



International Telecommunication Union

Enabling productivity, interoperability, and new end user experiences by integrating people, identity, profile, and relationship data

Anthony Nadalin
Chief Security Architect, IBM

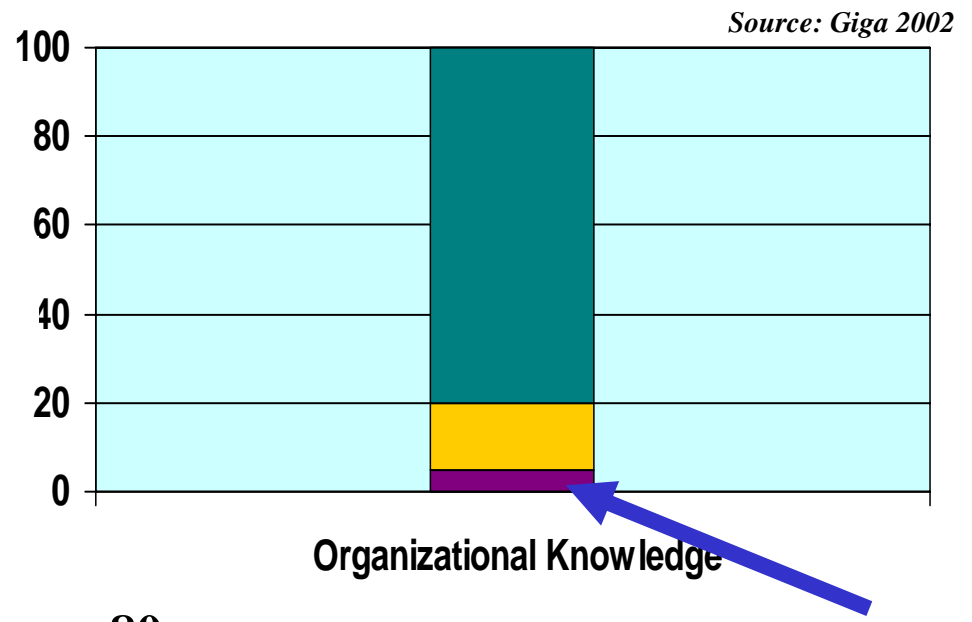
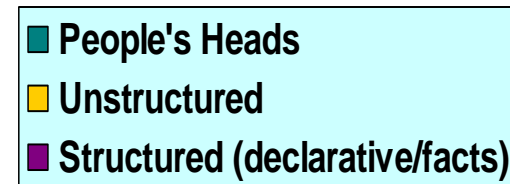


ITU-T

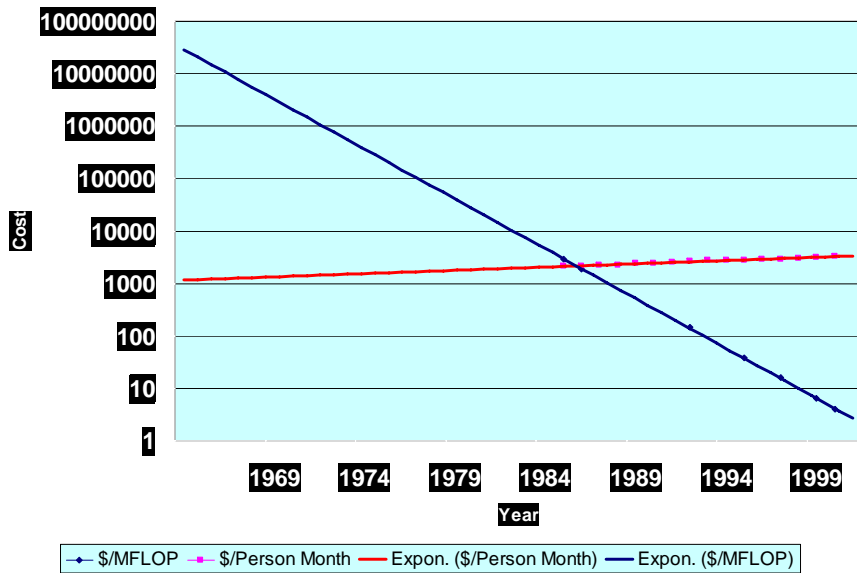
Why Focus on Optimizing Around People???

The relative cost of humans to technology resources has made humans the most expensive component of the system. Our focus remains on optimizing the efficiency of the system.

80% of Knowledge Not in Any System



80% of Formal IT budget spent on managing 4% of data, information and knowledge





The Evolution of Integration of Information About People

Concurrent

Sequential

Profile Information

Personal Account Information (continued)

Serial number: 837520
 Country code: 897
 Division: 22
 Department: G2QA
 Regular driver?: No

If any of the information on this screen is incorrect, please contact your manager and have your manager update your CERIS information.

Options... Back Next Finished Cancel

Email address: jvergo@us.ibm.com

If any of the information on this screen is incorrect, please contact your manager and have your manager update your CERIS information.

Options... Back Next Finished Cancel

IBM Intranet - Microsoft Internet Explorer

Address: http://w3.ibm.com/

YOU AND IBM

2004 Benefits: Enroll Now
 You can enroll or make changes to your IBM health benefits for 2004 between now and November 20, 2003 on NetBenefits.

Your Money: Money Matters. Learn all you can about how to make it grow, and protect it at IBM. Find out about base pay, variable pay, stock ownership, 401K and other offerings.

Your Health: Health benefit changes for 2004 include one medical and one dental option at no cost for employee-only coverage, healthy Living Features, Health Care Spending Account improvements and more.

Your Life: Adopting a child? Buying a house? Paying for college? Contributing to charity? IBM helps you do all that and more.

Your Career: Our philosophy is simple. Varied experiences, increased knowledge, learning and development and a challenging, stimulating environment all create opportunity at IBM.

65% of IBM employees agree that we are making changes necessary to compete effectively.

Planning your financial future? Get a forecast from Financial Engines.

Go to You and IBM US

Visually Coordinated

```

EUM1      Equal Opportunity meeting date      None: +
EM20-0833-14      Date: 11/04/03
Type the information. Then press the Forward (F8) key
Originating manager . . . : 837520   Vergo, John
Employee's serial . . . . : 837520 +
EO meeting date . . . . . : 11/04/03   (mm/dd/yy)
Note: To select more than one employee, use the Prompt (F4) key.

F1=Help  F3=Exit  F4=Prompt  F7=Backward  F8=Forward  F12=Cancel
020H200010E Employee is not within two levels of your department.
  
```

1970's

1985

2000

Trends: People and Information About Them

- Productivity is achieved through the integration of people with business processes
- Information about people in the enterprise is abundant and growing in richness and volume
- Information is scattered and not integrated
- A federated, digital representation will emerge
- Maintaining privacy of appropriate user information is key

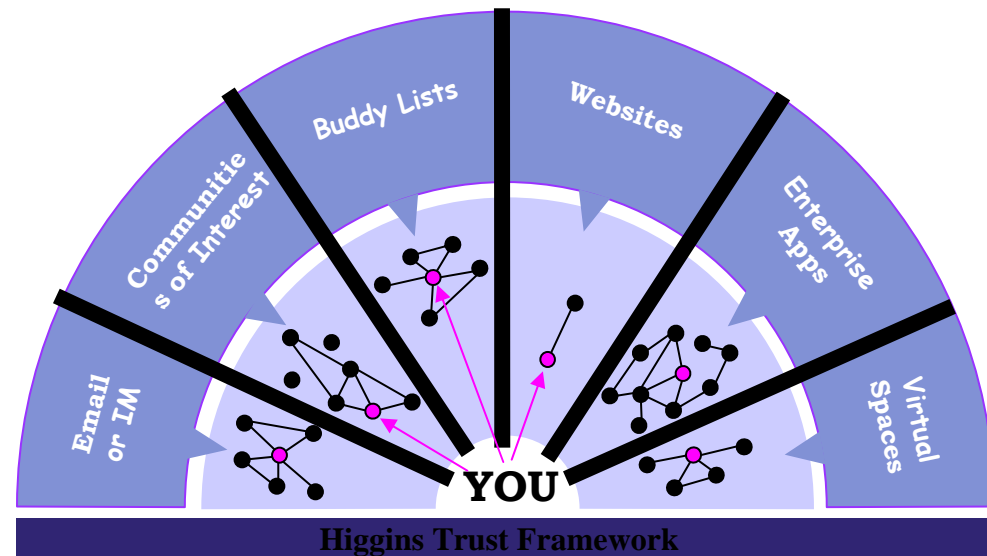


ITU-T

New Framework Enhances Identity Management

An Eclipse open source project supported by IBM, Novell, Parity, and others that will:

- Provide a foundation for "user-centric identity" and personal information management applications
- Enable dynamic, automatic capture of people information from disparate information repositories
- Facilitate integration with diverse identity management systems
- Ease management of identity, profile, reputation and relationship data across repositories



For Developers: Identity Tooling

- o Identity management framework
- o Saves developer from learning the details of multiple identity systems
- o Only one API to learn
- o Relies on plug-ins to support major protocols and technologies: CardSpace™, OpenID, RSS-H, XRI, LDAP, etc.

User-centric authentication

- Provides a consistent user experience
- User picks from a selection of visual “i-cards”
- Privacy-enabled claims to share only what is needed (and protect private information)

Personal information integration

- Remembers passwords, fills in forms
- Links and syncs your info across silos
- Gives more control over your personal data

For End Users: An Identity Metasystem

- Higgins provides an Identity Attribute Service to aggregate and federate information across systems and silos
- Its abstract data model can accommodate multiple heterogeneous identity systems
- Context Providers reflect identities and attributives relevant to those contexts



ITU-T

For End Users: Enabling Privacy

Manage private information

- Need to access consistent view of their data, metadata

Share and control access to private information

- Attach (privacy, access) policies at record (e.g. medical records) or attribute (e.g., salary) level

Present information on an “as needed” basis

- Transform attributes (e.g., bank balance = \$100k), to claims (e.g., bank balance > \$20K) as required
- Relying party only trusts the originating entity (e.g., bank) and does not need to trust the transforming intermediary

- Integrate identity, profile, reputation, and relationship information across and among complex enterprises
- Create common interfaces to identity and networking systems
- Support advanced process automation by providing “data context”

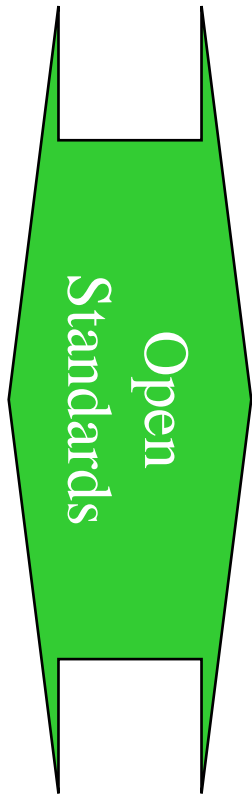
For the Enterprise: Enabling Privacy

- Enterprise privacy policies
 - Necessary but not sufficient to enforce corporate policies through enterprise systems
- Meet scaling requirements
 - Empower users to control more of their private information
 - Empowering does not imply users can override all policies
- Consumer and employee satisfaction
- Ultimately privacy is about the user
- So let's give the user some control !

- o User-centric identity
 - Fundamental goal (improve user control) and approach (framework + metaphor)
 - EU PRIME, Microsoft CardSpace, Eclipse Higgins, ...

- o Current discussion is too limited, and bears risk of over-simplification
 1. Identity disclosures happen in many types of transactions
 - Discussion focuses on *user-controlled* disclosures
 - But most privacy-relevant transactions happen *without* any user involvement
 - Extending user control to such transactions requires specific technology and trust
 - Reputation and accountability are very much intertwined with privacy
 2. An identity metasytem / framework is an important concept, but it only *manages* other systems
 - Privacy depends largely on *these* systems, not primarily on the metasytem
 3. Agreement on “laws” does not automatically lead to open standards.
 - Standards needed: interoperability of metasystems + minimum req. for actual systems
 - Needs an open process, leading to open, stable and freely usable standards
 - Candidate projects exists, e.g., Project Higgins

What is needed?



Context-adequate metaphors for identity and standard policies

Framework for the integration of identity, profile and relationship data

Cryptographic implementations supporting privacy, authenticity and accountability