Implications
- De-Identification
- The HighTechID
- Mobility and Identity



Inventory of Topics and Clusters



- Definitions of terms from different perspectives:
 - Philosophical, technical, legal, security,...
- Situated with cases, studies and scenarios, connecting the different terms and disciplines (work in progress)



Agenda



- Why FIDIS?
- Who is FIDIS?
- FIDIS Aims & Scopes
- First Results
- Summary and Outlook



Examples of Identity Concepts



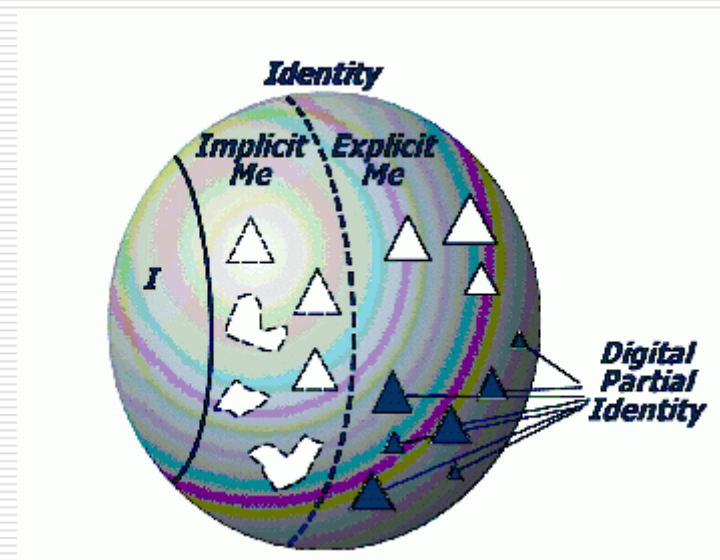
1. The I, the Implicit Me, and the Explicit Me
2. Three Tiers of Identity
3. Identities and Territories (Contexts)



The I, the Implicit Me, and the Explicit Me



- The I
 - The indeterminate first person perspective
- The implicit Me
 - The potentially representable identity
- ★ □ The explicit Me
 - The identity managed by digital infrastructures



[ICPP 2003]



Three Tiers of Identity

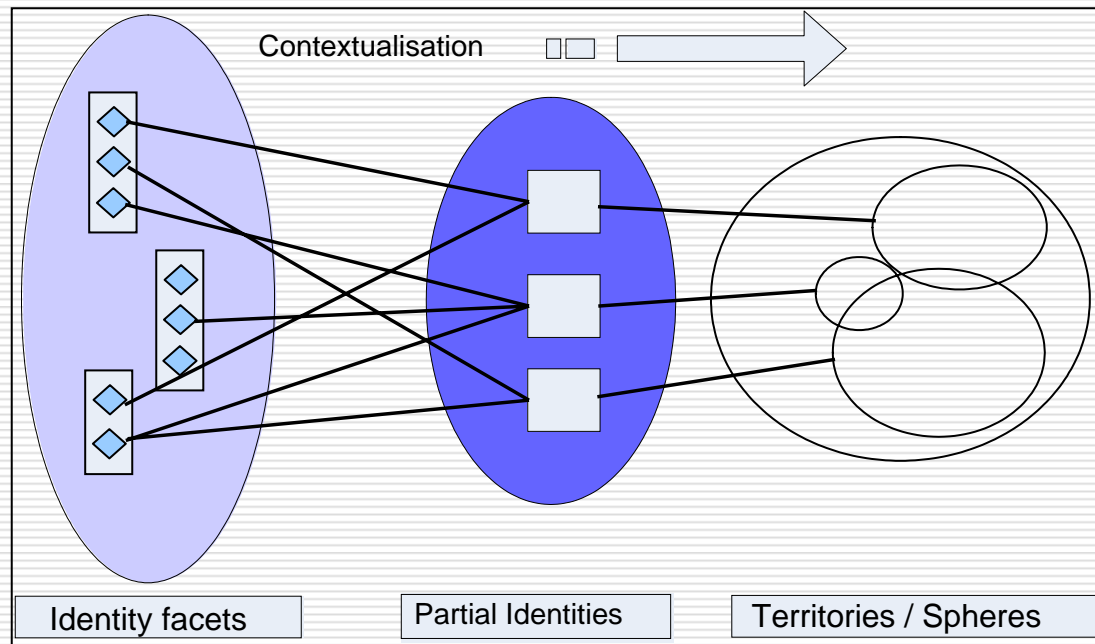
[Durand 2002]



- T1: The personal Identity
 - Inner and timeless
 - Controlled entirely by the person
- T2: The corporate (assigned) Identity
 - Related to a particular context only
- ★ □ T3: The marketing Identity
 - ★ ■ Abstracted or aggregated
 - ★ ■ Not attached to an individual (profiling)



Identities and Territories (Contexts)



□ Several partial identities (activated in context)

■ Sometimes need to isolate these partial identities



Database IMS Motivation



Problem	Solution Concept	State of the Art?
Confusing and inconvenient handling of my different "identities"	Password Management / Single Sign-on; Form Filler	+ +
Little knowledge of what others know about me	Anonymity as basis, on top: Controllability of data flow and of privacy preferences; Reputation Management	- - ±
Little control about what I permit from the outside	Reachability Management	±
Little legal liability; no protection against Identity Theft	Authenticity supported by infrastructure	-



Database IMS Examples



- E.g. Single Sign-On:
 - Microsoft Passport
 - Liberty Alliance (in spec. process, > 150 companies involved)
 - Yodlee
- Form Filler:
 - Mozilla Navigator, DigitalMe, CookieCooker
- E-Mail Client: Outlook Express
- Usage:
 - Big user numbers only when integrated such as Microsoft Passport (200 million accounts, 3.5 billion authentications per month, 91 websites supported)



Database IMS



Name	Client / Open System		Client / Server (Storage of Identity Data)		Access Management		Form Filing		Automatic Choice of Identity		Pseudonym Management		Responsible Management		Specific Functionality / Component	
	Open	C/S	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N
AccountCourier	Open	C/S	Y	N	N	(Y)	(Y)									Automated account provisioning and user ID management (mainly for organisations)
Anonymizer Privacy Manager	Open	Client	N	N	N	(Y)	(Y)									Allows user to customise an individual privacy and security level for each site
AssureAccess	Open	C/S	Y	N	N	(Y)	(Y)									Access management software for Java/JEE-based web, portals, and web services (for application developers)
ATUS	Open	Client	N	N	Y	Y	N									Choice between different partial identities
CertTrust	Open	C/S	Y	N	N	N	Y									E.g. Telesac.de, Verisign.com etc.
ClearTrust	Open	C/S	Y	N	N	N	N									Web access management
Cookie Pal	Open	Client	N	N	(Y)	N	N									Cookie manager
CookieCooker	Open	Client	(Y)	Y	(Y)	Y	N									Exchange of cookies, management of different identities, and form filing
DASIT	Open	C/S	N	N	N	Y	(Y)									Privacy control functionality for e-Commerce
Digital Handshake	Open	Client	(Y)	(Y)	N	(Y)	N									US standards-based electronic signature solution
Digital Identity	Open	Server	Y	N	N	(Y)	Y									Implements SOAP and supports relevant standards such as SAML
Digital Signature Certification	Open	C/S	(Y)	N	N	(Y)	N									Various PKI providers
DigitalMe	Open	Server	Y	Y	N	Y	N									Control of personal information presented to the public or single person (media)
Dotomi	Closed	C/S	(Y)	N	N	(Y)	(Y)									Users can specify the vendors from whom they wish to receive communication in advertising space on the web
DRIM	Open	Client	(Y)	N	(Y)	Y	(Y)									Comprehensive concept based on IDMAN, SSONET etc.
eBay	Closed	Server	N	N	N	(Y)	(Y)									Auction community in the web with own reputation system
Erreichbarkeitsmanager	Closed	Client	N	N	(Y)	Y	Y									Implementation of reachability management on Newton MessagePad
eTrust	Closed	C/S	Y	N	N	(Y)	N									Modular tool for user provisioning, single sign-on and authentication for business
Every one name	Open	Server	N	N	N	(Y)	(Y)									Provides e-mail addresses to customers for use by themselves from a pool of second level domains
eWallet	Open	Client	Y	Y	N	N	N									Form filing and password management
FINED	Open	C/S	(Y)	N	N	N	N									Identification card with digital signature
Fitmaschine.de	Closed	Server	N	N	N	(Y)	(Y)									Dating agency working with pseudonyms
Freedom	Open	Client	N	N	N	N	(Y)									Services include spam blocking, cookie management, anonymous surfing, and Internet content filtering service
Freer	Closed	Server	N	N	N	(Y)	(Y)									Mobile community management (chat) over SMS, MMS, WAP, and voice
GetAccess	Open	Server	Y	N	N	(Y)	(Y)									Provides organisations with single sign-on to web portal applications
Hushmail	Open	C/S	N	N	N	(Y)	(Y)									Web-based e-mail and document storage system with block lists, auto-responders, different e-mail domains, and digital signature verification
ID	Open	C/S	(Y)	N	N	N	N									Digital identification solutions on the Internet based on PKI and smart card technology
idemix	Open	Client	(Y)	N	(Y)	Y	N									Anonymous credential system
IDMAN	Open	Client	N	N	(Y)	Y	(Y)									Component of DRIM for management of identities and pseudonyms
Privacy	Open	C/S	N	N	N	(Y)	Y									Enables consumers to surf and purchase online anonymously, use different unique e-mail addresses and receive products without revealing names, addresses, or credit card information to the merchant
It's My Profile	Open	Server	N	N	N	(Y)	(Y)									Site allows the user to control information about own activities and preferences, e.g. to authorise email contacts from advertisers in relation to these activities
Xeon	Open	C/S	(Y)	N	N	(Y)	N									Enterprises can issue and manage their own web server SSL certificates, relying on a third party
Kariboo tickets	Open	C/S	Y	N	N	N	N									A unique key (a so-called ticket) is assigned to each person that authenticates to the network
KeyNote Trust management	Open	C/S	Y	N	N	(Y)	N									Provides a single, unified language for both local policies and credentials
LibertyAlliance	Open	C/S	Y	N	N	-	-									Developing open standards for network identity
Lotus Notes	Open	C/S	Y	N	N	N	(Y)									Management of communication and administration of information flow
ManagerID Suit	Open	Server	Y	N	N	(Y)	N									User life cycle management and automation solution for organisations
Match	Closed	Server	N	N	N	(Y)	(Y)									Dating agency working with pseudonyms
Metup	Open	Server	(Y)	N	N	(Y)	(Y)									Organises local interest groups
Micircles	Closed	Server	(Y)	N	N	N	Y									Phone / SMS equivalent of using mailing lists
Midentity	Open	Server	(Y)	N	?	?	?									Manage how to share digital information & content with other people
Mozilla 1.4	Open	Client	Y	Y	(Y)	(Y)	(Y)									Browser with e-mail client
NetIdentity	Open	C/S	N	N	N	(Y)	(Y)									Providing different e-mail addresses with different domain names to clients
NetKey	Open	Client	(Y)	N	N	Y	N									Possibility to manage different digital signatures
NetPoint	Open	C/S	Y	N	N	N	N									Unites enterprise identity management and web access control
OpenPrivacy	Open	C/S	Y	N	N	Y	N									Collection of software frameworks, protocols, and services providing a cryptographically secure and distributed platform for creating, maintaining, and selectively sharing user profile information
Orby Privacy Plus	Open	Client	N	Y	(Y)	N	N									PSP features
OTPW	Open	Client	(Y)	N	N	N	N									A one-time password login capability
Outlook Express 6 (Internet Explorer 6)	Closed	Client	Y	Y	N	(Y)	(Y)									Browser with e-mail client
P3P - APPEL	Open	C/S	N	N	(Y)	(Y)	N									Platform for Privacy Preferences (P3P) - standard for matching privacy policies (A P3P Preference Exchange Language (APPEL))
Parkinsonpas	Open	C/S	(Y)	N	N	N	N									Care and security card for Parkinson and chronic disease patients
Passport	Open	Server	Y	N	N	N	N									Single sign-on service
Persona	Open	C/S	(Y)	N	N	N	(Y)									Acts as a user-driven information broker between the consumer and a website, supports P3P and cookie management
PGP / GnuPG	Open	Client	N	N	N	Y	N									Cryptographic software for encryption, decryption, and managing different key pairs for different e-mail addresses
PingID	Open	C/S	Y	N	N	N	N									Independent and open system that interconnects with Net Passport and Liberty Alliance
Playboy Privacy Pass	Closed	Server	Y	N	N	N	N									Single sign-on solution for websites with erotic content
Policy Manager	Open	Client	N	N	N	N	Y									Allows organisations to automatically control the distribution, confidentiality, and retention of e-mail and attachments
PRIMA DataManager / Journal	Open	Client	N	N	(Y)	Y	N									Manages history of personal data that a user has permitted to service providers
Privacy Companion	Open	Client	N	N	(Y)	N	N									Allows automated cookie decisions based on the sites P3P policy
Privacy Manager	Open	Server	N	N	(Y)	N	N									Helps organisations to build privacy policies and practices into their e-business applications and infrastructure (supports P3P)
Privacy Network	Open	?	N	N	(Y)	(Y)	N									Privacy tools for B2B with support of P3P and APPEL
Private Credentials	Open	C/S	(Y)	N	N	Y	Y									Pseudonyms that contain no information that can be linked to the identity of their holder
Private Payments	Open	Server	Y	N	N	N	N									Using a random, unique number for each online payment
Roboform	Open	Client	Y	Y	N	(Y)	N									Password manager, form filler, password generator
SafeZone	Open	Server	N	N	N	(Y)	Y									Customers buy and receive products without revealing their names, addresses, or credit card information to the merchant
SAML	Open	C/S	(Y)	N	N	(Y)	N									Standard which defines user authentication, entitlements and attribute information in XML documents
Secretmaker	Open	Client	N	N	N	(Y)	N									Anonymous that exchanges specific information of the computer with "phantoms" before it is released to the Internet
SelectAccess	Open	C/S	Y	N	N	N	(Y)									Web access control and authorisation management product for organisations
StarMinder	Open	Server	Y	N	N	(Y)	(Y)									Authentication and authorization management and providing single sign-on for organisations
Shibboleth	Open	Client	Y	(Y)	(Y)	Y	N									Supports inter-institutional sharing and controlled access to web available services with privacy info monitor for the user
Spamex	Open	Client	N	N	N	Y	(Y)									Hides the user's e-mail address and uses disposable e-mail addresses
SpeedNames	Open	Server	N	N	N	Y	(Y)									Represents providers for domain name registration for building an Internet identity (cf. (Dyson 2002a))
Sun One / Network Identity	Open	Server	Y	N	N	(Y)	N									Account management and organization identity management
The Sims Online	Closed	Server	N	N	N	Y	Y									Game / Virtual Residence simulation with chat function
There	Closed	Server	N	N	N	Y	Y									Game / Virtual Residence simulation with chat function
TrueSign	Open	C/S	(Y)	N	N	N	Y									Secure verification of digitally signed electronic documents
TrustBridge	Open	C/S	Y	N	N	(Y)	N									Enable organisations to share user identities across business boundaries
Trusted Transaction Roaming Project	Open	C/S	(Y)	N	N	N	N									Aims to leverage the existing mobile telephony infrastructure to provide evidence of identity and payment capabilities

Application	Auth/Functionality	Type of ID	Identities	Issue of Use	Management	Universal routing	Security	Privacy	Open Profiles	Interoperability	Cost for User	Business Model	
Microsoft Passport	SSO	centralised	4	4	2	1.5	1.5	0	1	0	0	0	Paid by partner sites
Liberty Alliance	SSO	federated	4	2+X	X	1.5+X	1.5+X	0	2+X	0	0	0	Paid by partner sites
Yodlee	SSO	centralised	4	3.5	1	3.5	2	0	0	0	0	0	Presentation / Promotion
Mozilla Navigator	Form Filler	federated (client)	4	3.5	4	2	3	0	0	0	0	0	Open Source
Digitalme	Form Filler	centralised	4	3.5	2	2.5	3	1	1	0	0	0	Presentation / Promotion
CookieCooker	Form Filler	federated (client)	4.5	2	3	2	3.5	1	1	0	15	0	Paid by user
Outlook Express	Mail Identities	federated (client)	3.5	4.5	1	1.5	3	1	2	0	0	0	Part of MS Windows



First Results of IMS Comparison



Today's IMS: Playground for users & service providers

- Main goal: **usefulness**
- **Deficiencies** concerning **privacy and security** functionality, and if realised: usability problems
- **Digital evidence** is **not** addressed (lack of liability / no non-repudiation), no support for law enforcement
- **Identity theft** is not prevented
- Little functionality, **limited** purposes
- No general solutions, **no standards**
- Trustworthy computer systems and infrastructure are still missing ⇒ **no trustworthy and secure** IMS possible
- **Business models:**
Service and software mostly free for users



Agenda



- Why FIDIS?
- Who is FIDIS?
- FIDIS Aims & Scopes
- First Results
- Summary and Outlook



Summary and Outlook



- Europe (& the world) are in the middle of a silent “identity revolution”.
- Identity has many facets
- FIDIS convenes leading institutions in this area
- More on www.fidis.net

