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

Anthony Nadalin
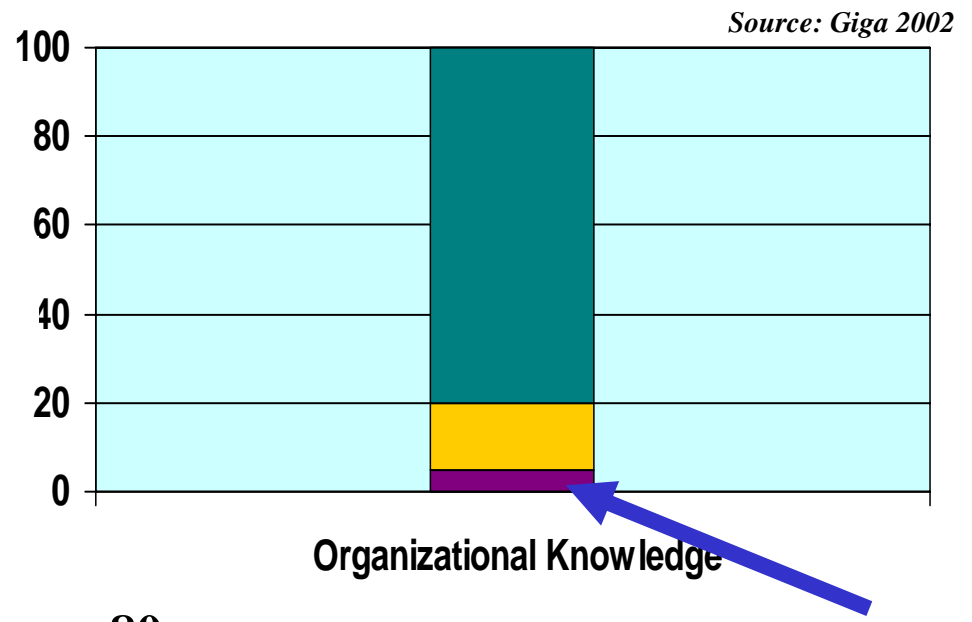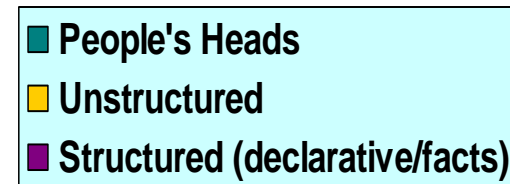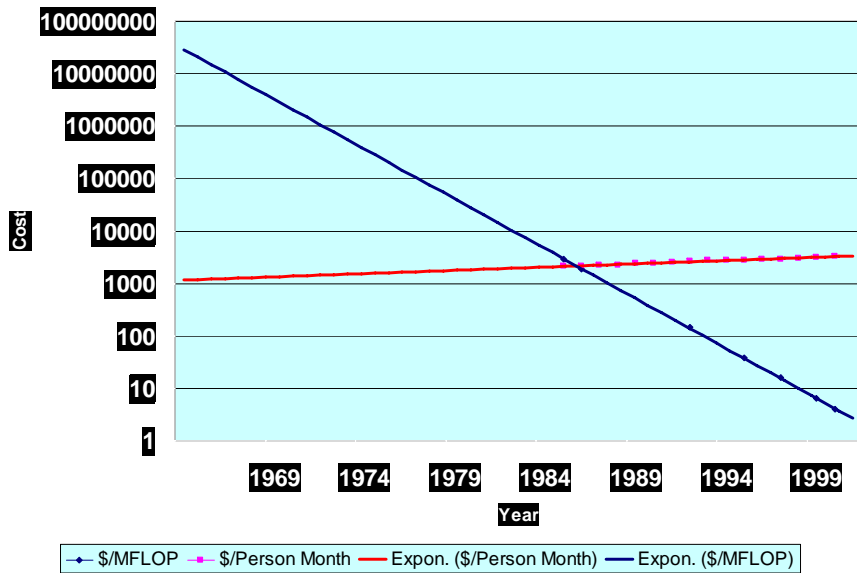
Chief Security Architect, IBM

Why Focus on Optimizing Around People???

ITU-T

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

- ■ People's Heads
- ■ Unstructured
- ■ Structured (declarative/facts)

Source: Giga 2002

Organizational Knowledge

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

Concurrent

Sequential

Visually Coordinated

1970's   1985   2000

o **Productivity is achieved through the integration of people with business processes**

o **Information about people in the enterprise is abundant and growing in richness and volume**

o **Information is scattered and not integrated**

o **A federated, digital representation will emerge**

o **Maintaining privacy of appropriate user information is key**

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
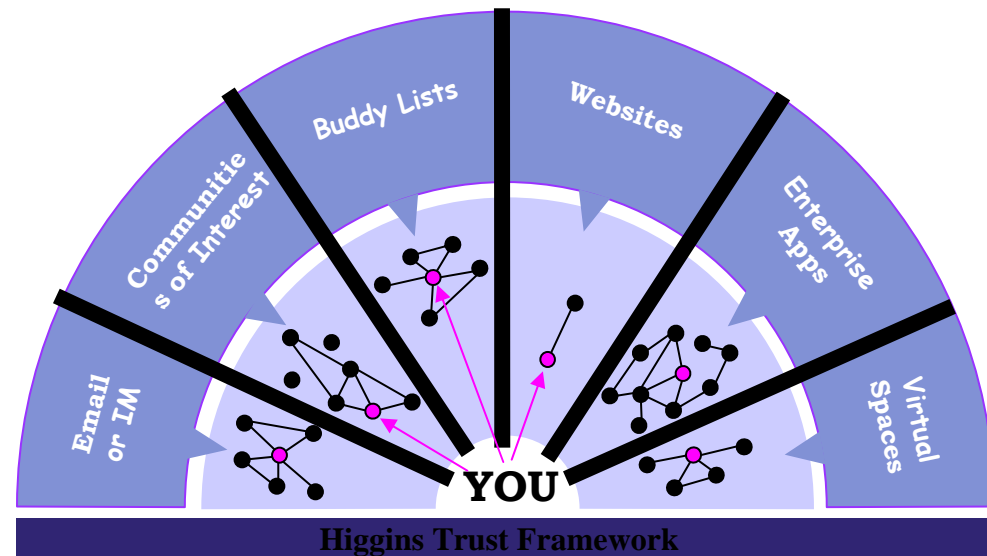
o Identity management framework

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

o Provides a consistent user experience

o User picks from a selection of visual "i-cards"

o Privacy-enabled claims to share only what is needed (and protect private information)

Personal information integration

o Remembers passwords, fills in forms

o Links and syncs your info across silos

o Gives more control over your personal data

For End Users: An Identity Metasystem

o Higgins provides an Identity Attribute Service to aggregate and federate information across systems and silos

o Its abstract data model can accommodate multiple heterogeneous identity systems

o Context Providers reflect identities and attributives relevant to those contexts

Manage private information

o   Need to access consistent view of their data, metadata

Share and control access to private information

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

Present information on an "as needed" basis

o   Transform attributes (e.g., bank balance = $100k), to claims (e.g., bank balance > $20K) as required

o   Relying party only trusts the originating entity (e.g., bank) and does not need to trust the transforming intermediary

o Integrate identity, profile, reputation, and relationship information across and among complex enterprises

o Create common interfaces to identity and networking systems

o Support advanced process automation by providing "data context"

o **Enterprise privacy policies**

- • Necessary but not sufficient to enforce corporate policies through enterprise systems

o **Meet scaling requirements**

- • Empower users to control more of their private information

- • Empowering does not imply users can override all policies

o Consumer and employee satisfaction

o Ultimately privacy is about the user

o So let's give the user some control !

Summary

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 metasystem / framework is an important concept, but it only *manages* other systems
     — Privacy depends largely on *these* systems, not primarily on the metasystem
  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?

ITU-T

Open Standards
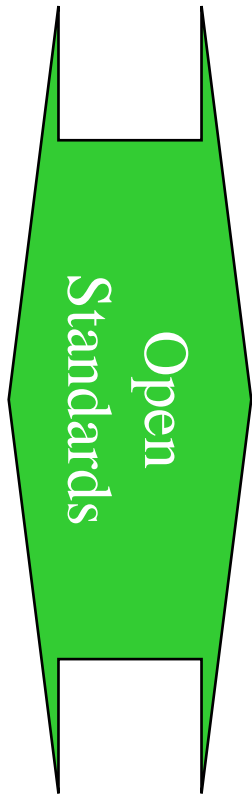
Context-adequate metaphors for identity and standard policies

Framework for the integration of identity, profile and relationship data

Cryptographic implementations supporting privacy, authenticity and accountability