

**Identity Management?  
or  
(Id)Entity Mismanagement?**

**Roger Clarke FACS  
Xamax Consultancy, Canberra**

**Visiting Professor/Fellow, Unis. of Hong Kong, U.N.S.W., ANU**

<http://www.xamax.com.au/EC/IdMngt> {.html,.ppt}

**A.C.S. Conference on 'I.T. in Government'  
Canberra - 5 November 2004**

# (Id)Entity (Mis)Management

## The Agenda

- Authentication – of what?
- Identity, Identifiers, Entities, ..., Nyms
- Entifiers for People – Biometrics
- ‘Identity Management’
  - Phases in User Access Security
  - Many Architectures
  - Competition Between and Within
  - Issues

## **Identification**

The process whereby data is associated with a particular Identity

## **Authentication**

The Process of Testing **an Assertion** in order to establish a level of confidence in the Assertion's reliability

## **Identity Authentication**

The Process of Testing **an Identity Assertion**

# Kinds of Assertions Relevant to eBusiness

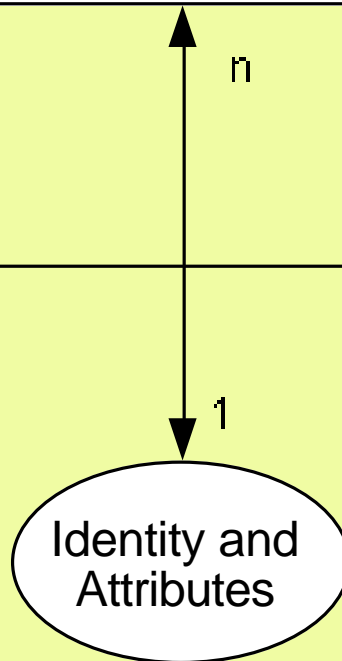
- About Data
- About Value
- About Location
- About Documents
- About Attributes
- About Principal-Agent Relationships
- About Entities
- About Identities

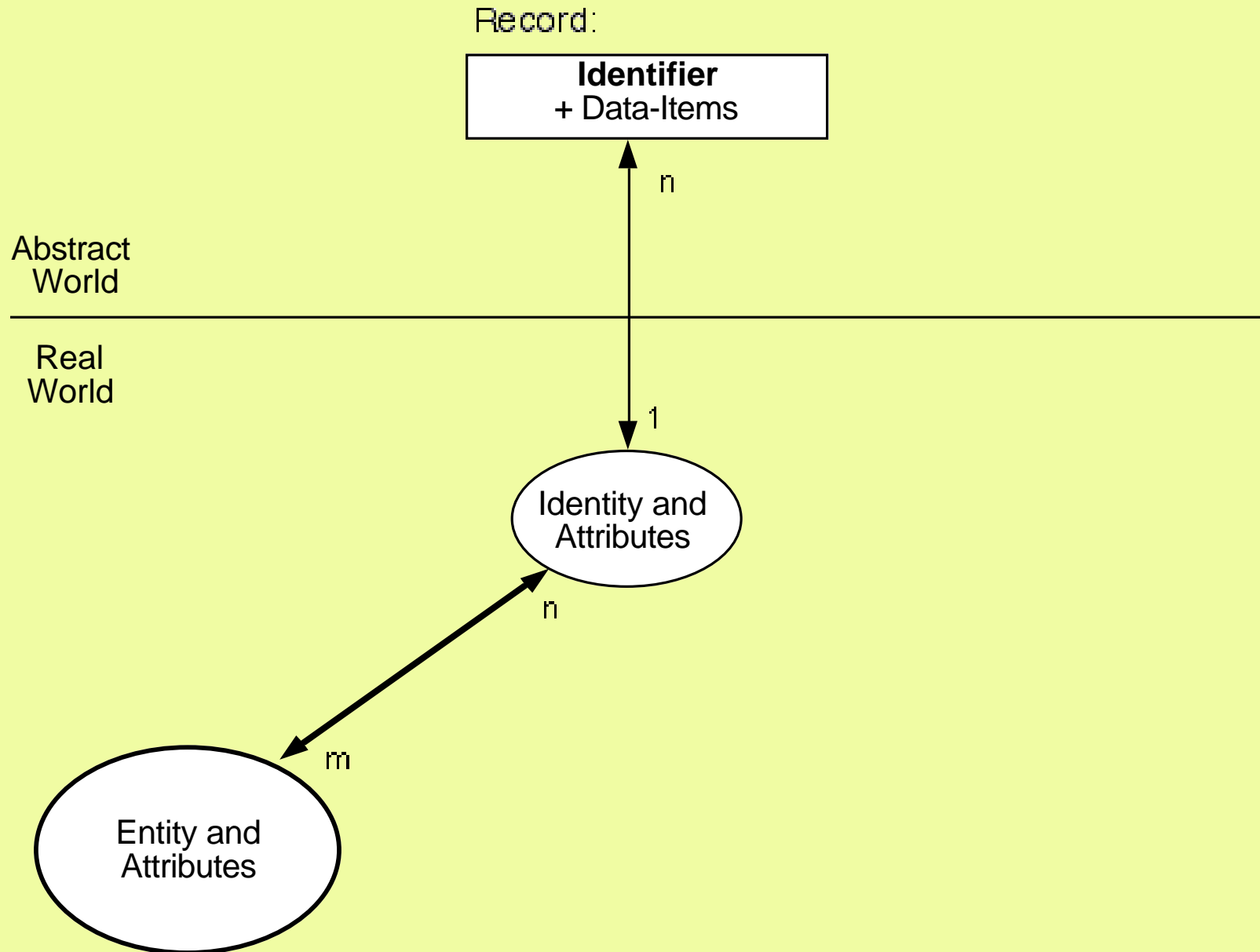
Record:

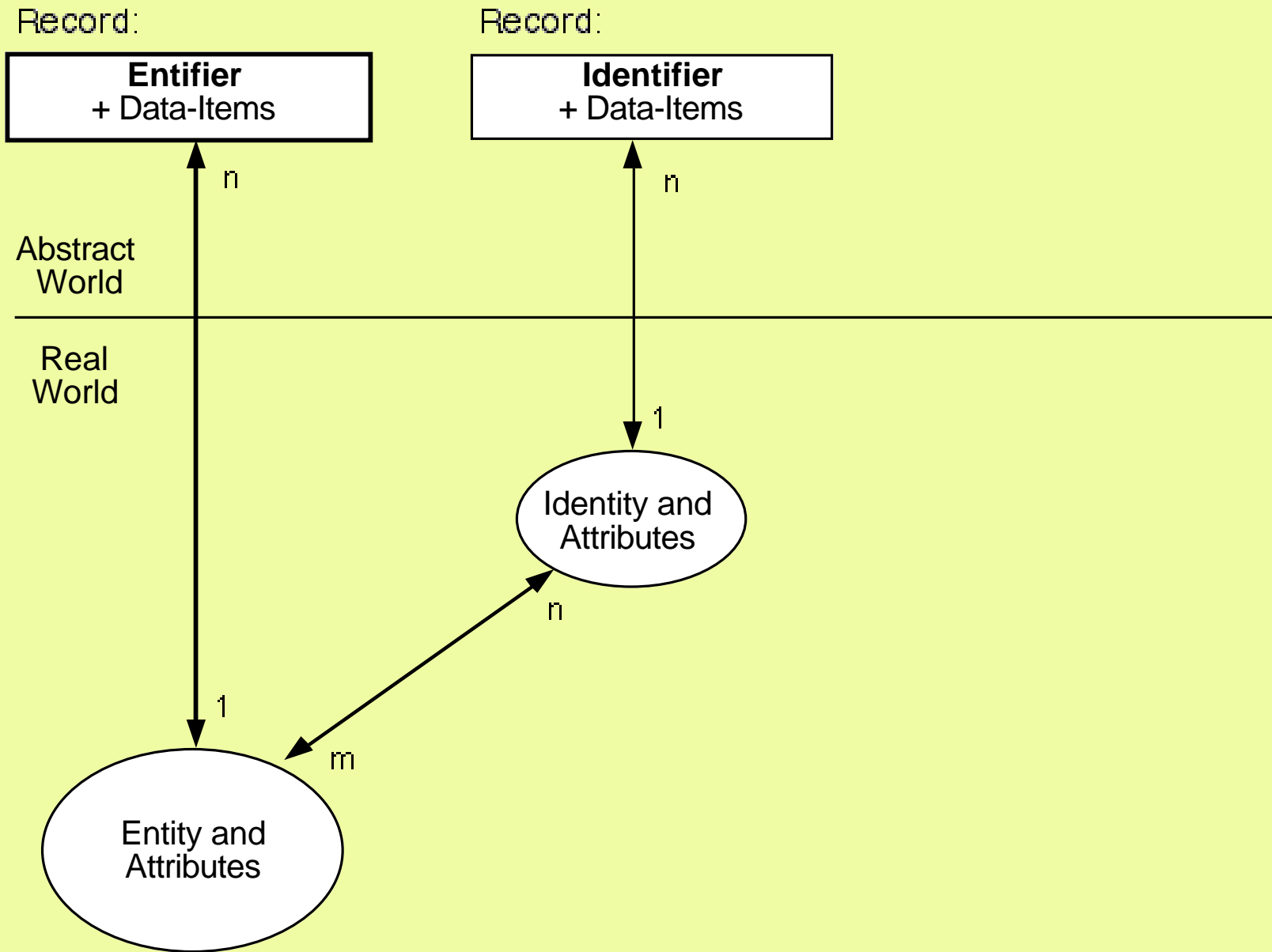


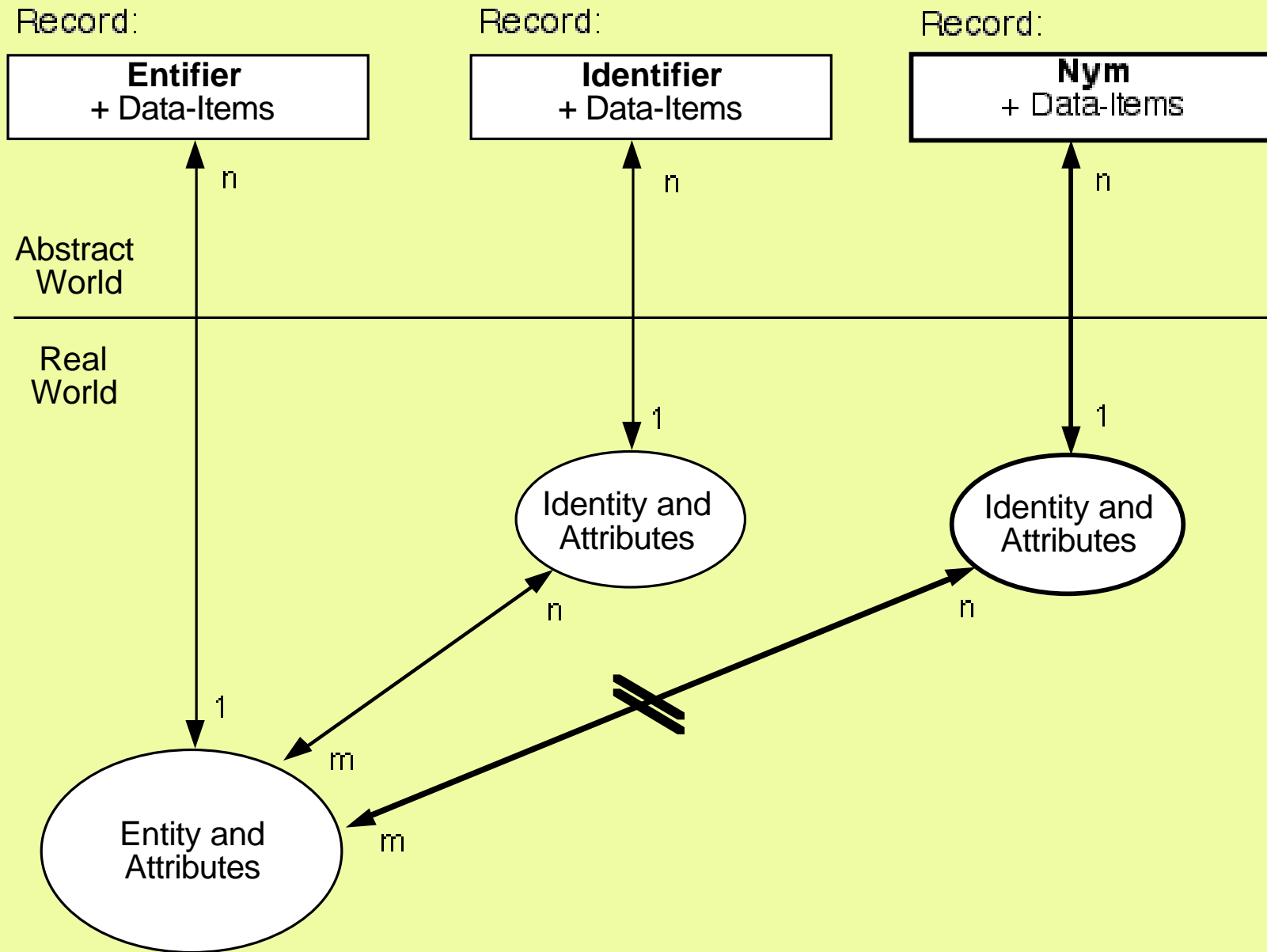
Abstract  
World

Real  
World









# **A Comprehensive Model with a Common Language**

**Australian Government Authentication Framework**

**AGAF II**

**under the Auspices of IMSC / CIOC / AWG  
project conducted by NOIE/AGIMO/?  
with the assistance of Convergence**

**With an Accompanying Glossary**

# Entity Identification and Authentication

- **Artefacts**
  - NIC Ids for Ethernet Cards
- **Legal Persons**
  - For corporations, associations, ...
  - But they're incorporeal !
- **Natural Persons**
  - Biometrics
    - 'what the person is'
    - 'what the person does'

# Identity Management

## A Working Definition

A set of processes and supporting infrastructure  
that enable  
**the authentication of identity assertions**

The term is often used in a more restrictive sense,  
to apply to the specific context of  
**online access over open public networks**

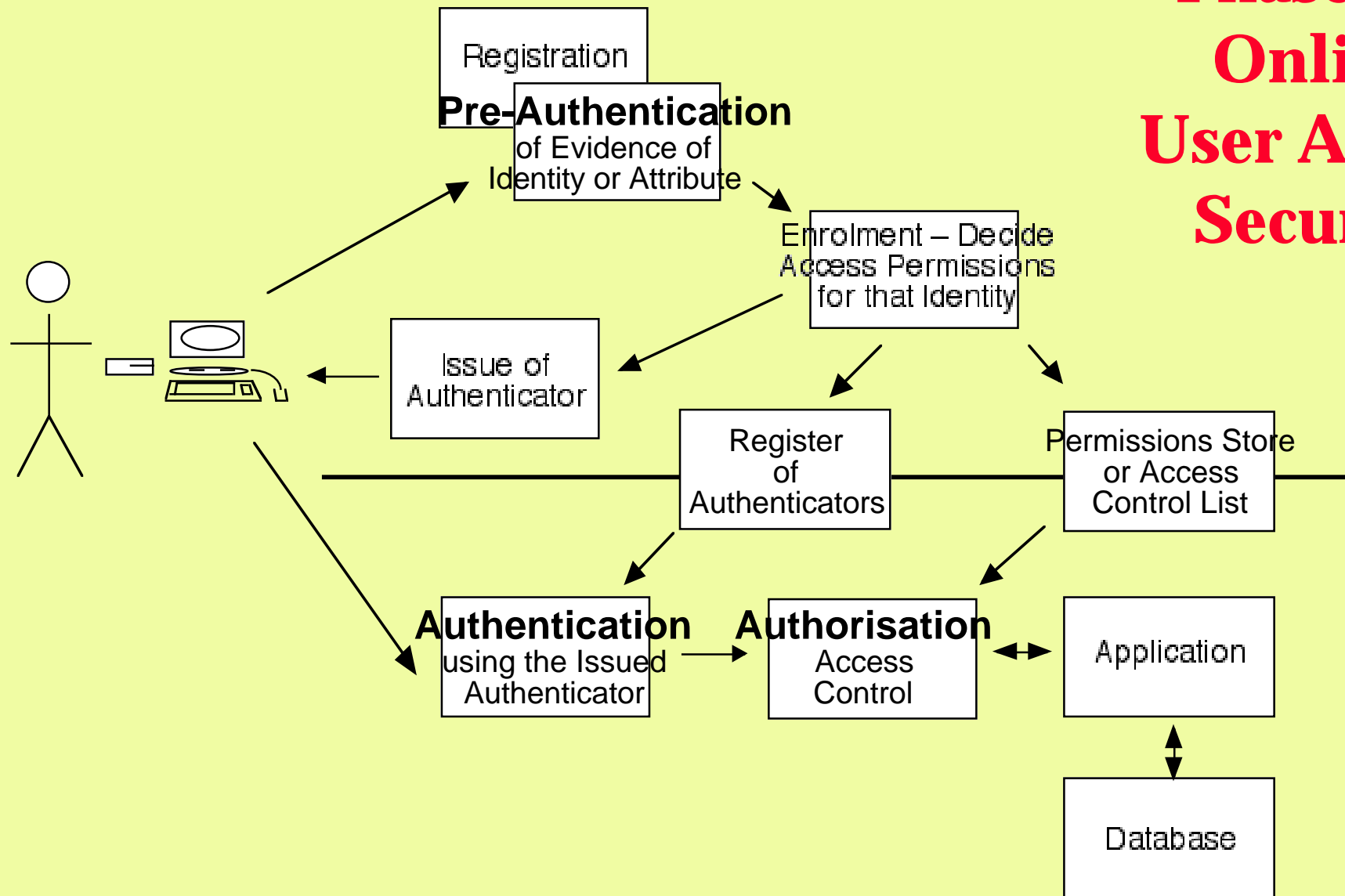
# Human Identity Authentication

Cross-Check of an Identifier / Nym against some kind of Authenticator(s), in particular:

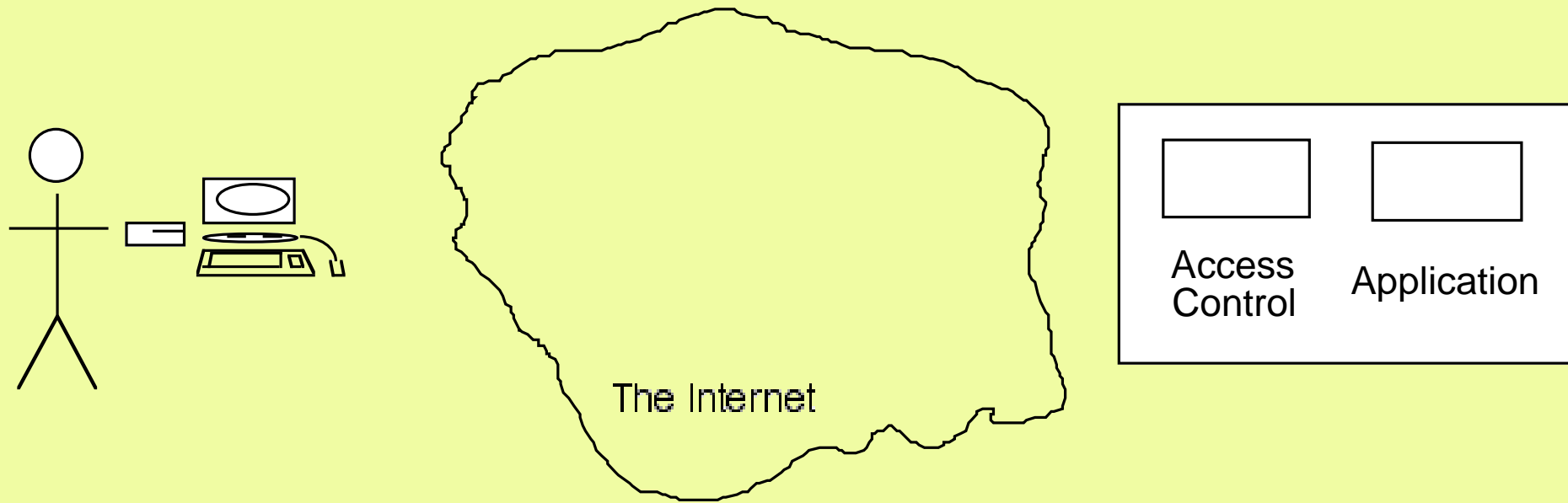
- **What the Person Knows**  
e.g. mother's maiden name, Password, PIN
- **What the Person Has ('Credentials')**  
e.g. a Token, such as an 'ID-Card', a Ticket  
e.g. a Digital Token such as  
a Digital Signature consistent with the  
Public Key attested to by a Digital Certificate

==>> 'Two-Factor Authentication'

# Phases in Online User Access Security



# User Access Security for a Single Application aka Silo'd Identity Management – Type I



# User Access Security for a Single Application

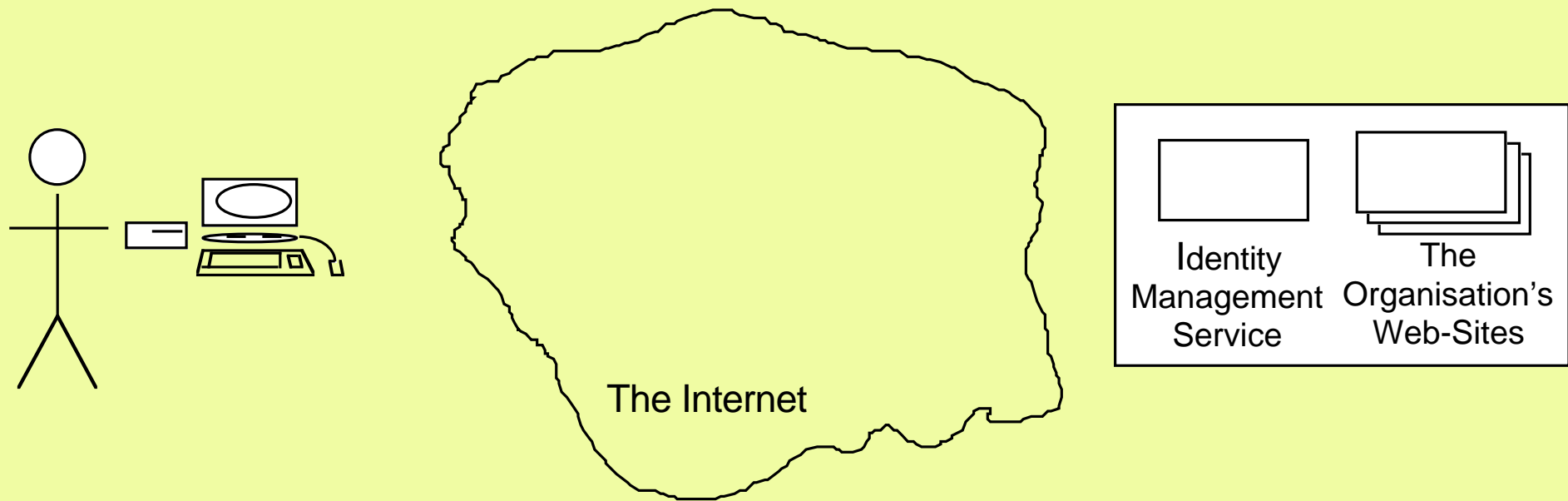
## The Conventional Process

1. User performs authentication via their browser  
e.g. keys username/password into a webform
2. Browser transmits data to a server  
(over an encrypted channel, e.g. SSL/TLS)
3. The server performs authentication, e.g.  
checking the password is correct for that username

# Extending The Conventional Process to Support Multiple Applications

1. User performs authentication via their browser  
e.g. keys username/password into a webform
2. Browser transmits data to a server  
(over an encrypted channel, e.g. SSL/TLS)
3. The server performs authentication  
e.g. checking the password is correct for that username
4. **The server creates a secure digital token**
5. **When the user clicks on a link to another site  
that token is made available to the second site**
6. **That site may accept the token as sufficient evidence that  
the request came from the user identified in the token**

# Single-Organisation Single-SignOn aka Silo'd Identity Management – Type II



# The Outsourcing Proposition

We can offer you a great deal!

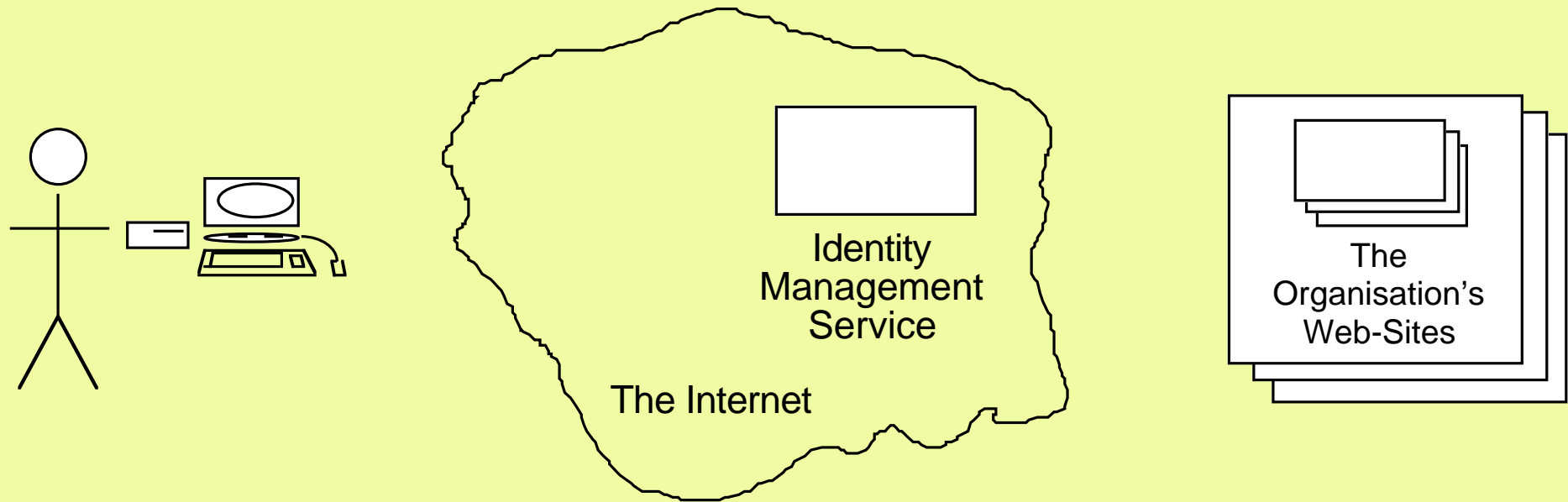
We already run a service like this!

You can use ours!

And it'll cost you less, for a better service!

'We' are Microsoft .Net Passport, or similar,  
or a specialist third-party service provider

# Multi-Organisation Single-SignOn Identity Management



## **But There's a Competitive Market**

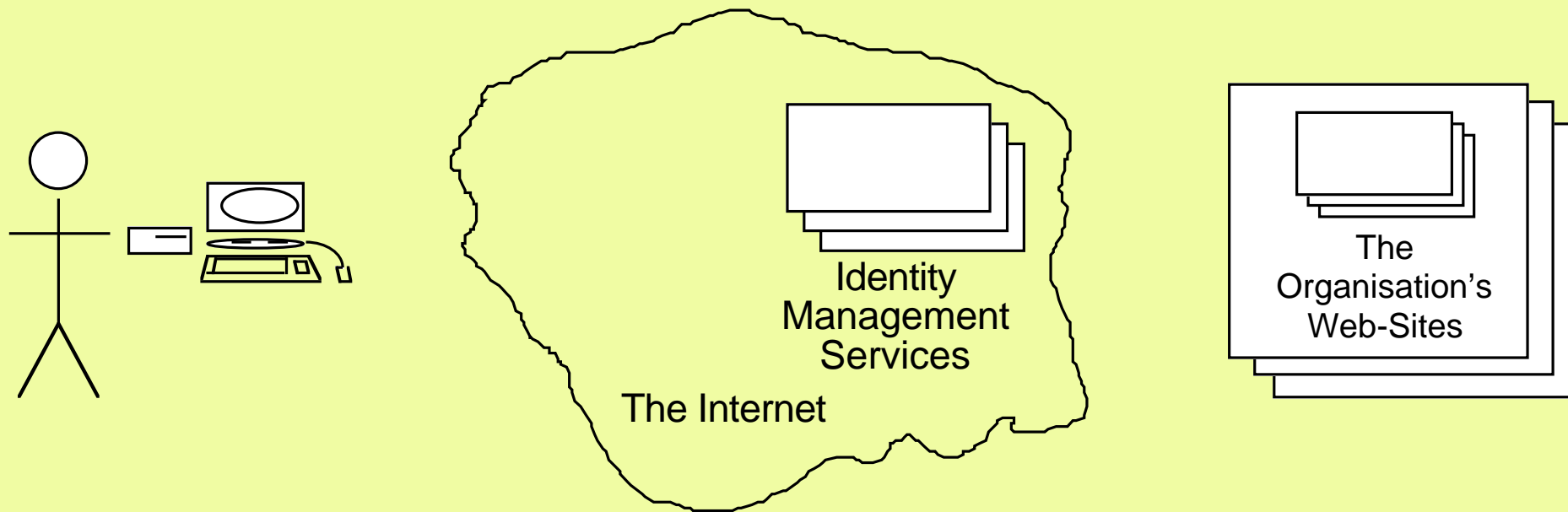
Services are run by multiple organisations

A relying site may accept a user that has been authenticated by any of a range of participating id mngt service providers

So we have to cope with multiple sources

(e.g. eBay runs its own, and accepts Passport)

# Federated Identity Management



# The Protocol Hierarchy for Federated Identity Management

- **High-Level Identity Management Protocols**  
(Liberty Alliance and WS-Federation, in XML), using:
  - Standardised Message Formats between remote devices (e.g. SAML/XML, WS-Federation)
  - an Identity Exchange Protocol (e.g. XNS)
  - a Data Release Protocol (e.g. APPEL, EPAL)
- **Process Invocation on Remote Devices**  
(e.g. Simple Object Access Protocol (SOAP)/XML)
- **World Wide Web Message Transfer** (HTTP, DNS)
- **Internet Transmission Protocols** (TCP/IP, UDP/IP)

## Service Providers

- Ascio Digital Identity
- AOL Screen Name / Quick Checkout / Wallet / Magic Carpet
- Digital ID World
- IBM Tivoli Identity Manager
- IBM Research Labs idemix ?
- Microsoft Passport
- Novell digitalme, eDirectory
- Passlogix Single Sign-On
- RSA Security
- Yodlee ?

# Industry Associations and Standards Initiatives

## Existing Associations

- Identrus
- Internet2 Shibboleth
- OASIS SAML
- The Open Group

## New Associations

- Liberty Alliance
- OpenSAML
- PingId
- SourceID
- XNS
- The Web Services Federation

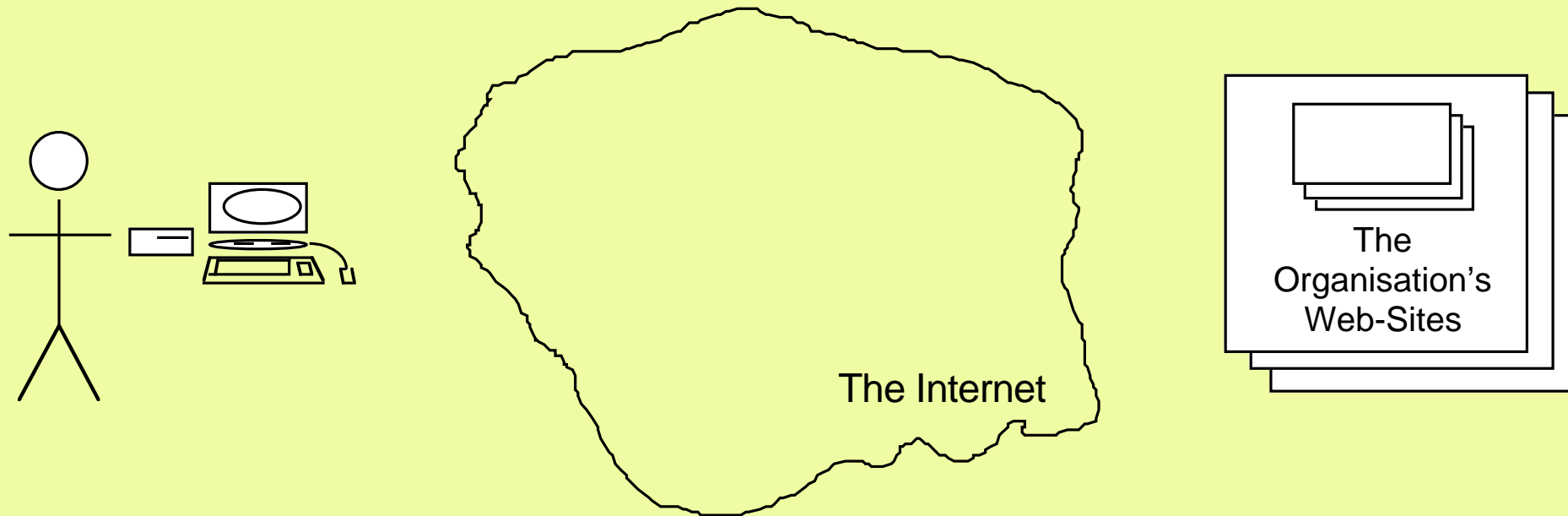
## Other Service-Providers

- GhostSurf
- IBM Research Labs idemix ?
- Privacy Inc's MPP
- Yodlee ?

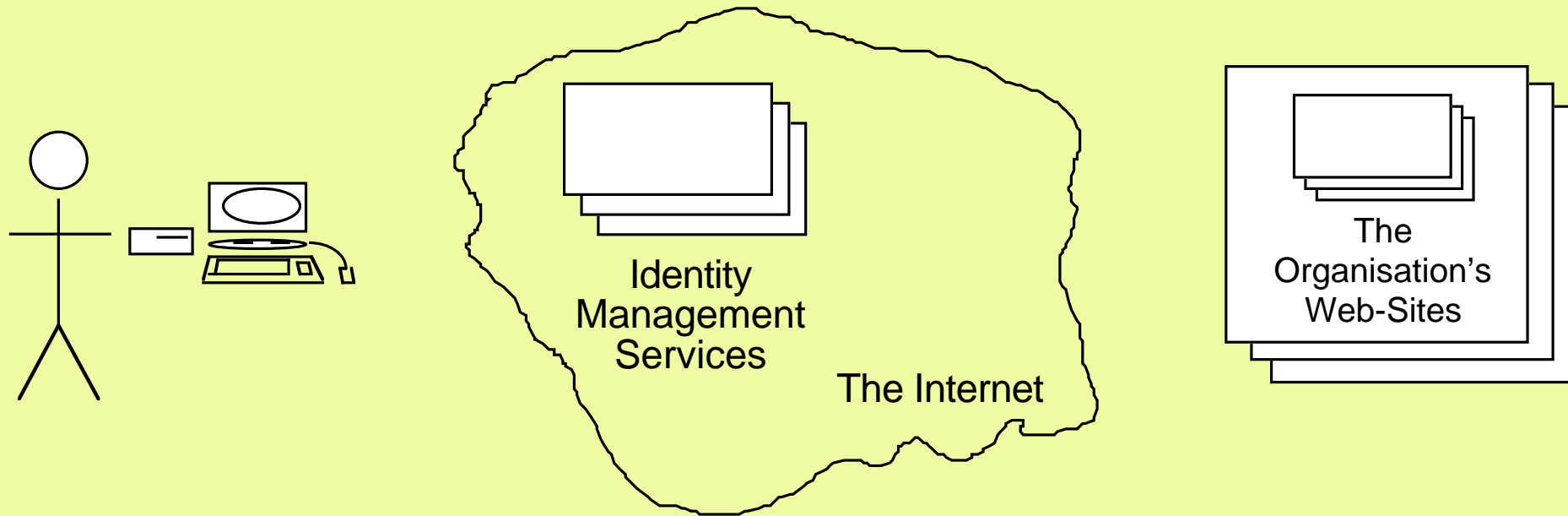
## Projects

- ATUS (A Toolkit for Usable Security)
- DRIM (DResden Identity Management)
- Icepick
- Sunshine

# Own-Device Identity Management

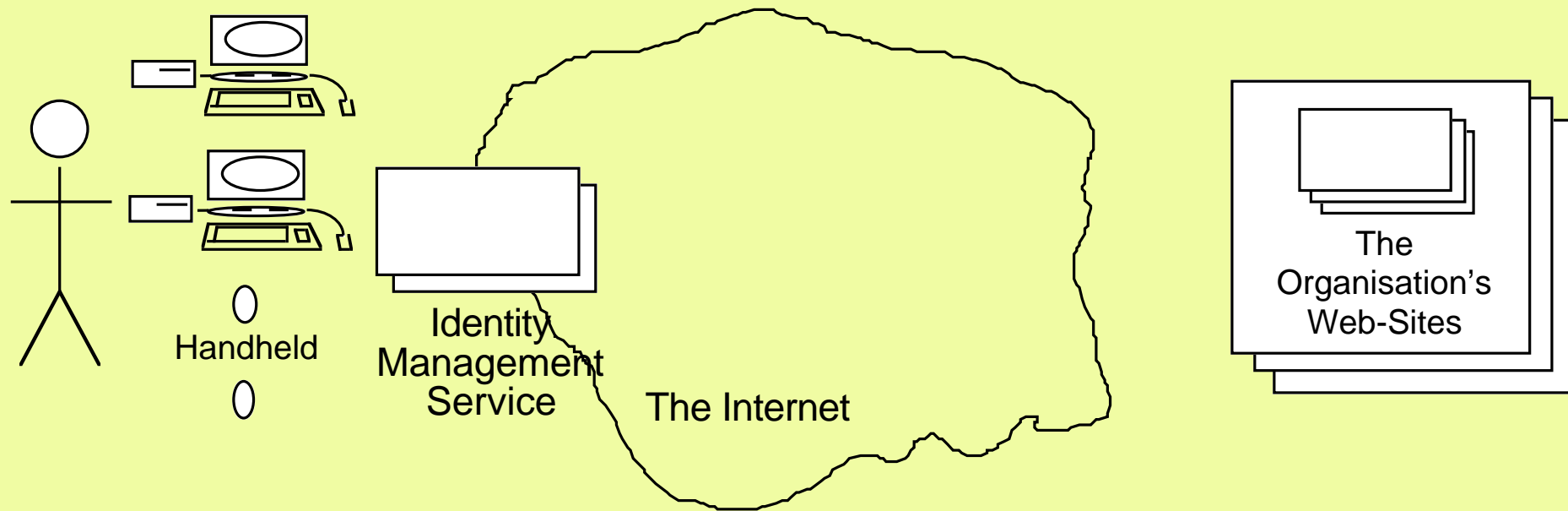


# Identity Management by a User-Selected Intermediary

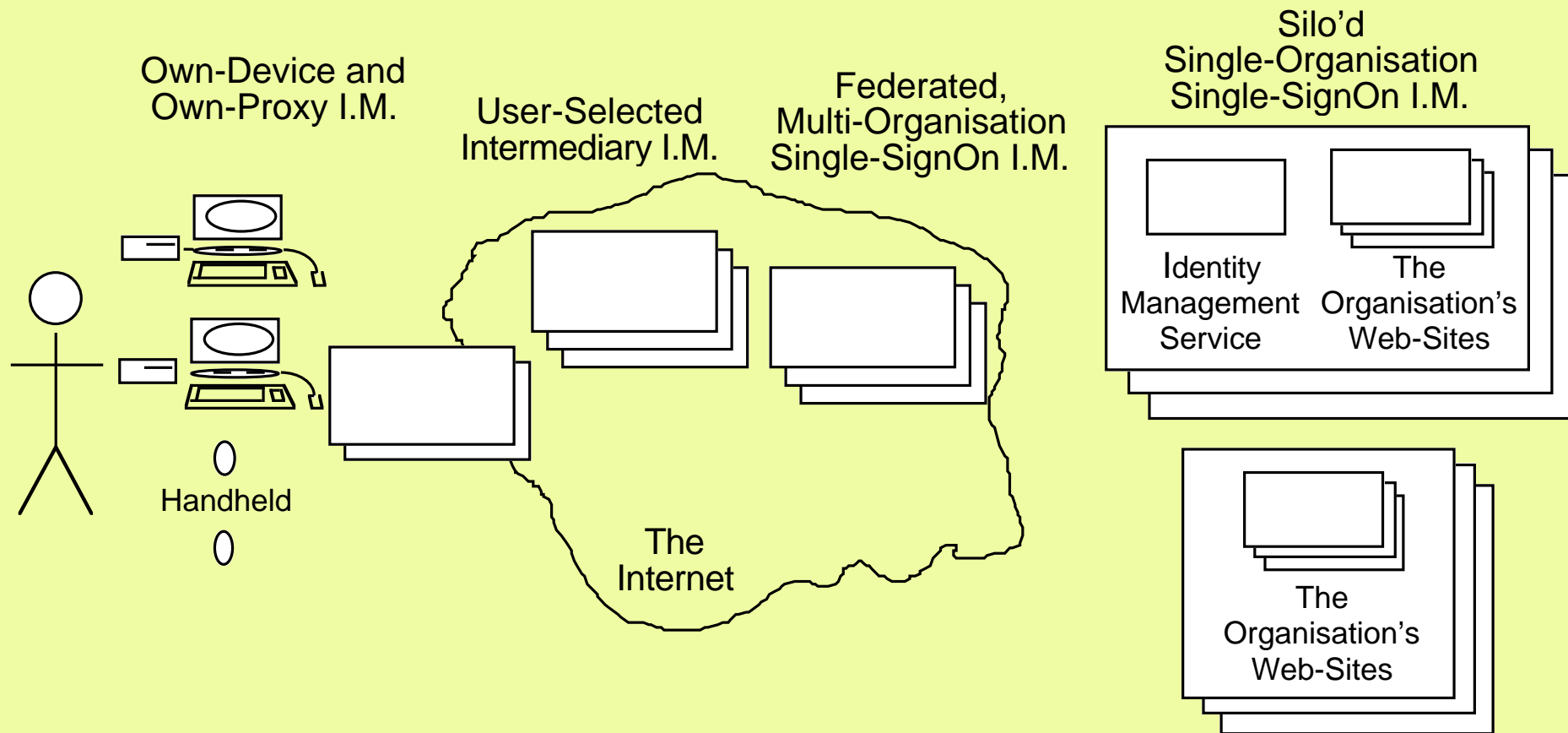


cf. Hagel's 'info-mediaries'

# Own-Proxy Identity Management



# The Multi-Mediated Super-Architecture



# Countermeasures by Individuals

- Web-Forms can be filled with:
  - pre-recorded data
  - pseudo-random data
  - convenient data
  - 'false' data
- Personal data can be automatically varied for each remote service, in order to detect data leakage, e.g. spelling-variants, numerical anagrams
- Personal data can be automatically varied for the same remote service on successive occasions (to pollute the data-store and confuse the userprofile)
- Users can exchange cookies, resulting in compound profiles rather than profiles that actually reflect an individual user's behaviour

# Weaknesses in the Mainstream Identity Management Offerings

- **Conceptual Weaknesses**
  - Limited Understanding of 'Authentication'
  - No Distinction Between Identity and Entity
  - Lack of Clarity of the Meaning of 'Account'
  - Confusion about the Forms of Nymity
- **Incompleteness**
  - Lack of Attention to Pre-Authentication and to Linkage forward to Authorisation
  - Inadequate Handling of Principal-Agent

# Public Policy Aspects

- **Understanding and Valuation of Privacy**
  - Limited Conception of Privacy
  - 'Opt-Out' in Lieu of Consent / 'Opt-In'
  - Lack of Consumer Trust
- **No Appreciation of the Value of:**
  - Multiple Identities and Silo'd Personal Data
  - Anonymity and Pseudonymity
- **No Representation of Consumer Interests**
  - No Consumer Focus Groups
  - No Consultation with Reps, Advocates
  - Wholly US-Centric (1/3rd of the World's users)

# (Id)entity (Mis)management?

## The Agenda

- Authentication – of what?
- Identity, Identifiers, Entities, ..., Nyms
- Entifiers for People – Biometrics
- ‘Identity Management’
  - Phases in User Access Security
  - Many Architectures
  - Competition Between and Within
  - Issues

**Identity Management?  
or  
(Id)Entity Mismanagement?**

**Roger Clarke FACS  
Xamax Consultancy, Canberra**

**Visiting Professor/Fellow, Unis. of Hong Kong, U.N.S.W., ANU**

<http://www.xamax.com.au/EC/IdMngt> { .html, .ppt }

**A.C.S. Conference on 'I.T. in Government'  
Canberra - 5 November 2004**