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 – 8 December 2023

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

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

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**)

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
  - Identifies the proponent's 'metatheoretic assumptions'
  - Is pragmatic, and supports instrumentalism

==>> A Pragmatic Metatheoretic Model

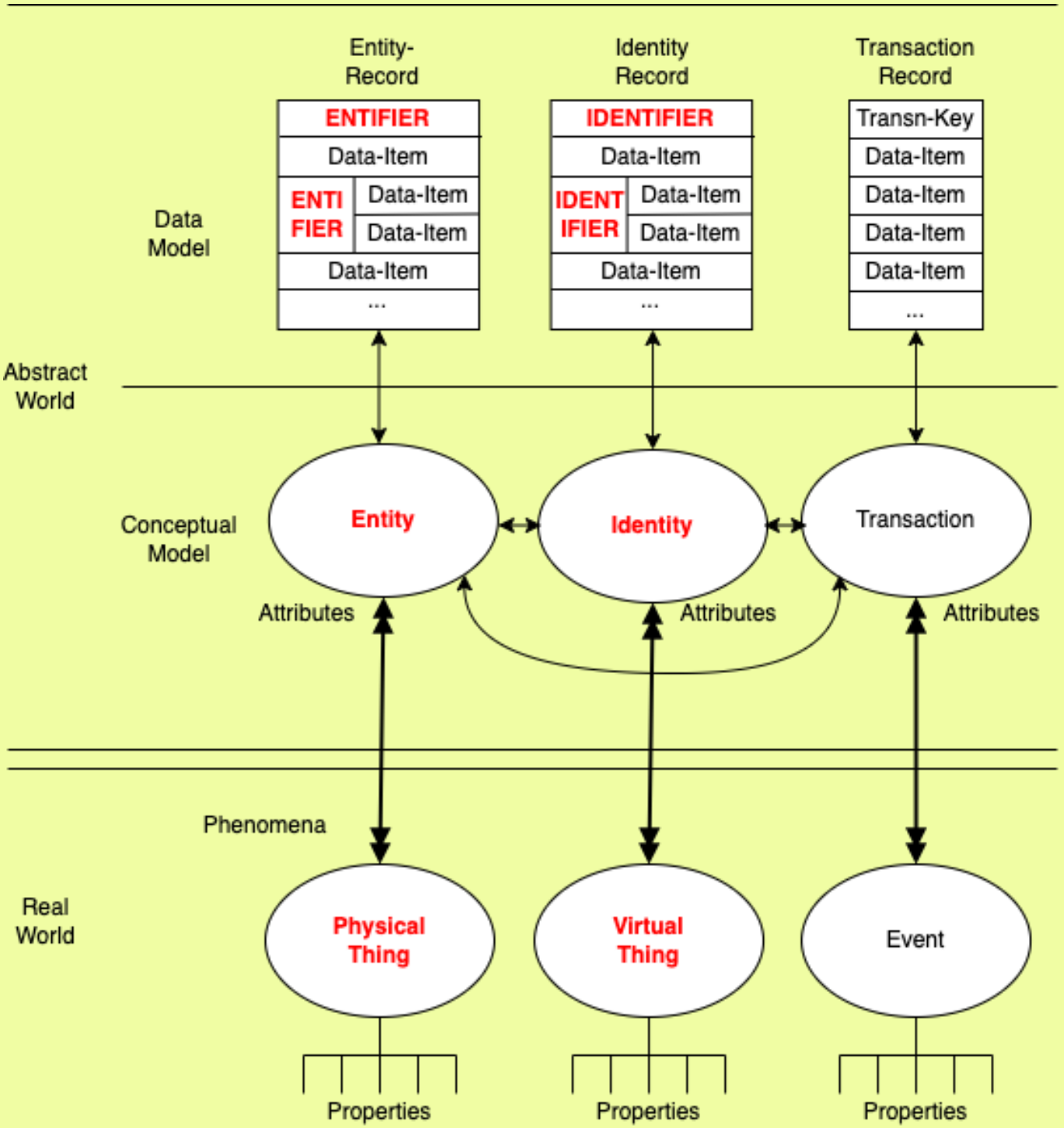
(a) for IS Practice and Practice-Relevant Research

(b) to underpin improvements to Id Management

XAMAX Consultancy Pty Ltd

Key Differences about the Pragmatic Metatheoretic Model

Clarke (2021)
at ACIS #32
http://www.rogerclarke.com
/ID/PMM.html



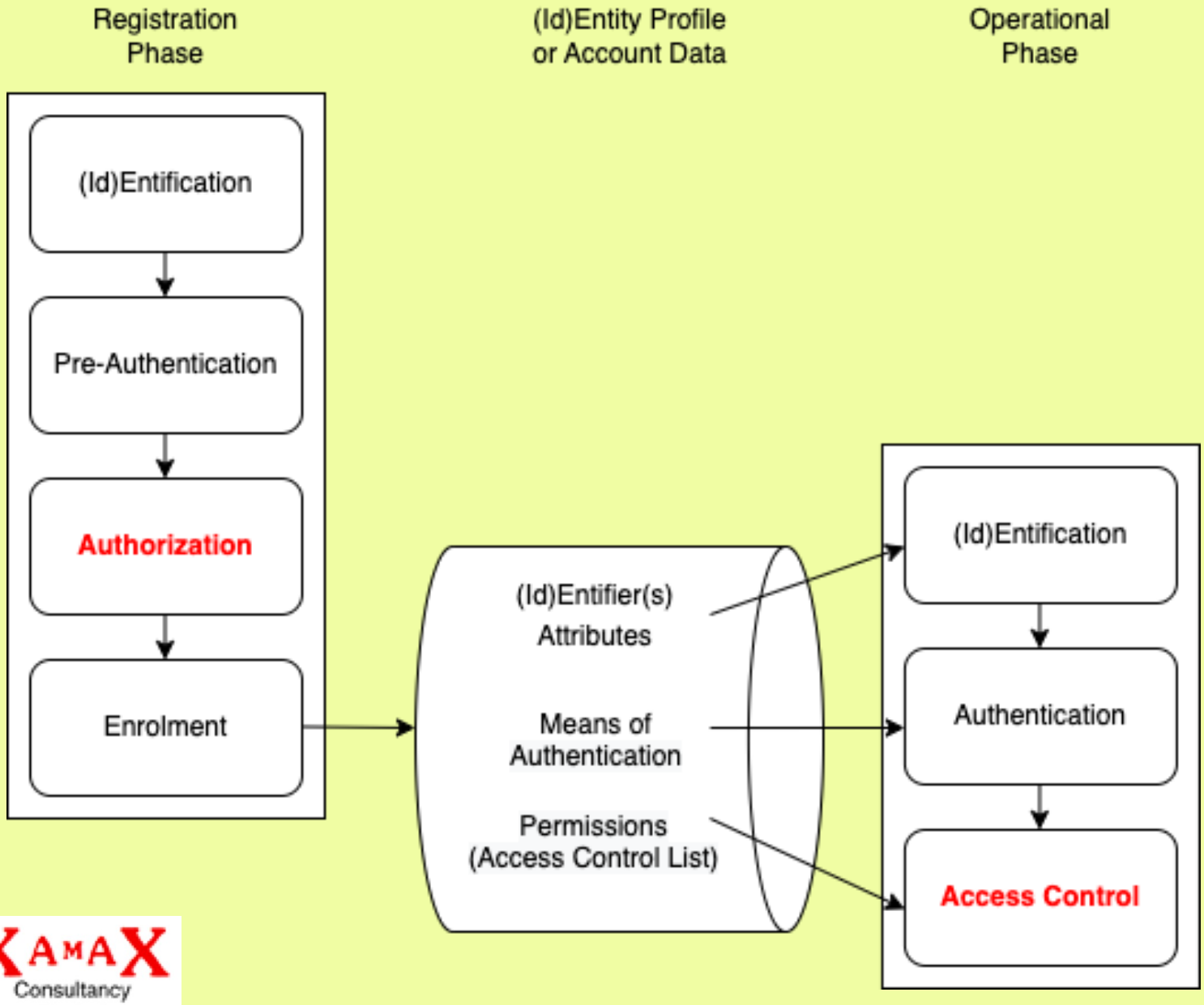
XAMAX Consultancy Pty Ltd

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, ...

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



XAMAX Consultancy Pty Ltd

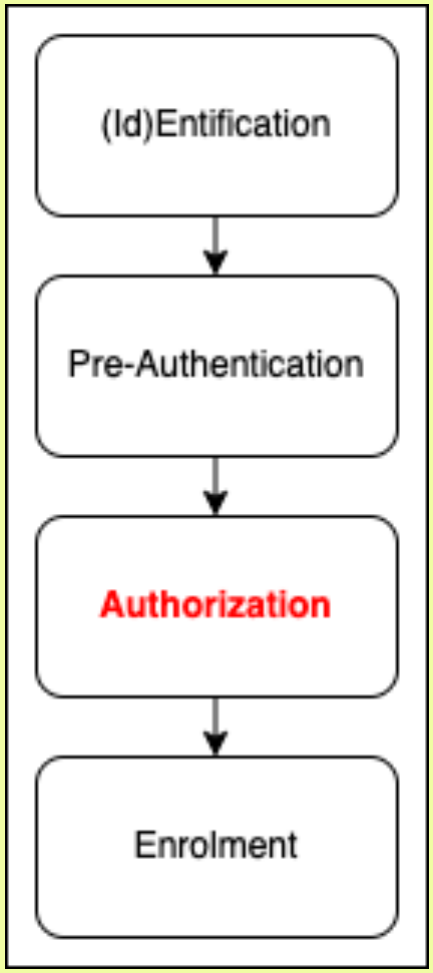
(Id)EM Terminology

- **Actor:** A Real-World Thing capable of action on an IS Resource, including humans and some categories of artefact. Real-World Actors may be Physical or Virtual Actors
- **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 (typically Read, Create, Amend, Delete) in relation to a particular IS Resource

XAMAX Consultancy Pty Ltd

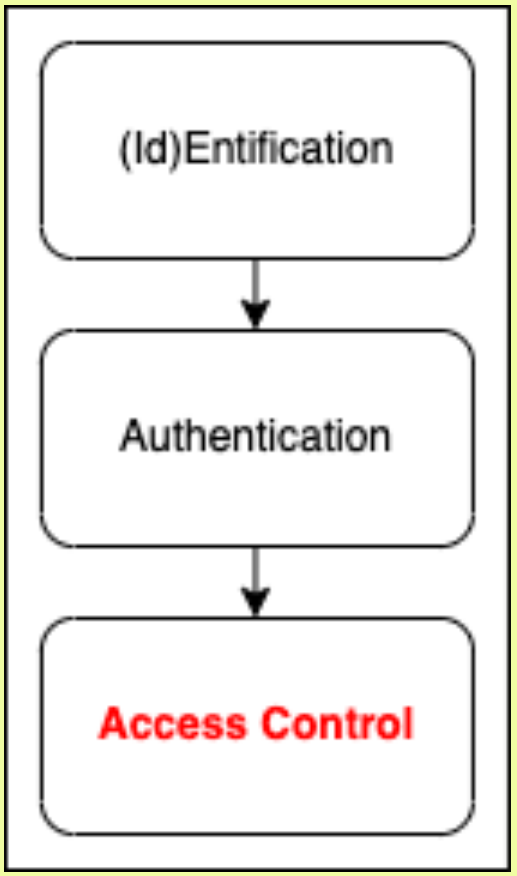
The Registration Phase



- **(Id)Entification**: Make an Assertion that a particular (Id)Entity should be given some kind of 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 an (Id)Entity is to be given in respect of what IS Resources
- **Enrolment**: Record Data to enable the Operational Phase to be conducted in an effective and efficient manner

The Operational Phase

- **(Id)Entification**: Make an Assertion 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 (Id)Entity to exercise the appropriate Permissions



Actor ===>>> IS Resource

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

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

Basic Proposal:

This is a 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

Enhanced Proposal:

This is a 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

Access Control to Resources (= Real-World Things and Events)

- The focus of IS has been on Abstract-World IS Resources
- **But 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 Era of Active Artefacts

Actor ===>>> ~~IS~~ Resource

A Real-World Thing capable of action on a Resource

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

A Real-World Thing

Physical Things

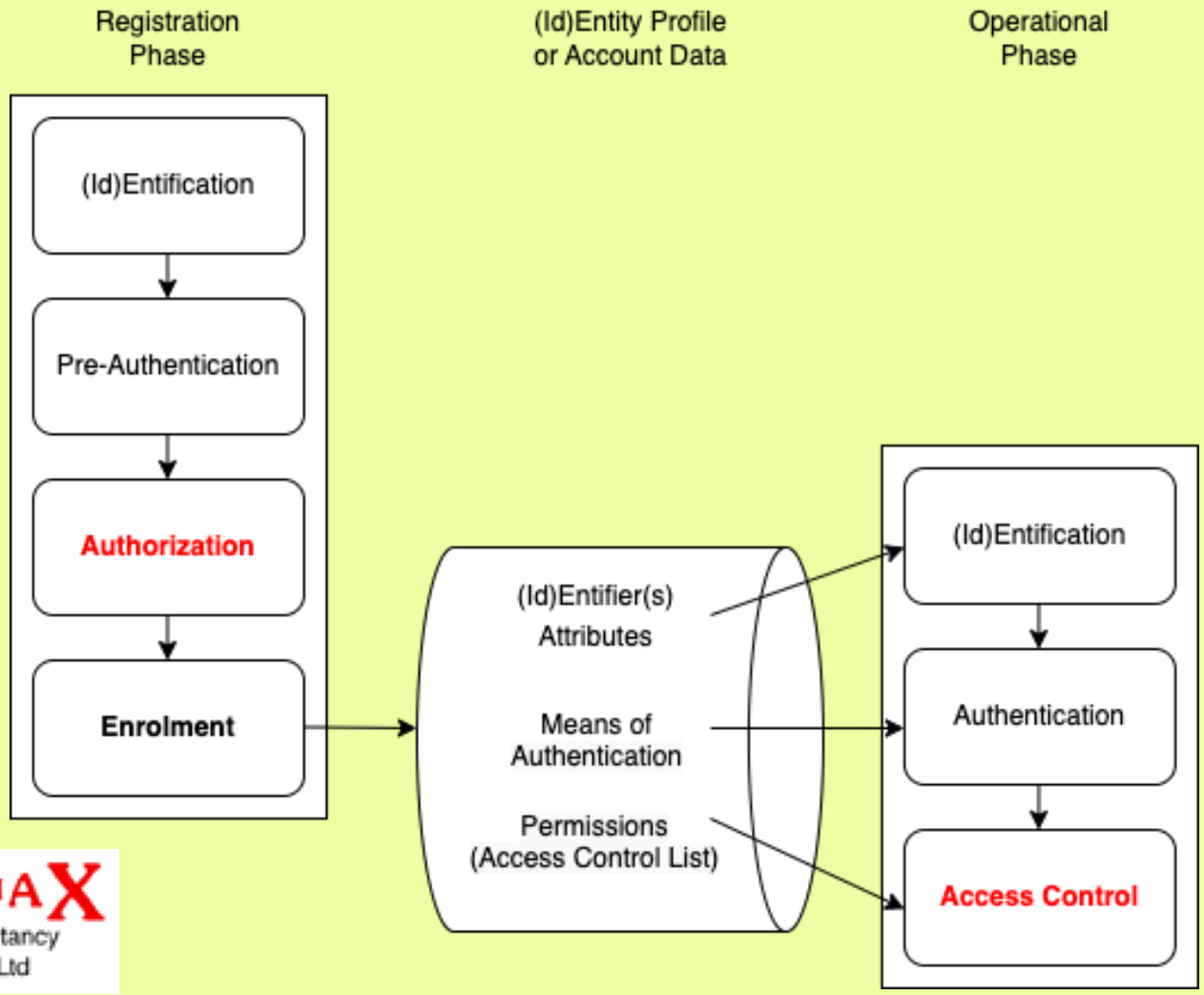
- Humans
- Artefacts

Virtual Things

- Human Identities
- Organisational Identities
- Computer Processes

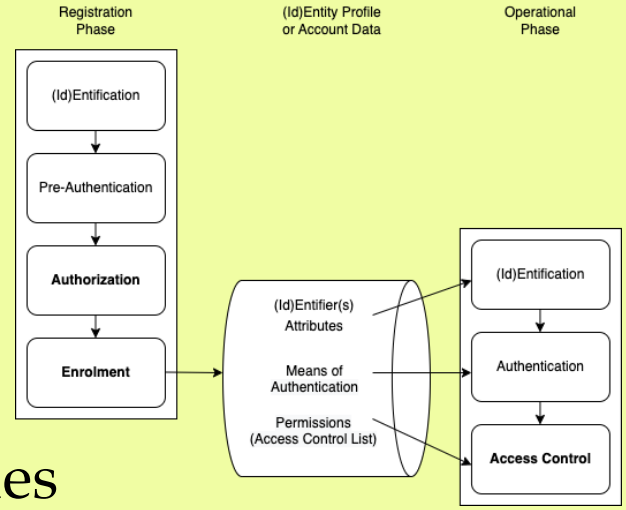
Implications of (Id)Entity Management (IdEM)

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 Practice and Theory



- **Standards** need to be revised to reflect the (Id)EM model
- **Entities are distinct from Identities** (Distinguish Physical and Virtual Things)
- The (Id)EM model defines an **orderly set of phases** and steps, uses **intuitive terms**, provides **coherent definitions**, and identifies relevant data
- 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**
- The model is **readily extended to 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 – 8 December 2023

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