Access Control in the Era of Active Artefacts
A Generic Theory of Authorization to Support IS Practice and Research

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra

Visiting Professor in the School of Computing, ANU
and in the Allens Hub for Technology, Law and Innovation, UNSW Law

ACIS #34 – 5-8 December 2023

http://rogerclarke.com/ID/PGTAz {.html, .pdf}

The Agenda

- Context and Motivation
- A Quick Recap on **ICT Conventions** re Authorization, Access Control, and Identity Management (IdM)
- **The Pragmatic Metatheoretic Model**
- A Generic Theory:
  - **(Id)Entity Management (IdEM)**
    - Registration Phase, incl. Authorization
    - Operational Phase, incl. Access Control
  - Implications

XAMAX Consultancy Pty Ltd

Context

- The crisis in Data Insecurity
- Ongoing misconceptions inherent in Id Management

Motivation

- Effective representation of relevant phenomena, to overcome **Id Management inadequacies**, past and present
- A framework that reflects the intellectual complexities and identifies the proponent's **'metatheoretic assumptions'**
- A model that's **pragmatic**, and supports instrumentalism – for IS practice, and for IS-relevant research

Dictionary Definitions

- **Authorization**

  "The action of authorizing a person or thing ..." (OED 1)

- **Authorize**

  "To give official **permission** for or formal **approval** to (an action, undertaking, etc.);
  to approve, **sanction**" (OED 3a)

  "To give (a person or agent) legal or formal **authority** (to do something);
  to give formal permission to; to **empower**" (OED 3b)

XAMAX Consultancy Pty Ltd

ICT Standards Definitions

- ***Authorization*** *is* ***a process*** *for granting approval to a system entity to access a system resource (RFC4949 2007, at 1b(I), p.29)*
- ***Access control or authorization*** *... is* ***the decision*** *to permit or deny a subject access to system objects (network, data, application, service, etc.) (NIST800-162 2014, p.2)*
- Ambiguities in other important sources, e.g. ISO/IEC 27000, X.800 Security Architecture, the NIST Guide (Josang 2017)

XAMAX Consultancy Pty Ltd

ICT Standards Definitions

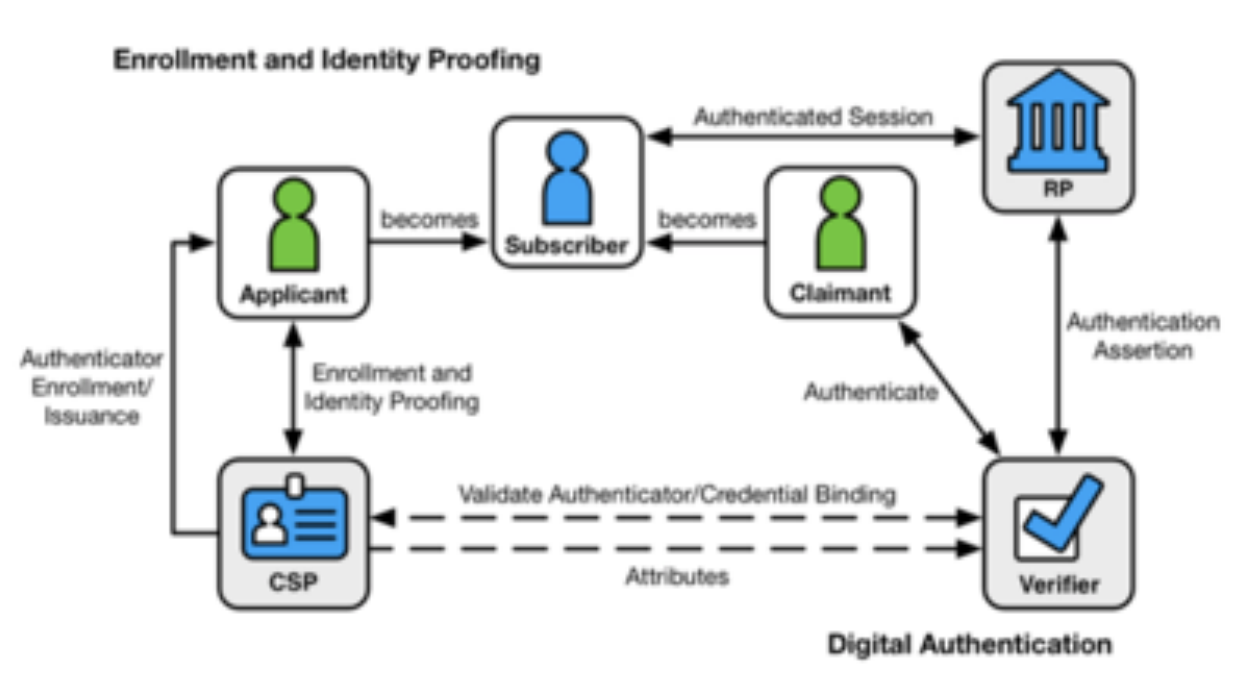
- ***Authorization** is **a process** for granting approval to a system entity to access a system resource (RFC4949 2007, at 1b(I), p.29)*
- ***Access control or authorization** ... is **the decision** to permit or deny a subject access to system objects (network, data, application, service, etc.) (NIST800-162 2014, p.2)*
- Ambiguities in other important sources, e.g. ISO/IEC 27000, X.800 Security Architecture, the NIST Guide (Josang 2017)

- So Josang (2017) proposed:
  - **Authorization** as specification of access policies
  - **Access control** as application/enforcement thereof

XAMAX Consultancy Pty Ltd

ICT Industry and 'Identity Management' (IdM)

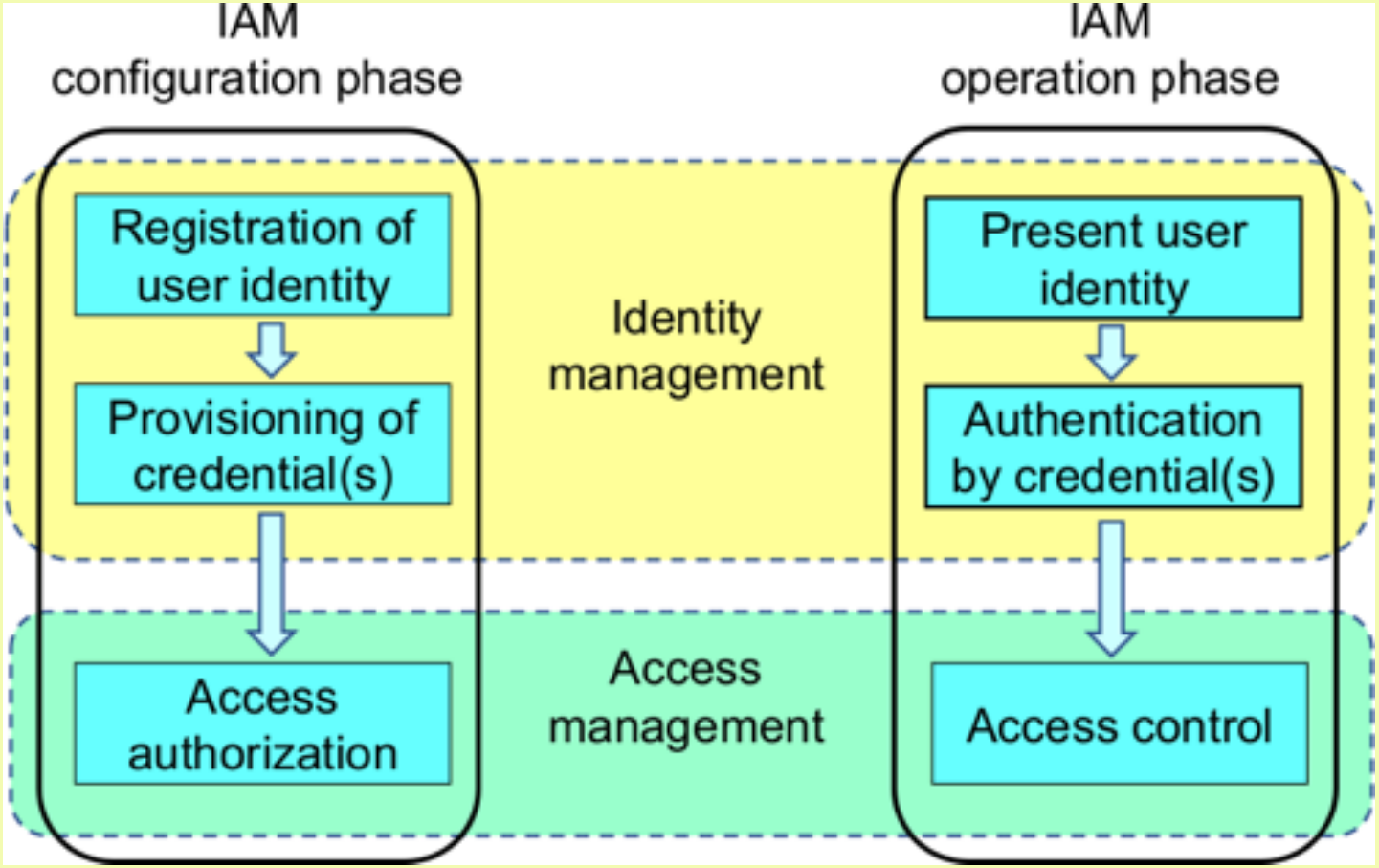
- *Identity management ... concerns the governance and administration of* ***a unique digital representation of a user****, including all associated attributes and entitlements (Gartner, extracted 29 Mar 2023, emphasis added)*



XAMAX Consultancy Pty Ltd

NIST-800-63-3 2017 (p.10)

A More Coherent Model of Identity Management



XAMAX Consultancy Pty Ltd

https://en.wikipedia.org/wiki/File:Fig-IAM-phases.png
See also Josang (2017, p.137), Fig. 1

Access Control Models and Their Foci

- **Identity** of the Actor
  - Discretionary Access Control (DAC)
  - Identity-Based Access Control (**IBAC**)
- **Role** performed by the Actor
  - Role-Based Access Control (**RBAC**)
- **Attribute**(s) of the Actor, of the IS Resource, and/or of environmental variables
  - Attribute-Based Access Control (**ABAC**)
- **Task** being performed by the Actor
  - Task-Based Access Control (**TBAC**)

Context

- The crisis in Data Insecurity
- Ongoing misconceptions inherent in Id Management

Motivation

- Effective representation of relevant phenomena to overcome Id Management inadequacies, past and present
- A framework that reflects the intellectual complexities and identifies the proponent's 'metatheoretic assumptions'
- A model that's pragmatic, and supports instrumentalism – for IS practice, and for IS-relevant research

==>> A Pragmatic Metatheoretic Model
(a) for IS Practice and Practice-Relevant Research
(b) to underpin improvements to Id Management

XAMAX Consultancy Pty Ltd

A Pragmatic Metatheoretic Model

'Metatheory'

Ontology – the study of existence
Epistemology – the study of knowledge
Axiology – the study of value

A Pragmatic Metatheoretic Model

'Metatheory'

Ontology – the study of existence
Epistemology – the study of knowledge
Axiology – the study of value

'Pragmatism'

In philosophy, 'concerned with understanding and action'
not just describing and representing

In IS practice, approximates and articulates 'common sense'

A Pragmatic Metatheoretic Model

'Metatheory'

Ontology – the study of existence
Epistemology – the study of knowledge
Axiology – the study of value

'Pragmatism'

In philosophy, 'concerned with understanding and action'
not just describing and representing

In IS practice, approximates and articulates 'common sense'

Metatheoretic Assumptions

Conscious / Unconscious

Explicit / Undeclared

Metatheoretic Commitments

Metatheoretic Commitments

- **Pragmatism**
  For understanding and action, not just describing and representing, and hence oriented towards IS Practice and Practice-Relevant Research
- **The Conception of an IS**
  "A set of interacting artefacts and human activities that performs one or more functions involving the handling of data and information"
- **Socio-Technical View**
  Interweaving of artefacts with human activity means that neither a technical nor social view provides a sufficient basis for understanding

The Ontological Aspect of the Model

- **The Dualism postulate**:
  - There <u>are</u> material realities (the Real-World)

  & There <u>is</u> internal 'mind-stuff'
  (spiritual, intellectual or Abstract-Worlds)

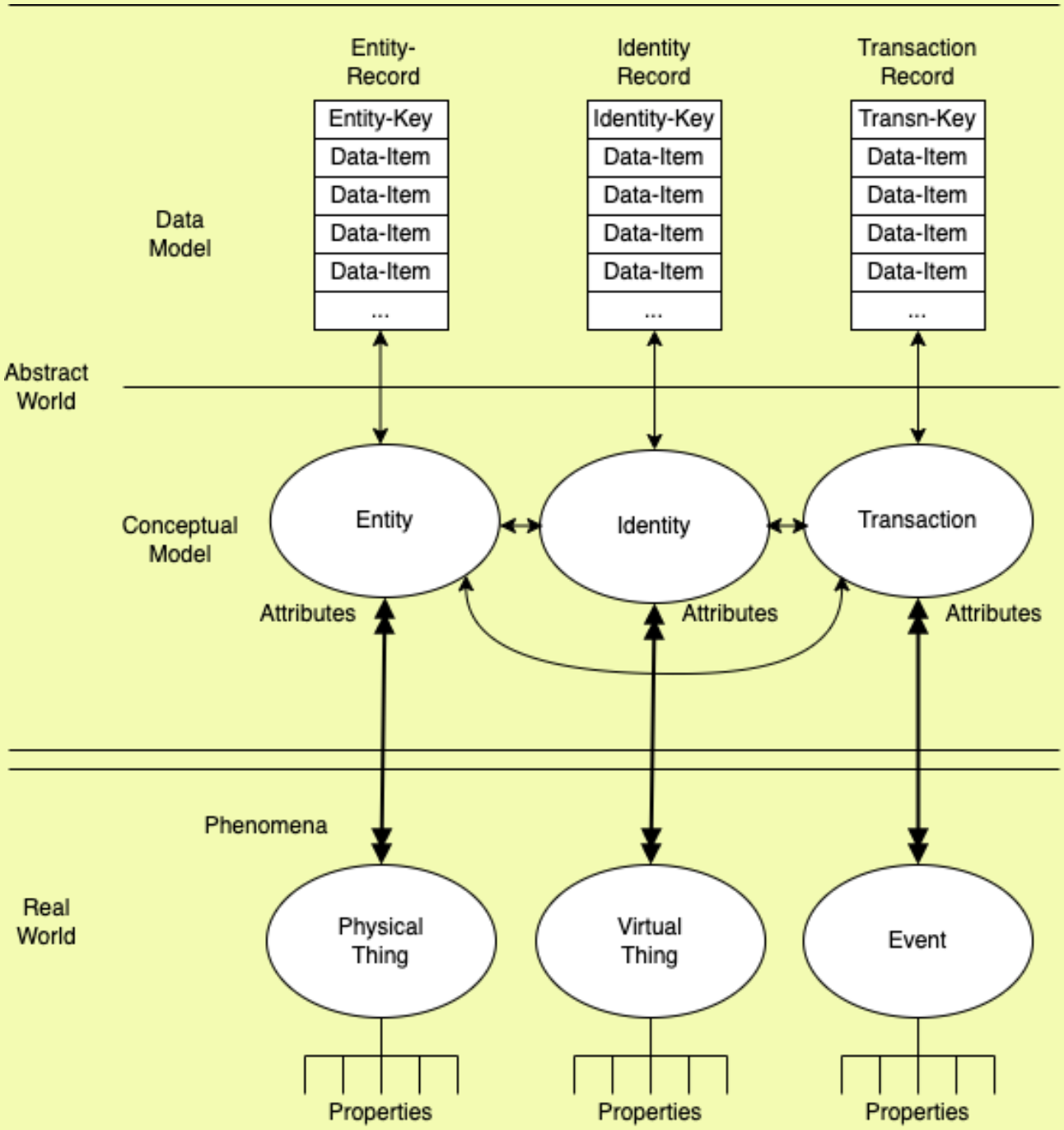
- **Real-World <u>Phenomena</u> and <u>Properties</u>**
  The wavelength of electromagnetic radiation, hardness and brittleness of things, event-duration
- **Abstract-World <u>Ideas</u>**
  Numbers, colours, names, addresses, time, ...

XAMAX Consultancy Pty Ltd

Metatheoretic Commitments

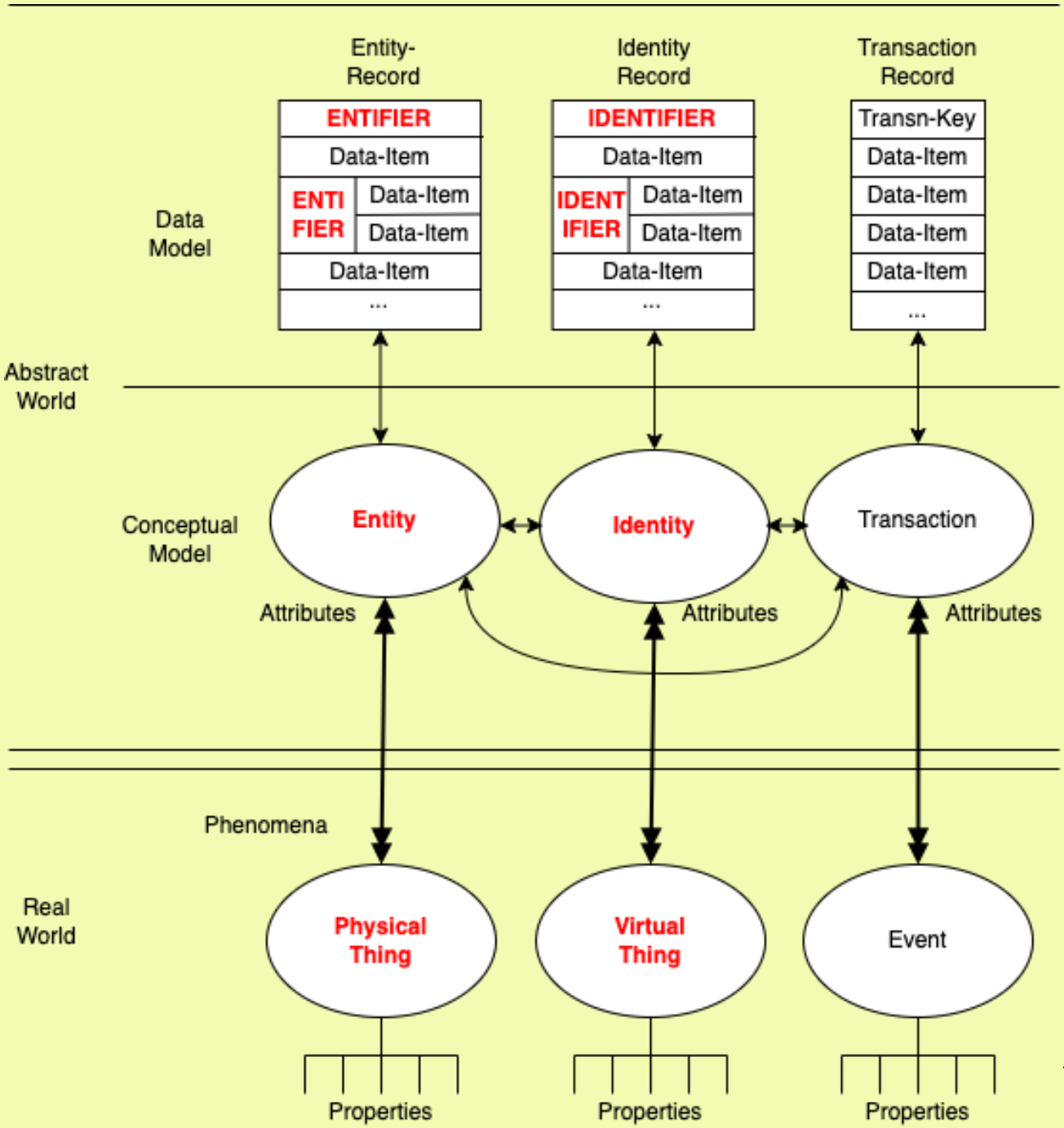
- **Pragmatism**
  For understanding and action, not just describing and representing, and hence oriented towards IS Practice and Practice-Relevant Research
- **The Conception of an IS**
  "A set of interacting artefacts and human activities that performs one or more functions involving the handling of data and information"
- **Socio-Technical View**
  Interweaving of artefacts with human activity means that neither a technical nor social view provides a sufficient basis for understanding
- **Ontology**
  Realism and Idealism, blended, dependent on circumstances
- **Epistemology**
  Empiricism and Apriorism, blended, dependent on circumstances
  In IS, assumptions of humanly-accessible Truth are seldom justifiable
- **Axiology**
  Teleological and Instrumentalist, supporting effective, efficient and adaptable IS serving the needs of the sponsor but also all stakeholders

Key Elements of the Pragmatic Metatheoretic Model



XAMAX Consultancy Pty Ltd

Key Differences about the Pragmatic Metatheoretic Model



XAMAX Consultancy Pty Ltd

Physical Things and Virtual Things

- **Inanimate Objects** (Inventory-Items, Equipment)
  - Containers ⊃ Pallet-Loads ⊃ Boxes ⊃ Cartons
- **Active Objects**
  - Mobile-Phone/Handy/Cellulare ⊃ **SIM-Cards**
  - Computer ⊃ **Processes**
  - Car ⊃ **Convoy-Lead, Get-Away Car, Speed-Check, ...**
- **Organisations** (Companies, Associations, Govt Agencies, ...)
- **Humans and The Roles Humans Play**

  Seller, buyer, supplier, receiver, debtor, creditor, payer, payee, principal, agent, franchisor, franchisee, lessor, lessee, copyright licensor, copyright licensee, employer, employee, contractor, contractee, trustee, beneficiary, tax-assessor, tax-assessee, business licensor, business licensee, plaintiff, respondent, investigator, investigatee, defendant, ...

XAMAX Consultancy Pty Ltd

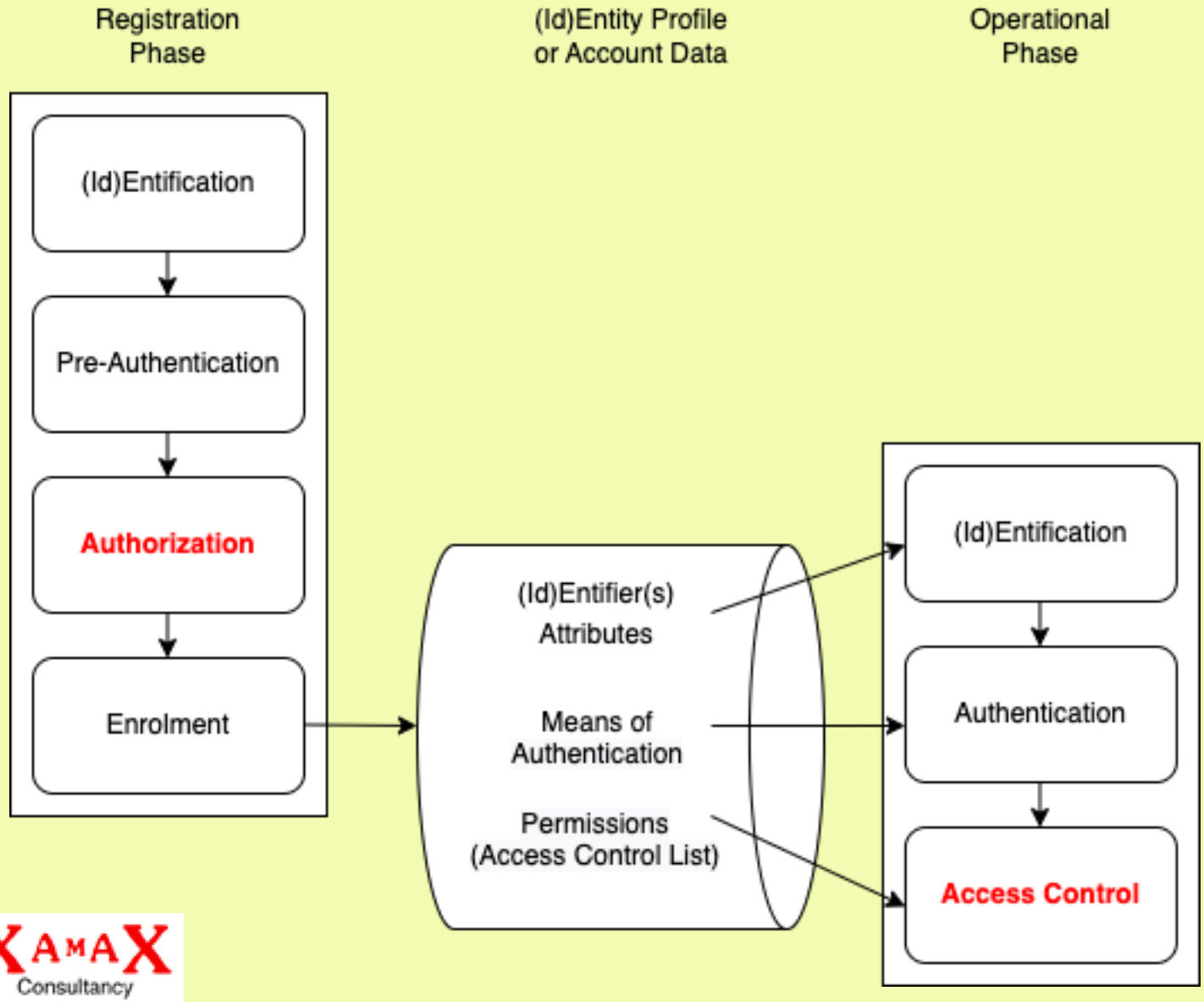
An Application of the Pragmatic Metatheoretic Model
A Fully-Coherent Model of
(Id)Entity Management (IdEM)

The architecture,
the infrastructure
and the processes

whereby Access to IS Resources
is enabled for appropriate Users,
and otherwise denied

XAMAX Consultancy Pty Ltd

Generic Process Model of (Id)Entity Management (IdEM)



XAMAX Consultancy Pty Ltd

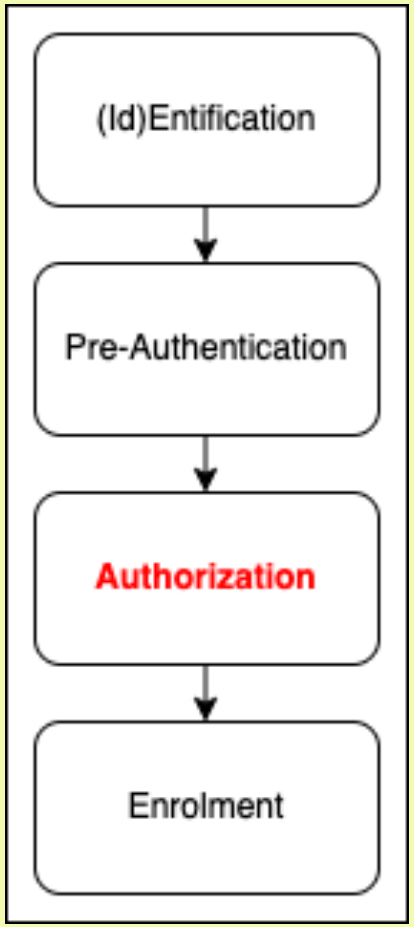
(Id)EM Terminology

- **Actor:** A Real-World Thing capable of action on an IS Resource, including humans and some categories of artefact
- **Entity**: An Abstract-World representation of a Physical Actor
- **Identity**: An Abstract-World representation of a Virtual Actor

- **IS Resource:** Data or a Process in the Abstract World, that an IS is capable of acting upon
- **Permission:** An entitlement or authority to be provided with the capability to perform a particular act in relation to a particular IS Resource

XAMAX Consultancy Pty Ltd

The Registration Phase

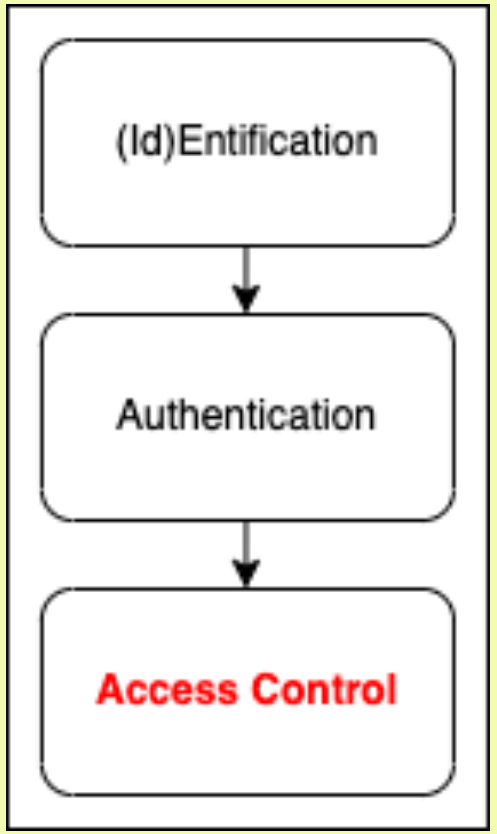


- **(Id)Entification**: Assert the appropriateness of providing a particular (Id)Entity with access to particular IS Resources
- **Pre-Authentication**: Acquire and evaluate Evidence, to assess the degree of confidence in the reliability of the Assertion
- **Authorization**: Apply decision criteria to determine what Permissions are to be made available to that (Id)Entity
- **Enrolment**: Record Data to enable the Operational Phase to be conducted in an effective and efficient manner

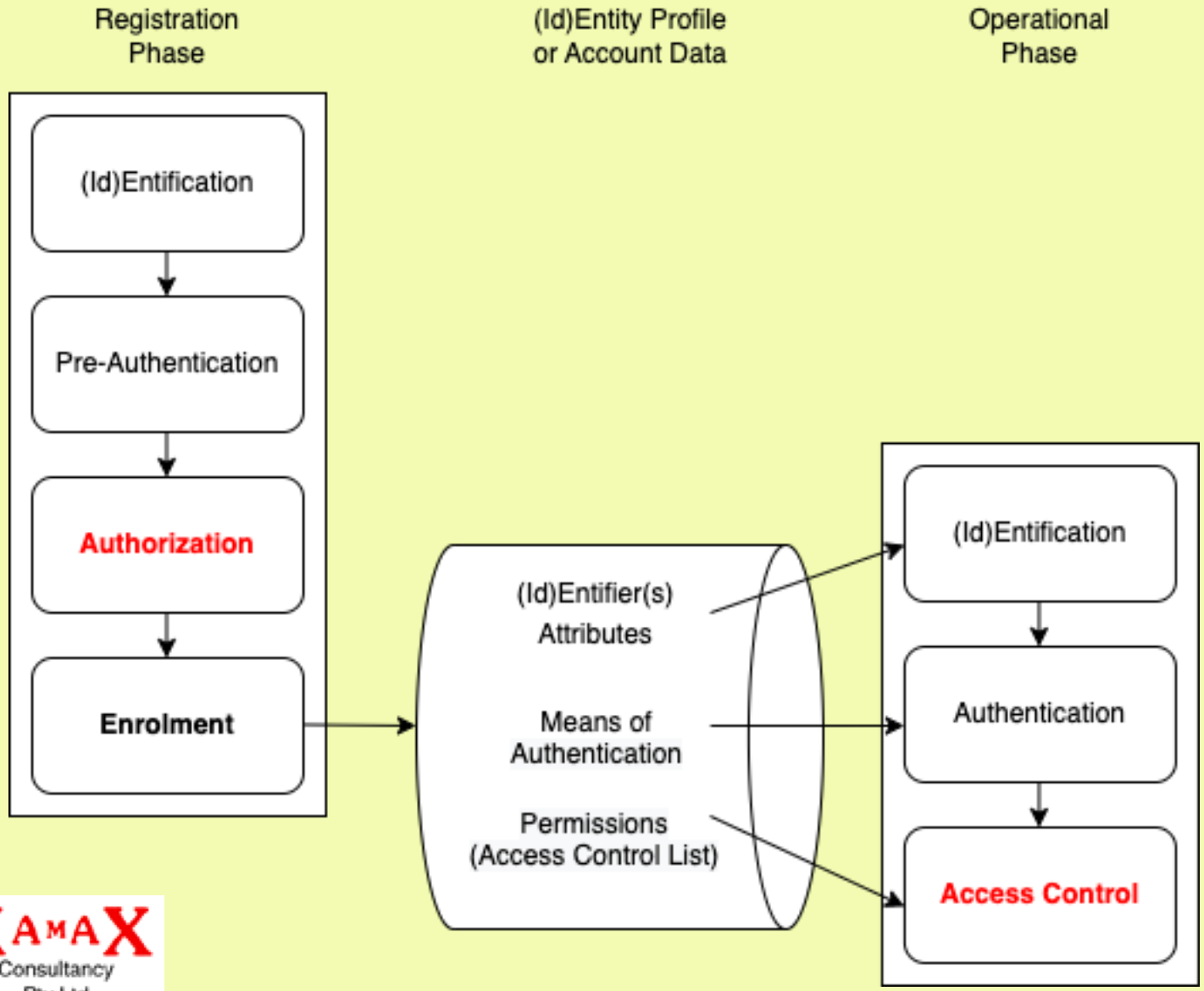
XAMAX Consultancy Pty Ltd

The Operational Phase

- **(Id)Entification**: Assert that the presenting (Id)Entity is the or an appropriate one to operate as that (Id)Entity
- **Authentication**: Use the previously-recorded Means of Authentication to assess the degree of confidence in the reliability of that Assertion
- **Access Control**: Use the previously-recorded Permissions to establish a Session that enables an authorized user to exercise the appropriate Permissions



Generic Process Model of (Id)Entity Management (IdEM)



XAMAX Consultancy Pty Ltd

Key Aspects of Authorization

- **Authorization**: A process whereby an Authorization Authority decides whether to declare that an Actor has one or more Permissions in relation to a particular IS Resource

  A Permission may be specific to an Actor, or the Actor may be assigned to a Role and inherit Permissions from that Role

- **Authorization Authority**: An Entity with legal or practical power (*de juré* or *de facto*) to determine Permissions that a particular Actor has in relation to a particular IS Resource

- **Role**: A coherent pattern of behaviour performed in a particular context

  Job-Description / Appointment – call-centre operator, CISO, CEO
  Organisational Function – fire warden, appointment committee member
  External Function – supplier, customer, applicant, consumer advocate

Actor

A Real-World Thing capable of action on an IS Resource

- **Physical Things**
  - Humans
  - Some Artefacts
- **Virtual Things**
  - Human Identities
  - Computer Processes

A Thing not capable of action needs a capable Thing as Agent

IS Resource

Data or a Process, in the Abstract World, that an IS is capable of acting upon

Data
Database
File
Record
Item
Document

Process
Service
Application
Function
Program
Transaction
Action-Capability

Key Aspects of Access Control

- **Access Control:** A process that establishes a Session that enables an Authorized User to exercise appropriate Permissions
- **Login:** A process whereby an (Id)Entity communicates a request to exercise Permissions, which triggers an Authentication process, and, if successful, an Access Control process
- **Session:** A period of time during which an authenticated (Id)Entity is able to exercise its Permissions in relation to IS Resources
- **{Authorized} User:** An authenticated (Id)Entity, commonly with an (Id)Entifier (userid, loginid or username), that is provided with means to exercise Permissions in relation to particular IS Resources
- **Account:** The data-holdings associated with an Authorized User for which an Authorization process has created a Permission
- **End User:** A User provided Permissions for application purposes
- **System User:** A User provided Permissions for system management

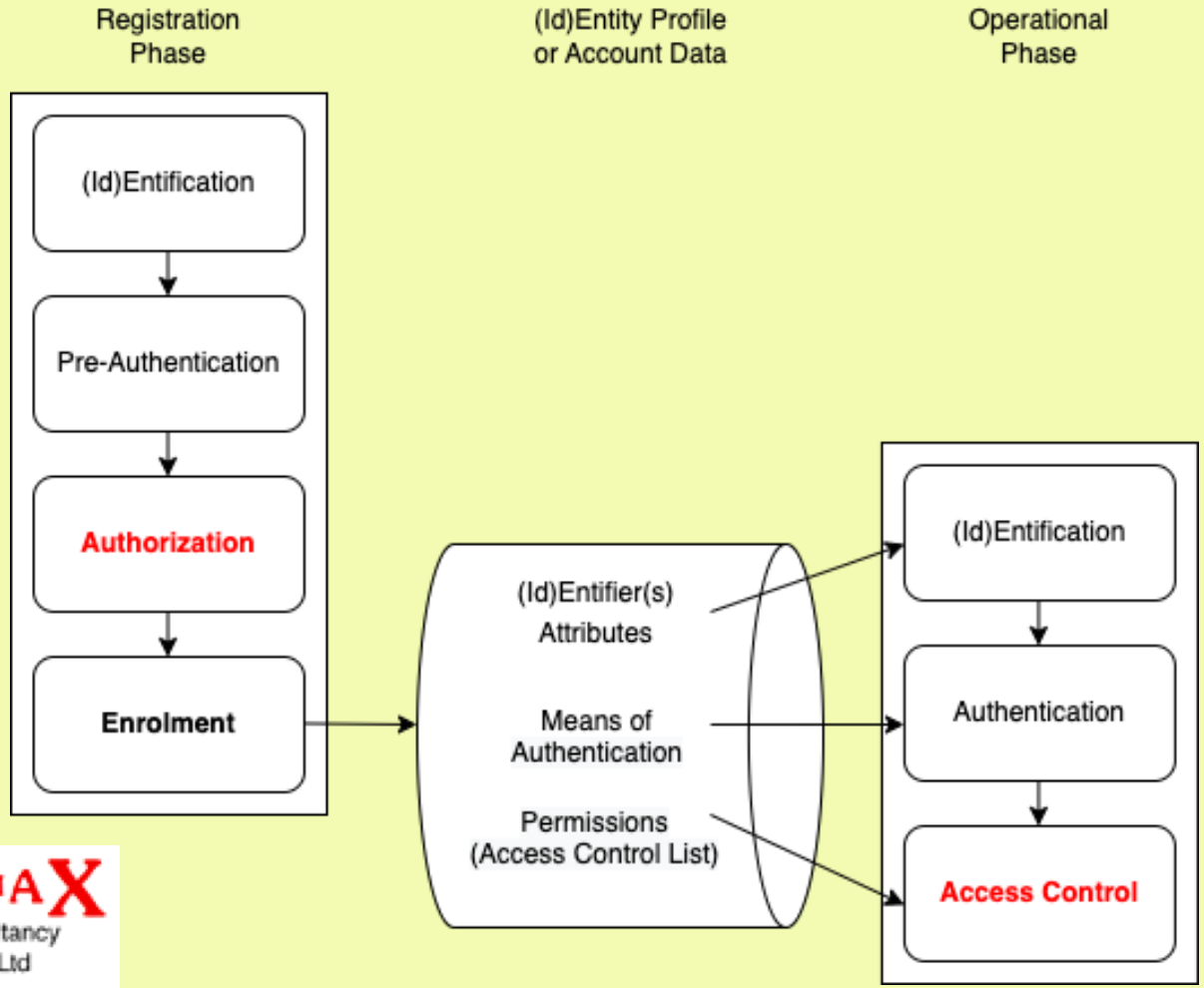
The Agenda

- Context and Motivation
- A Quick Recap on **ICT Conventions** re Authorization, Access Control, and Identity Management (IdM)
- **The Pragmatic Metatheoretic Model**
- A Generic Theory:
  - **(Id)Entity Management (IdEM)**
    - Registration Phase, incl. Authorization
    - Operational Phase, incl. Access Control
  - **Implications**

XAMAX Consultancy Pty Ltd

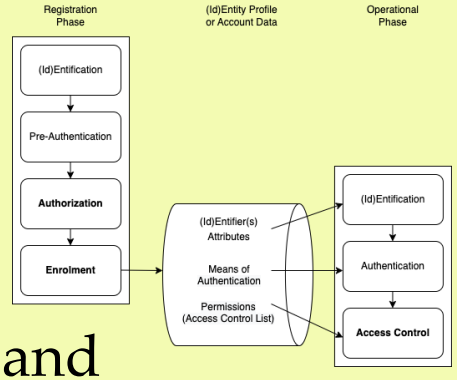
Implications of (Id)Entity Management (IdEM)

The Pragmatic Metatheoretic Model enables clarity about weaknesses in conventional Identity Management (IdM), and the development of **a robust replacement model** referred to as (Id)Entity Management



XAMAX Consultancy Pty Ltd

Implications for IS Theory and Practice



- **Entities** (for Physical Things) **are distinguished** from Identities (for Virtual Things)
- The (Id)EM model offers an **orderly set of phases** and steps, applies **intuitive terms** to them, provides **a coherent set of definitions**, and identifies the categories of data necessary to enable the operational steps
- The (Id)EM model conceives **Authentication relative to a degree of confidence in an Assertion**, not accessible truth
- In the (Id)EM model, Roles and associated Identities are **plural**, and **relative to an IS, not organisational positions**
- The (Id)EM model recognises the cost and intrusiveness of (Id)Entity Authentication, and **encourages careful choice of which Assertions really require Authentication**

XAMAX Consultancy Pty Ltd

A Further Implication for IS
Access Control to Real-World Things and Events

- The focus of IS has been on Abstract-World IS Resources
- ICT also acts in the Real-World, on Phenomena
  - Supervisory Control and Data Acquisition (SCADA)
  - Industrial Control Systems (ICS)
  - Mechatronics
  - Robotics
  - The Internet of Things (IoT)
- The model is readily extended to such Active Artefacts

XAMAX Consultancy Pty Ltd

Access Control in the Era of Active Artefacts
A Generic Theory of Authorization to Support IS Practice and Research

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra

Visiting Professor in the School of Computing, ANU
and in the Allens Hub for Technology, Law and Innovation, UNSW Law

ACIS #34 – 5-8 December 2023

http://rogerclarke.com/ID/PGTAz {.html, .pdf}

Approach

- **Pure Research**
  'I want to discover and understand what is'
- **Applied Research**
  'I have a research tool, so I'll use it' (hammer, so nail)
- **Instrumentalist Research**
  There's a problem, so I'll try to solve it
- **'Pragmatism'**
  - In philosophy, 'concerned with understanding and action', not merely describing and representing
  - In IS practice, approximates and articulates a layman's 'common sense' interpretation

A Pragmatic Epistemological Model

- "An open attitude toward any kind of epistemological foundation that might work"
- "Epistemological and methodological diversity"
- "Disciplined methodological pluralism"

- **Empiricist orientation, if mostly non-human entities**
  - Guidance systems for aircraft and spacecraft
  - Heavily-automated production control /inventory systems
- **Recognition of innateness, for systems with human involvement or with significant impact on humans**

Employee Attributes

- **Human Entity**
  - Emergency Contact-Name, Bank a/c for Salary
    Do they <u>really</u> need a biometric/brand/embedded chip?
- **Human Identity**, persistent, but change over time
  - Position, Start-Date, End-Date, Permissions
- **Human Identity**, occasional and may be shared
  - Fire Warden, Zone, Training Certs, Permissions

XAMAX Consultancy Pty Ltd

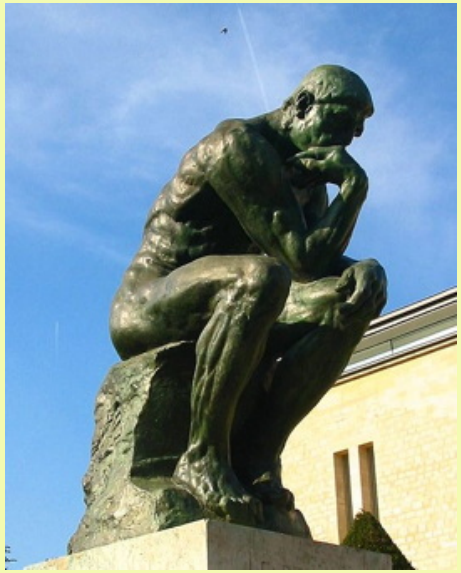
Spares from Prior Presentations

XAMAX Consultancy Pty Ltd

Ontology / Existence or 'Being'

Phenomena – Matter, Things, Events, Properties

Materialism
Matter exists, independently
of whether a human detects it



Cogito ergo est
I think it is, therefore it is

Idealism
Everything exists in the human mind.
The 'real world' I think I see is only an idea.
That idea may be shared, but not identically

Epistemology – Different Forms of Knowledge

- **'Codified Knowledge'** (Empiricist / Positivist)
  Expressed
    In text, defined dialect, flowcharts, formulae, blueprints, ...
  Disembodied, but communicable among people
  Capable of delivering a coherent body of information to individuals in particular contexts

- **'Tacit Knowledge'** **(**Innate or Reasoned)
  Exists in a particular person
  Informal and intangible
  Not readily communicated

XAMAX Consultancy Pty Ltd

Axiological Aspects

- The study of **Value(s)**
  - A **'Virtue'** dimension of 'good / bad'
    (Loose even mystical criteria?)
  - A **'Deontic'** approach, related to duty / obligation on a 'mandated / optional / forbidden' dimension
  - A **'Utilitarian' or 'Consequentialism'** approach based on impacts or outcomes,
    which depends of clarity of purpose (Teleology)
- Positivism assumes a common denominator ('Utils'?)
- Antipositivism rejects that as fantasy

XAMAX Consultancy Pty Ltd

Axiology in IS

- Dominance of a narrow interpretation, based on **Economic** and **Financial** factors – **'Shareholder Value'**
- **Social** and **Environmental** factors?
  Triple-bottom-line reporting / 'people, planet and profits'
  Corporate Social Responsibility (CSR)
- **Human** values?
  - Hedonism
  - Conservation/ism: Conformity, Tradition, Security
  - Openness to Change: Self-Direction, Stimulation
  - Self-Enhancement: Achievement, Power
  - Self-Transcendence: Benevolence, Universalism
- **Evident in**: Multiview, Soft Systems Methodology, Participatory Systems Design, Value-Sensitive Design

Stakeholder Theory

- Postulated in 1963/83 as **a counterpoint to Shareholder**
- "Any party that can affect, or is affected by, the achievement of the organisation's objectives"

- **Participants** – But in IS often conflated with 'User'
- **Non-Participants / 'Usees'**

- Characteristics:
  - **P – O – W – E – R**
  - Legitimacy
  - Urgency

Researcher Perspective Theory

- **c. 90%** of papers on research of relevance to IS practice are **Single-Perspective, i.e. all other stakeholders' interests are constraints on the primary stakeholder**
- **c. 90% of those papers privilege the System Sponsor**

- Far less Single-Perspective other-than-System-Sponsor
- Little Dual-Perspective Research (cf. win-win!?)
- Very little Multi-Perspective Research (cf. win-win-win) (even in supply chain and network studies!?)

- **IS Researchers score a Fail on axiological insight**

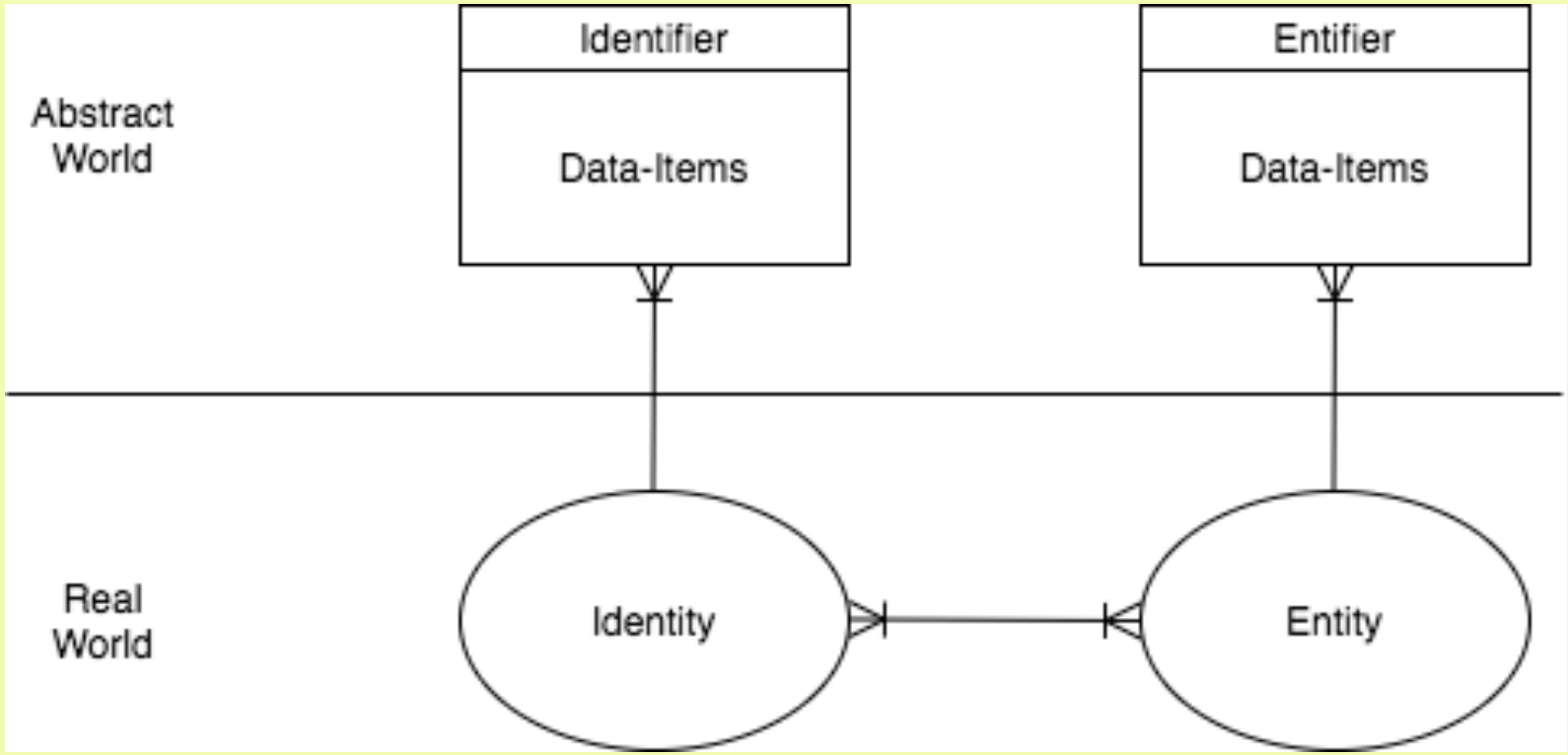
A Pragmatic Axiological Model

- "An open attitude toward any kind of axiological foundation that might work"
- "Axiological diversity"
- "Disciplined axiological pluralism"

- Single-Perspective
  - System-Sponsor 90%
  - Other Stakeholder 5%
- Dual-Perspective 3%
- Multi-Perspective 2%

XAMAX Consultancy Pty Ltd

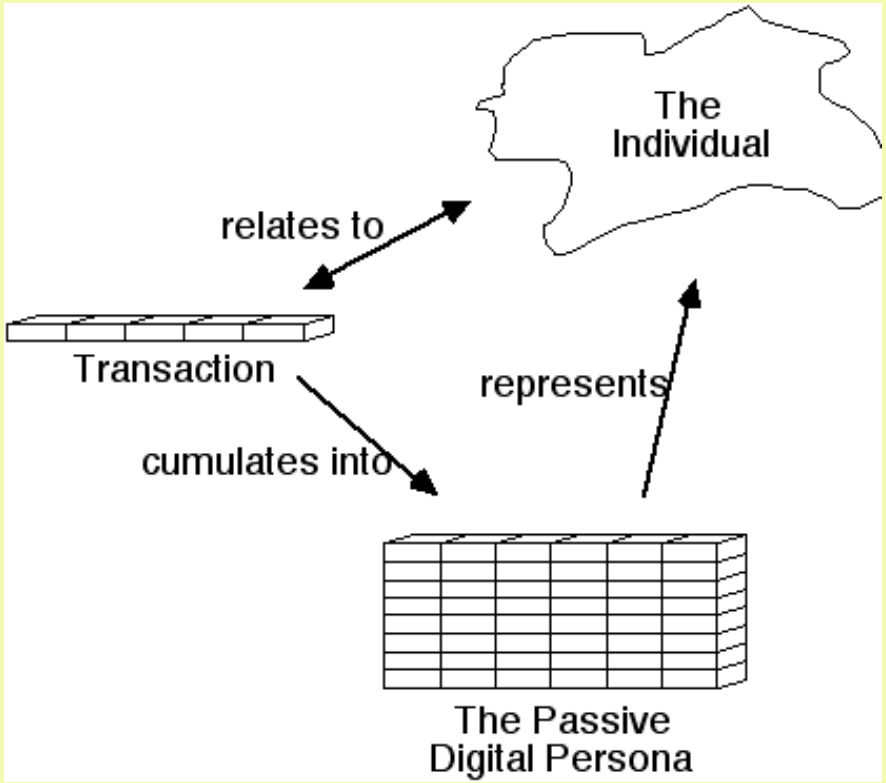
Application to (Id)Entity Management



XAMAX Consultancy Pty Ltd

The Digital Persona

A model of the public personality of an (Id)Entity, based on Data, maintained by Transactions, for use as **a proxy for the (Id)Entity**

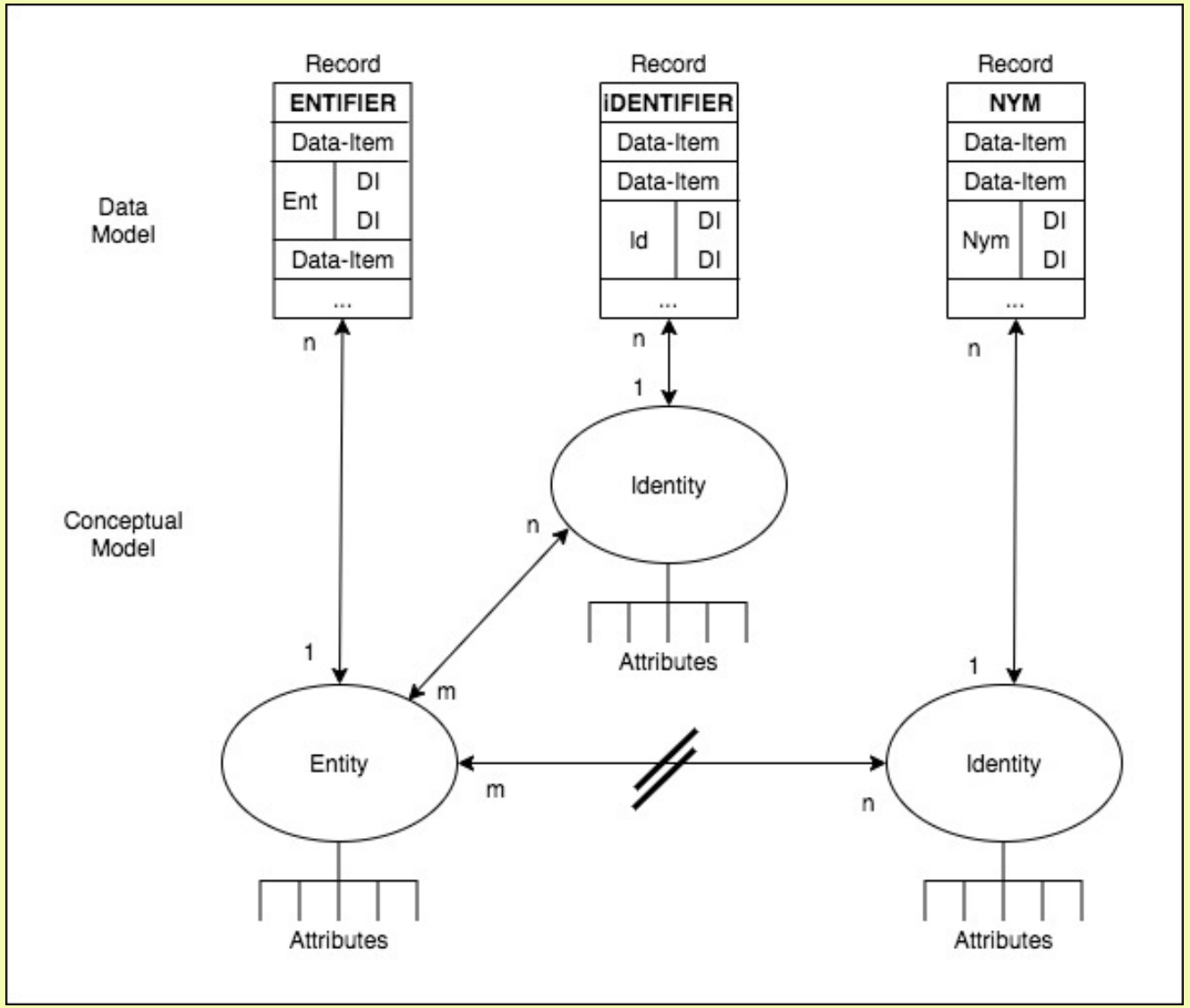


XAMAX Consultancy Pty Ltd

Clarke (1994, 2014)

The Digital Surveillance Economy (JIT, 2019)

(Id)Entities, (Id)Entifiers and Nyms



XAMAX Consultancy Pty Ltd

- **Personal Data De-identification** purports to prevent association of Personal Data with the relevant human (Id)Entity (if any)
- **Personal Data Re-identification** purports to reliably associate Data with the relevant human (Id)Entity, despite prior attempts at de-identification

- **Personal Data Falsification** is a process whereby Personal Data is changed so as to render it valueless for any purpose relating to the administration of relationships between organisations and particular individuals

  It **converts Empirical Data**, that reflects an Attribute of a Real-World human (Id)Entity, **into Synthetic Data** that represents a plausible Phenomenon, but not a real one

Contemporary Weaknesses the Model Addresses

** **Conventional Id Management fails** because **it conflates**:
Identities-Entities, Identifiers-Entifiers, Identification-Entification

- Conventional IS models have **unreliable association** of data records with human (id)entities
- Conventional IS have **mediocre correspondence** between Data-Item-Values and human phenomena
- **Conventional IS feature naive reuse and merger of data** ignoring purpose-specific QA, definitional incompatibility
- **Conventional IS depend on inaccurate digital personae** Impersonation, composite ids, masquerade, spoofing, id fraud, ...
- Organisations overlook **human (id)entity values**, risking mis-matched designs, resistance, low ROI

XAMAX Consultancy Pty Ltd

Authentication Process Quality Factors

- Effectiveness
- Implementation Ease
- Ease of Use
- User Attitude and Acceptance

Zviran & Erlich (2006)

- Accuracy
- Robustness
- User Acceptance
- Accessibility
- Feasibility
- Applicability
- Responsiveness
- Non-Reputability [sic: Non-Refutability]
- Maintainability

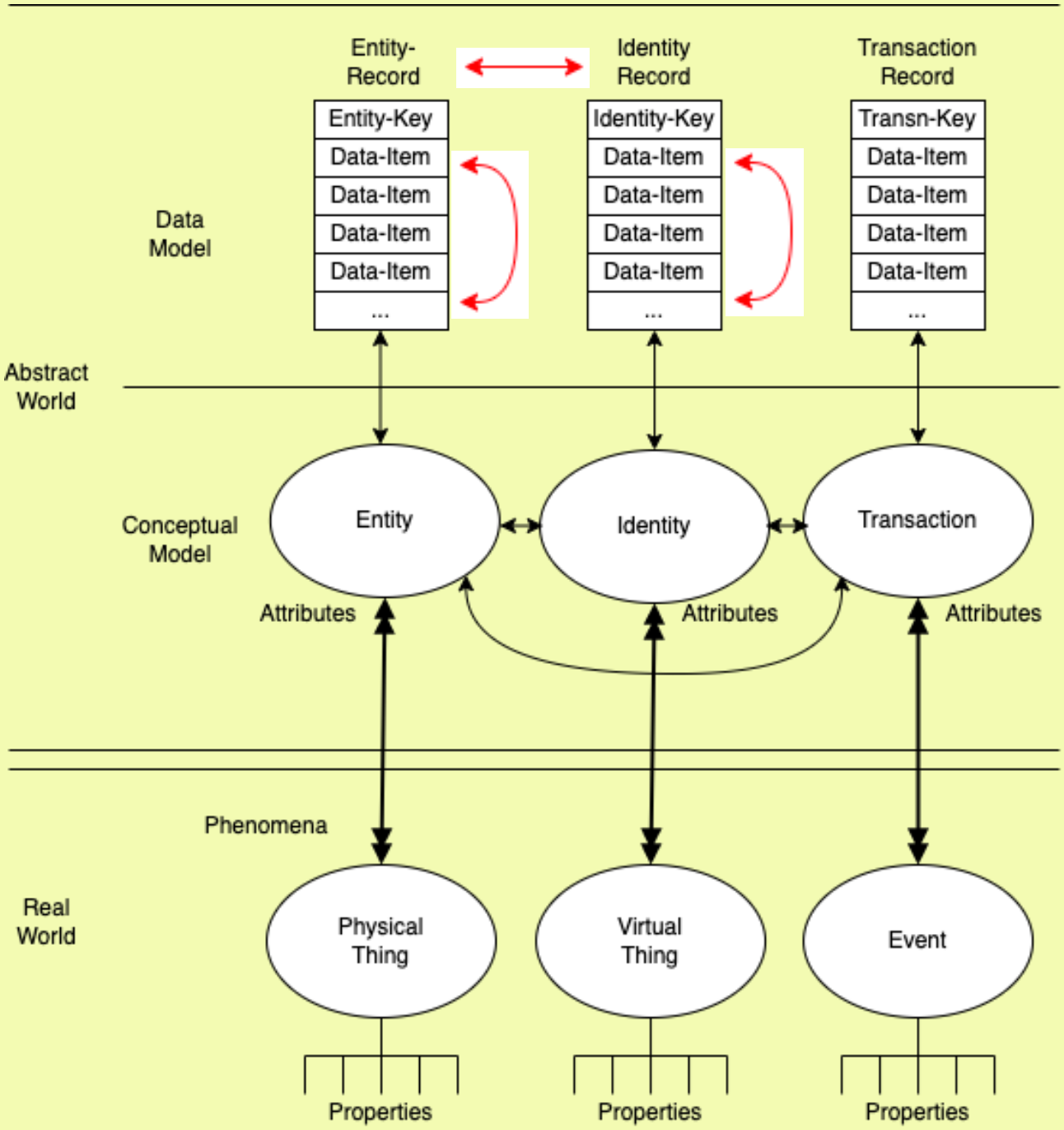
Way & Yuan (2009)

(6) (Id)Entity Match Assertion

- ***This Id-Record is appropriately associated with this other Id-Record***
  'The record containing this tax-file-identifier matches to the record containing this driver's licence number'
- ***This Entity-Record is appropriately associated with this other Entity-Record***
  'This description of recovered stolen goods is of the same diamond necklace as this description of stolen goods'
  'This DNA sample is from the same person as is represented by this DNA sample data from a particular family history database'
- ***This Id-Record is appropriately associated with this Entity-Record***
  'This process is running in this computing device'
  'The record for this client-number corresponds to this fingerprint-based record'
- ***This Transaction-Record is appropriately associated with this (Id)Entity-Record***

XAMAX Consultancy Pty Ltd

A particular (Id)Entity Record is appropriately associated with this other (Id)Entity Record



XAMAX Consultancy Pty Ltd

Evidence to Support the Authentication Process

Identity Assertion (1)

- Association is achieved by means of an Identifier

  ~~Rely on Proof of Identity (PoI)~~

  Rely on **Evidence of Identity (EoI)**:

  - 'What you **know**' (i.e. Data of some kind)
  - 'What you **have**' (Credential, Token containing one)

Entity Assertion (2)

- Each association is achieved by means of an Entifier
- Rely on **Evidence of Entity (EoE)**:
  - 'what you **are**' (i.e. Biometric, natural or implanted)

Implications

1) **The Effectiveness of Identity Management**
   - Distinguish (Id)Entity/(Id)Entifier
   - Understand that Evidence is not 'Proof'
   - Use Evidence appropriate to Assertion-Category
2) **The Effectiveness of Other Business Processes**
   - Recognise the risks of reliance on the Digital Persona and the abandonment of 'high-touch' Authentication
3) **The Economics of IS Design**
   - Avoid Expensive (Id)Entity Authentication when Property, Location or Value Authentication may do
4) **Stakeholder Interests**
   - Recognise the intrusiveness and costs for other actors