

# The Theory of Identity Management – Extended to the Authentication of Identity Assertions

**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

**36th Bled eConference – 27 June 2023**

<http://rogerclarke.com/ID/IEA-Bled> {[.html](#), [.pdf](#)}

## Context

- Digitalisation's Impacts on 'Digital Economy and Society'
- Ongoing Misconceptions about Identity Management

## Motivation

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

**==>> A Pragmatic Metatheoretic Model**

# A Pragmatic Metatheoretic Model for IS Practice and Practice-Relevant Research

## 'Metatheoretic'

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

## Metatheoretic Assumptions

- Conscious / Unconscious
- Explicit / Undeclared

## Metatheoretic Commitments

## 'Pragmatism'

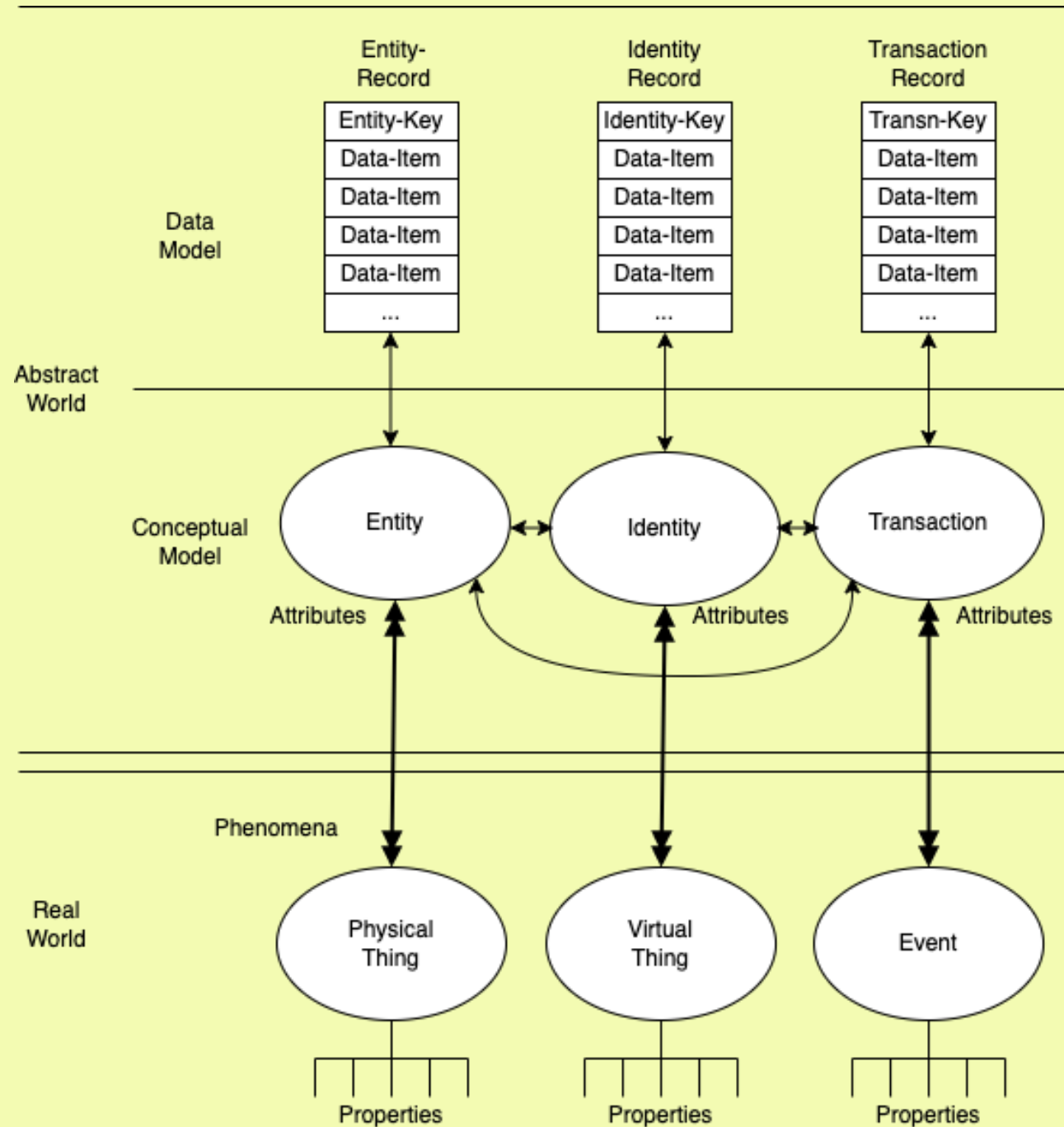
**In philosophy**, 'concerned with understanding and action'  
not just describing and representing

**In IS practice**, approximates  
and articulates 'common sense'

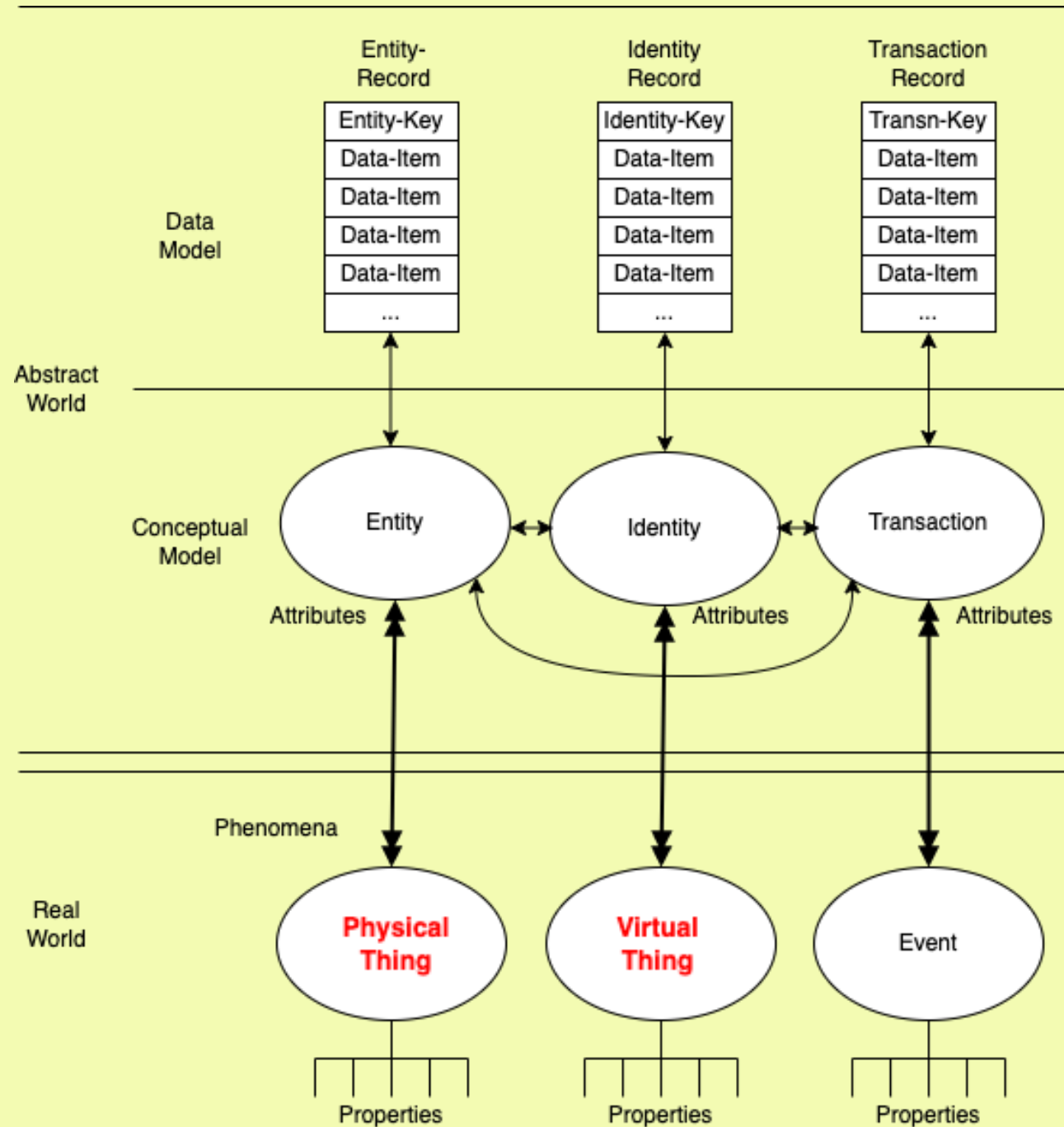
# The Ontological Aspect of the Model

- **The Dualism postulate:**
  - There are material realities (the Real-World)
  - & There is internal 'mind-stuff'  
(spiritual, intellectual or Abstract-Worlds)
- **Real-World Phenomena and Properties**  
The wavelength of electromagnetic radiation,  
hardness and brittleness of things, event-duration
- **Abstract-World Ideas**  
Numbers, colours, hardness, brittleness, time, ...

# Key Elements of the Pragmatic Metatheoretic Model



# Key Differences about the Pragmatic Metatheoretic Model



# Physical Things and Virtual Things

- **Inanimate Objects** (Inventory-Items, Equipment)
  - Containers  $\supset$  Pallet-Loads  $\supset$  Boxes  $\supset$  Cartons

# 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 – **Speed-Check, Convoy-Lead, Get-Away Car, ...**



# 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 – **Speed-Check, Convoy-Lead, Get-Away Car, ...**
- **Organisations** (Companies, Associations, Govt Agencies, ...)

# 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 – **Speed-Check, Convoy-Lead, Get-Away Car, ...**
- **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, ...

# Foundations of Authentication Theory

- *An **Assertion** is an expression of knowledge about one of more elements of the pragmatic metatheoretic model*
- May be made by a party, implied by context, inferred by a party, or postulated by a party. Assertions may be about:
  - Particular Phenomena in the Real World;
  - Particular elements of an Abstract World; or
  - Relationships between Real- and Abstract-World elements
- ***Authentication** is a process that establishes an appropriate degree of confidence in the reliability of an Assertion*
- The terms ~~'Verification'~~ and ~~'Validation'~~ are deprecated, because they assume humanly-accessible truth

# Further Concepts in Authentication Theory

- **Authentication Process**

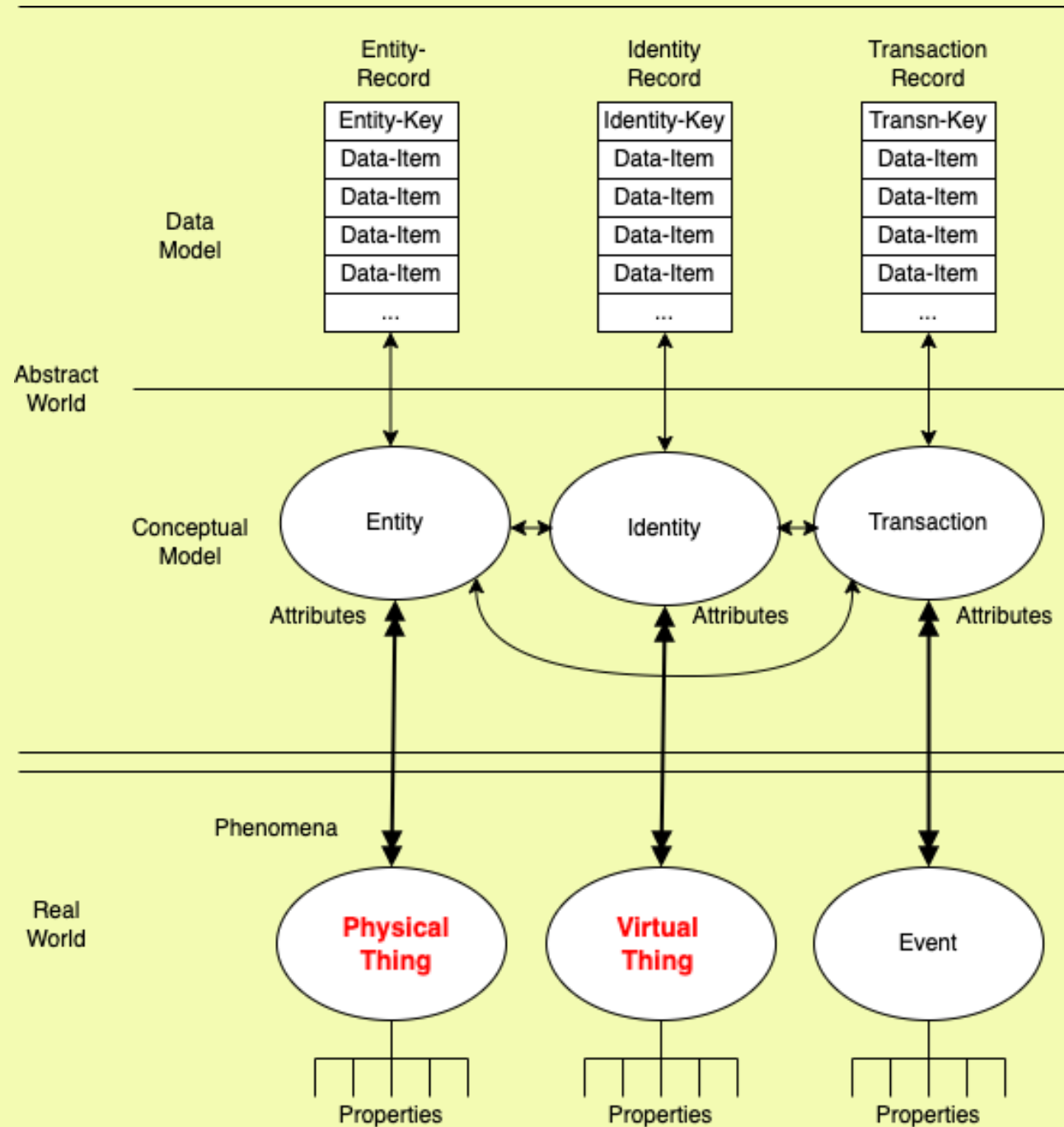
Abstract World:

Check logic and language

Abstract-to-Real World:

Observe / measure, compare

# Key Differences about the Pragmatic Metatheoretic Model



# Further Concepts in Authentication Theory

- **Authentication Process**

Abstract World: Check logic and language

Abstract-to-Real World: Observe / measure, compare

- **Evidence**

Data that assists in an Authentication Process

- **Authenticator**

An item of Evidence, e.g. a document (in any medium)

- **Credential**

An Authenticator with the imprimatur of an authority

- **Token**

A recording medium on which useful data is stored  
e.g. (Id)Entifiers, Attributes, Authenticators, Credentials

# Authentication Quality Management

- Checks of the Authentication Process
- Checks of the Evidence used in the Process
- Effort proportional to the likelihood of error, and the harm arising from False Positives (Assertions wrongly accepted) and False Negatives (Assertions wrongly rejected)
- Care with:
  - Means for contesting or repudiating assertions
  - Which party bears the onus of proof
  - Which party bears the risks, costs and inconvenience

# The Authentication of Assertions Relating to (Id)Entity

- 1) Identity Assertion
- 2) Entity Assertion
- 3) Simple Property Assertion
- 4) Complex Property Assertion
- 5) Principal-Agent Assertion
- 6) (Id)Entity Match Assertion



## (1) Identity Assertion

- *A particular Virtual Thing is appropriately associated with one or more Identity-Records*

'This client's profile information is displayed on the screen in front of me'

- *The Data-Item-Values in a particular Identity-Record are appropriately associated with a particular Virtual Thing*

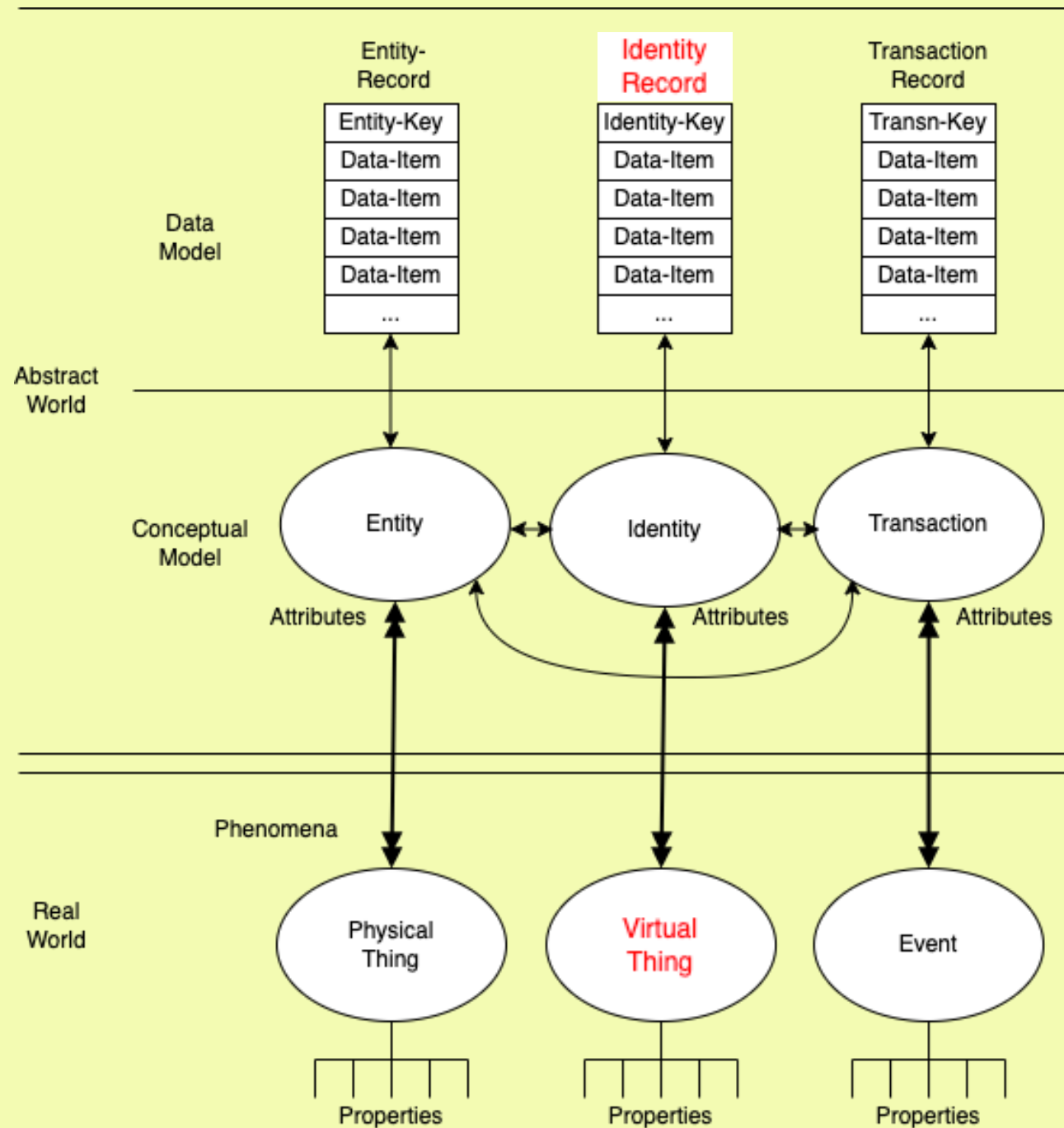
'This data on my screen relates to this software-agent'

- *This Virtual Thing is the Virtual Thing with which this particular Identity-Record is appropriately associated*

'This corporation is the corporation we're doing business with'

'This patient is the one to whom this medical record relates'

*A particular **Thing** is appropriately associated with one or more **(Id)Entity-Records***



### (3) Simple Property Assertion

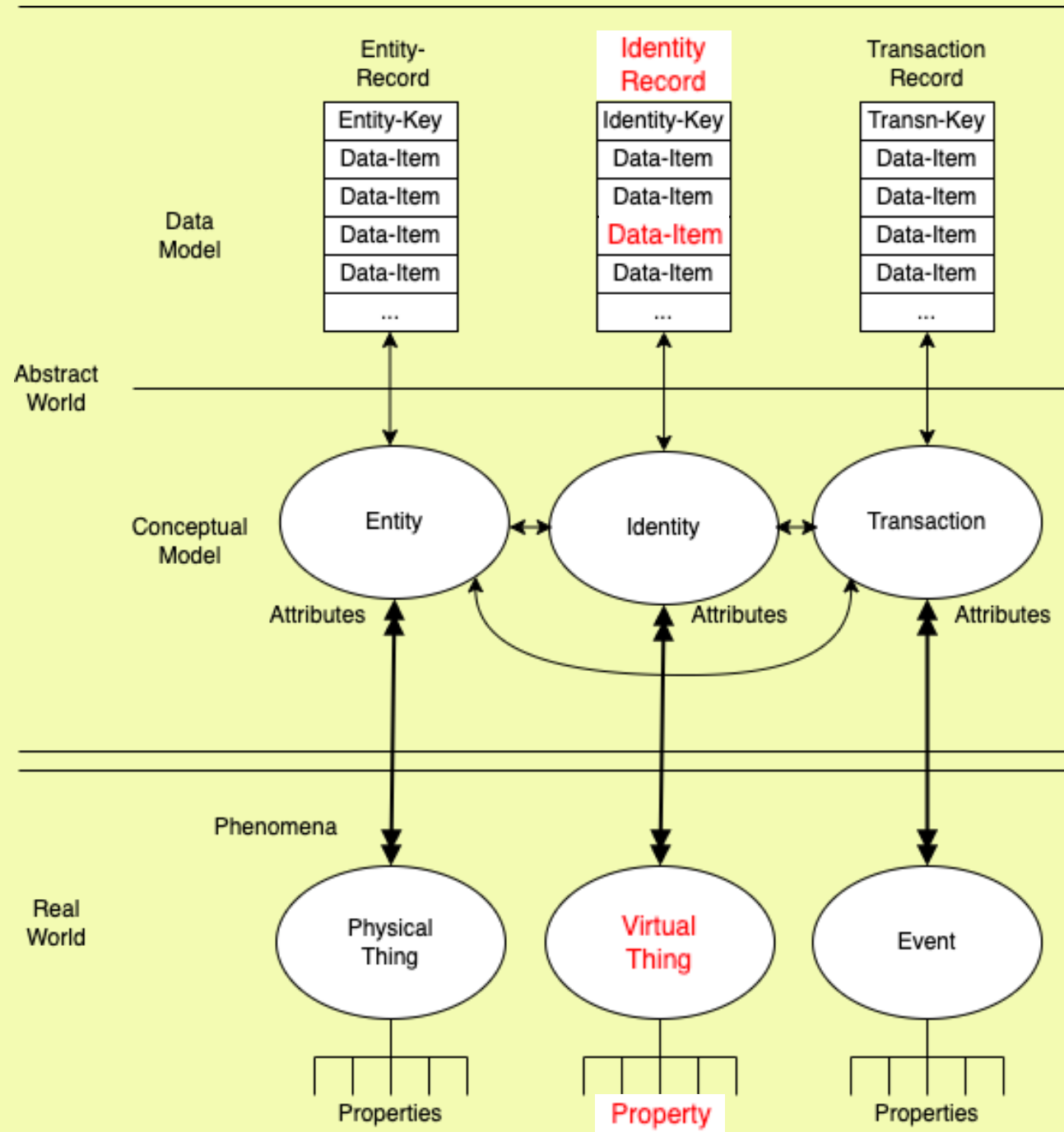
- *A particular Data-Item-Value in a particular (Id)Entity Record is appropriately associated with, and reliably represents, a particular Property of a particular Thing*

'This person is old enough to enter the night club'

'This customer is a frequent-buyer who qualifies for the loyalty discount'

'There are 13 widgets in stock because the inventory system says there are'

*A particular **Data-Item-Value** in a particular (Id)Entity Record is appropriately associated with, and reliably represents, a particular **Property** of a particular Thing*



## (4) Complex Property Assertion

- *A particular Thing is inferred to have a particular Property, on the basis of multiple particular Data-Item-Values in one or more particular (Id)Entity Records, and on the assumption that those Data-Item-Values are appropriately associated with that Thing and reliably represent that Property*

'This borrower is behind on their loan repayments'

'This welfare recipient has been overpaid because they understated their income'

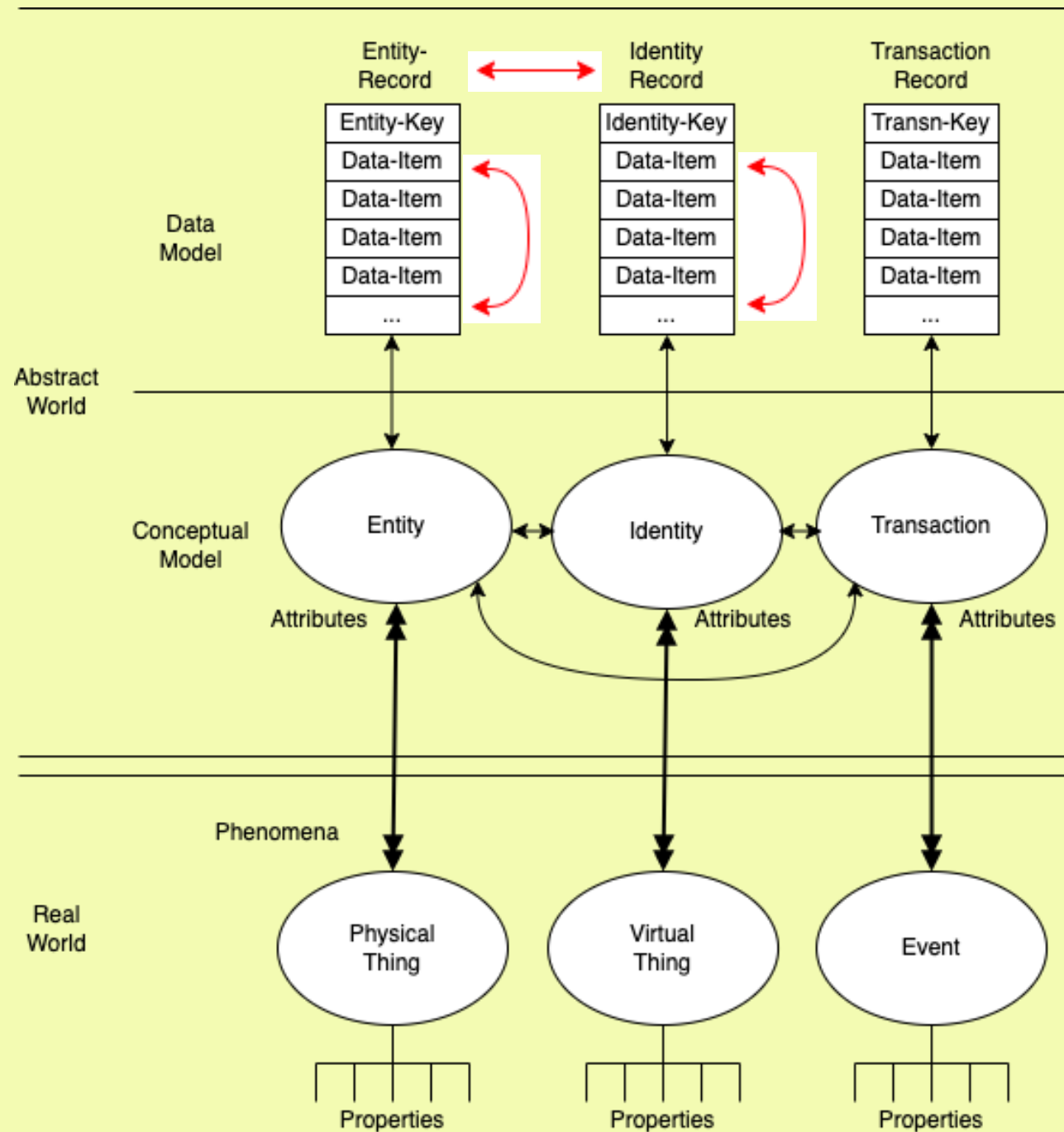
## (5) Principal-Agent Assertion

- *A particular Thing has a particular Property, based on one or more particular Data-Item-Values in one or more particular (Id)Entity Records, which are appropriately associated with that Thing and which reliably convey that the particular Thing has the authority to act on behalf of another particular Thing*  
*'This human / legal-person / software-agent is the approved representative of this customer / client / accusee'*

## (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*

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





# Threats to Authentication Process Quality

- **Accidental Errors**
- **Intentional Errors:**
  - **Intentional False Positives**  
e.g. masquerade or 'spoofing'  
to enable a person or process to exercise a power that should be exercised by some other (Id)Entity
  - **Intentional False Negatives**  
e.g. avoidance, undermining or subversion of (Id)Entification to avoid accountability

# 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)

# Evidence to Support the Authentication Process

## Property Assertions (3)-(6)

- **Rely on Data already held**
  - 'Trade Customer', 'Old-Age Pensioner', ...
- **Apply logical processes to Data already held**
  - A claim of being owed a refund for a failed delivery
  - A claim to having reached a particular age or period of association with an organisation
- **Rely on new Data checked against another source**
  - A claim of an educational or skills qualification against a testamur, or a database listing graduates

# 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

# The Authentication of Identity Assertions

## Agenda

- Motivation
- A Pragmatic Metatheoretic Model to support IS practice and relevant research
- The Theory of Assertion Authentication
- Assertions Relating to (Id)Entity
- Authentication Processes
- Implications

# The Theory of (Id)Entity Management – Extended to the Authentication of (Id)Entity Assertions

**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

**36th Bled eConference – 27 June 2023**

<http://rogerclarke.com/ID/IEA-Bled> {[.html](#), [.pdf](#)}