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

ROGER CLARKE

Xamax Consultancy Pty Ltd, Canberra, UNSW Law, Sydney;
Australian National University School of Computing, Canberra, Australia
Roger.Clarke@xamax.com.au

At the 35th Bled eConference, a previously-published pragmatic metatheoretic model was articulated in the context of identity management. The present paper extends that theory to the authentication of the various categories of assertions that arise in identity management activities. The extended theory reflects the important distinction between the concepts of identity and entity. It deals with the fundamental categories, in which a particular data-record is claimed to relate to a particular physical entity or virtual identity; but it also encompasses claims about the properties of real-world things, and assertions that records in two different data-sets apply to the same (id)entity. The analysis has important implications for the practice of IS, and for IS researchers whose work is intended to influence IS practice.

Keywords:
IS practice,
assertion,
evidence,
property,
principal-agent

University of Maribor Press

DOI https://doi.org/10.18690/um.fov.6.2023.40
ISBN 978-961-286-804-8

1 Introduction

Organisations have encountered ongoing difficulties in the areas of identification and authentication, particularly where the entities in question are human beings. The topic of identity authentication is addressed in the technical information technology (IT) literature, although far less so in information systems (IS). On the other hand, authentication as a general concept and a family of business processes has attracted remarkably little attention. For example, of the 465 refereed papers from the Bled eConference accessible in the AIS electronic Library (AISeL), covering the last two decades, only 2 have the term 'authentication' in Title or Abstract. In AISeL as a whole, the corresponding count is only 38 of >17,000, and across the Basket of 8 IS journals, a mere 12 of >10,000 articles. Effective IS depend on a deep appreciation by IS designers of the nature of the relevant phenomena, and hence researchers need to pay far more attention to the topic.

IS professionals need to be supported by a model that is pragmatic, by which is meant that it is a fit to the needs of IS practitioners, but that also reflects insights from relevant aspects of philosophy. This paper builds on prior work in two areas. The first presents a pragmatic metatheoretic model to support IS, and the second examines the general concept of authentication. Together, these provide a suitable basis for an analysis of processes to authenticate assertions about identity.

The paper commences with a recapitulation of prior work that establishes the pragmatic metatheoretic model, and explains the generic concept of assertion authentication. The main body of the paper identifies and discusses specific categories of assertion in which identities and/or entities play a key role. Processes are then presented whereby the reliability of those kinds of assertions can be assessed. The effectiveness of those processes is shown to be dependent on evidence, and hence on the quality of the data on which reliance is placed. The application of these ideas to IS practice is argued to enable improvements in authentication design and operation. The need is shown for further work on their application to particular kinds of entities and identities and in particular contexts.

2 Prior Work

Organised activity involves dependence by parties on statements made by other parties. The longstanding maxim 'Trust, but verify' conveys that, in principle, all such statements on which dependence is placed need to be checked, but with effort invested proportionately to the harm that would arise from unjustified trust. Organisations need IS to be designed in a manner that reflects, supports and facilitates the checking of important statements. For that to be achieved, the model on which IS practice is founded needs to have an effective fit with the manner in which business enterprises, government agencies, not-for-profits and small businesses perceive the realities of their operational environment.

The first sub-section below summarises a model that is pragmatic, in that it supports understanding about and action in the world, yet has a firm foundation in relevant aspects of meta-theory, particularly ontology (the study of existence), epistemology (the study of knowledge), and axiology (the study of values). The second sub-section introduces a further area of prior work which examines the general notion of authentication. On these two foundations, the remainder of the paper builds an analysis of the authentication of assertions that involve identities and entities.

2.1 The Pragmatic Metatheoretic Model

Prior work reported at the Australasian Conference in Information Systems (ACIS) in Clarke (2021) presents a pragmatic metatheoretic model conceived in order to support both IS practice and that portion of IS research activity that is intended to be relevant to IS practice.

The foundational metatheoretic aspect is ontology, which is concerned with phenomena, and hence with the properties of things and events. The assumption adopted in the model is a conventional compromise between materialist and idealist notions, postulating that there are both material realities (the Real World) and internal mind-stuff (as that term is used by William Kingdon Clifford to refer to the intellectual or Abstract World – Coneybeare 1892): phenomena and their properties inhabit the Real World; whereas ideas are of the Abstract World.

The second aspect, epistemology, is the study of knowledge, and its sources, varieties and limits. Competing views are empiricism, which holds that knowledge is derived from sensory experience, and apriorism or rationalism, which considers that knowledge is or at least can be innate and/or derived from the human faculty of reason.

A pragmatic metatheoretic approach must support IS practitioners not only in contexts that are simple, stable and uncontroversial, but also where there is no expressible, singular, uncontested 'truth'. Some relatively closed systems, such as fly-by-wire, industrial control, and robotic assembly line management, can reasonably be treated as technical systems. In the large majority of IS, on the other hand, interaction among IT artefacts and people is intrinsic, and meaningful study of them requires the adoption of both a socio-technical perspective (Abbas & Michael 2022), and interpretivist or critical theory approaches to research. The epistemological commitment underlying the model is accordingly that knowledge depends on appropriately blending sensory experience, human imagination, and reasoning, and accommodating both tacit and codified knowledge.

A third important branch of philosophy, axiology, is less familiar. It is concerned with how value is imputed to things. Organised activities depend on people, artefacts, and effective interactions among them. IS also affect people, including those participating in the system (conventionally called 'users') and some who are not participants in the system, but are affected by it (usefully referred to as 'usees' – Berleur & Drumm 1991 p.388, Clarke 1992, Fischer-Huebner & Lindskog 2001, Baumer 2015). Examples of usees include people to whom records in shared industry databases refer, such as those for police suspects and tenants. Human values are accordingly central to the model.

In addition, IS involve various stakeholders, and value-conflicts are inherent. The approach adopted in the pragmatic metatheoretic model is that value is dependent on the observer, that there are generally multiple observers of any given phenomenon, and hence that IS must support the integration of multiple perspectives rather than assume that one necessarily dominates (Clarke & Davison 2020), and must continue to function where tension continues among two or more perspectives.

At the Bled eConference, in Clarke (2022), the pragmatic model was applied to identity management. A diagrammatic form of the full model is in Figure 1. The Properties of phenomena in the Real World can be sensed by humans and artefacts with varying reliability. Within the Abstract World, two levels are then distinguished. At the Conceptual-Model level, the Real-World phenomena are conceptualised by people, in many cases on behalf of organisations. In the remainder of this paper, capitalised terms are defined in the text, with the full set of definitions gathered into a Glossary, provided as Supplementary Material.

At the Data-Model level, the concepts are operationalised, enabling the Data-Items to represent the states of Properties of phenomena, in a manner that enables coherent collection, processing, management and use of the Data. At the Conceptual-Model level, Real-World Things and Events are represented as (Id)Entities and Transactions, and their Properties as Attibutes. Relationships exist among the various elements. These aspects of the model provide a useful formalisation of the way in which IS practitioners view the relevant parts of the surrounding world and the representations of that world expressed in their systems.

The compound and intentionally attention-attracting term (Id)Entity is used to refer to elements of the Conceptual Model that represent Real-World Things. An Entity corresponds with a Real-World Physical Thing, and an Identity with a Real-World Virtual Thing. Virtual Things lack the corporeal nature of a Physical Thing, but are treated as being real because they perform functions relevant to IS. Virtual Things include processes running inside computing devices, and human presentations or roles. For example, the role of CEO is an Identity that is usually performed by a single human Entity at any give time; but it is performed by different human Entities over time.

Virtual Things may have associations with Physical Things, e.g. a computer process with a computing device, a software-agent with a human principal, and a role with one or more humans. Some Physical Things have associations with multiple Virtual Things, and vice versa, and most associations are time-bounded.

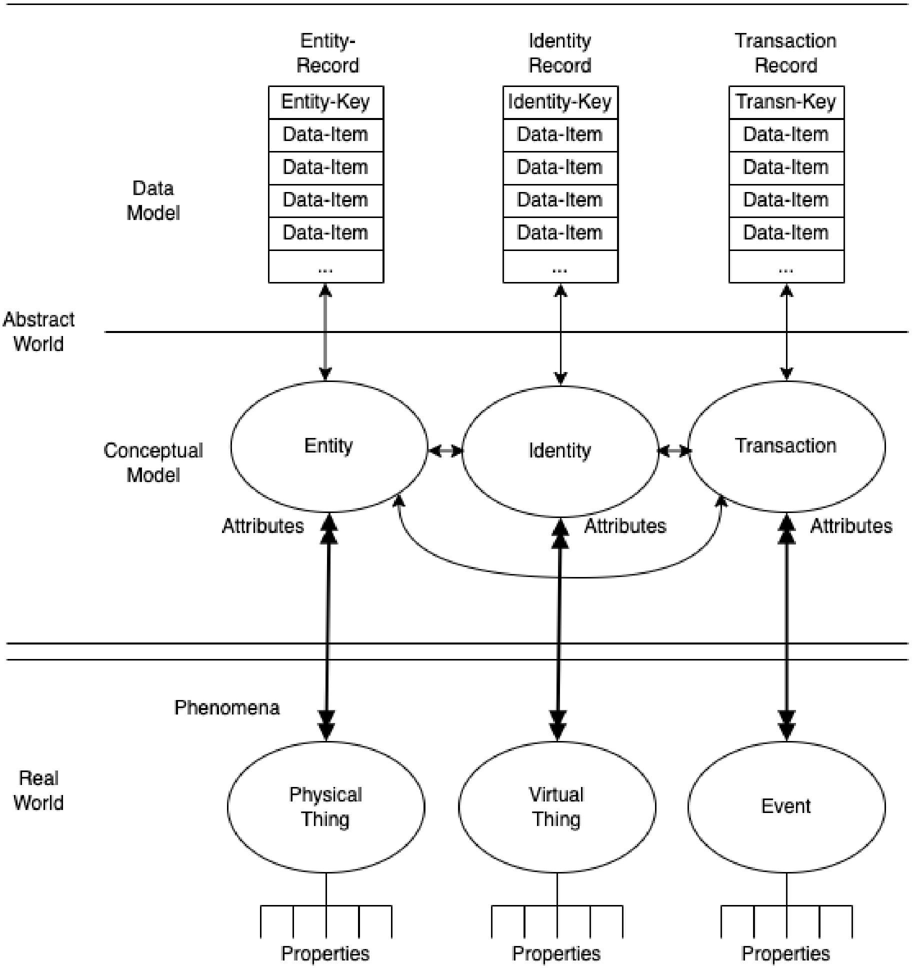

Figure 1: The Pragmatic Metatheoretic Model

Each element at the Conceptual Level has 'Attributes', which contain an 'Attribute-Value' for each instance. For example, the Entity shipping-containers has Attributes such as colour, owner and type (with Attribute-Values fot type such as refrigerated and half-height). A Relationship has the Attribute of cardinality, reflecting how many of each of the elements that it links can exist – typically zero, one or many.

At the operational, Data-Model level, a Data-Item is a storage-location in which a discrete 'Data-Item-Value' can be represented. For example, Entity-Attributes of cargo-containers may be expressed at the Data Model level as Data-Items and Data-

Item-Values of Colour = Orange, Owner = MSK (indicating Danish shipping-line Maersk), Type = Half-Height. A set of Data-Items that relate to the same (Id)Entity or Transaction make up a Record. Record-Keys are Data-Items or Data-Item groups that are capable of distinguishing which (Id)Entity-Instance a particular Record relates to. Record-Keys for Identities are called Identifiers, and Record-Keys for Entities are Entifiers.

Identification refers to the process whereby a Data-Record is associated with a particular Virtual Thing. It involves the acquisition of a Record-Key, that is to say an Identifier. The corresponding process is Entification, whereby a Data-Record is associated with a particular Physical Thing, involving the acquisition of an Entifier. Some computing devices, being a Physical Thing, have a unique number stored internally which can be reliably used as an Entifier; whereas each of the processes running within a device and communicating with remote devices is a Virtual Thing, for which a workable Identifer is the combination of IP-Address and Port-Number. For human beings, a customer-code is an Identifier, and a biometric is an Entifier.

The (Id)Entity and (Id)Entification distinctions were first proposed in 2001, and have been applied in about 25 articles within the Google Scholar catchment, which together have over 400 citations. However, despite the concept's importance, it has to date attracted far too little attention. This aspect of the pragmatic metatheoretic model represents a major contribution to practice and theory.

The basic features of the model can deal with passive Things, including natural objects (such as gems and dinosaur bones), animals, and artefacts (such as *objets d'art*, pallets, and stock-items). Further articulation is needed when dealing with active Things, including artefacts capable of action in the Real World (such as computing devices and robots), and human beings. The notion of identities of human entities, foundational to the discussion, has been treated elsewhere at length, both generally (e.g. Brown 2020) and specifically within IS (e.g. Clarke 1994b, Halperin & Backhouse 2008, Clarke 2008). In IS that extend beyond data-processing, to information production, to inferencing, to decision-making and even to action, values loom large, conflicts among value-sets occur, and designers must take much greater care.

2.2 Authentication Theory

The pragmatic metatheoretic model outlined in the previous section postulates a Real World comprising Things and Events, which have Properties. These can be sensed by humans and artefacts with varying reliability. Authentication is a process whereby that reliability can be assessed. This paper's purpose is to present an analysis of Authentication in contexts in which Identity or Entity plays a central role. No sufficiently general body of theory has been located in the IS or any other literature. As a basis for the analysis, this sub-section accordingly summarises prior work by the author on the generic notion of Authentication (Clarke 2023).

Dictionary definitions of 'assertion' refer to declarations or affirmations, and to the action of making such statements. In the present context:

> *An* ***Assertion*** *is an expression of knowledge about one of more elements of the pragmatic metatheoretic model.*

An Assertion may be made by a party, implied by context, inferred by a party, or postulated by a party. Assertions may be about:

1. Particular Phenomena in the Real World;
2. Particular elements of an Abstract World; or
3. Relationships between elements in both the Abstract and Real Worlds.

It is common in the IT industry for the process of establishing the reliability of an Assertion to be referred to as 'Verification', or sometimes 'Validation'. It is preferable to avoid those terms in favour of one that is consistent with the pragmatic model's recognition of the impracticality of the notion of humanly-accessible truth, and that interprets reliability in constructively loose terms:

> ***Authentication*** *is a process that establishes an appropriate degree of confidence in the reliability of an Assertion.*

In designing Authentication processes, organisations generally select a trade-off among key factors such as cost, reliability, and convenience for, and acceptability to, affected parties. This inevitably results in shortfalls in the quality of the

Authentication process. The term 'appropriate' has been included in the working definition above, to reflect the fact that the degree of confidence is compromised by, or balanced against, other factors.

Assertions in category (1) above, relating solely to the Real World, may be authenticated by empirical means, that is to say by observation of the Phenomena. Assertions in category (2), on the other hand, relate solely to the Abstract World. They may be authenticated against Data available in the Abstract World. Authentication processes for such Assertions may involve the application of reasoning, in order to infer additional Assertions.

Classical logic, such as the propositional calculus, is of limited use, because it only supports binary / true-or-false assertions. More useful logics support qualitative data on nominal and ordinal scales, and preferably on ordinal scales (such as the non-linear Richter scale for the intensity of earthquakes), interval scales (with equal distances between consecutive values, cf. Celsius for temperature), and most powerfully on ratio scales featuring a natural zero (cf. Kelvin for temperature – Stevens 1946).

Nomatter what approach is adopted, however, Authentication of Abstract-World Assertions cannot, alone, satisfy the criterion of 'establishing an appropriate degree of confidence', because it does nothing to test the relationship between Data and the Real World. The primary focus of Authentication processes needs to be on Assertions in category (3), straddling the two Worlds.

Authentication processes depend on evidence, for which dictionary definitions refer to observations adduced in support of a conclusion or statement. In the present context:

> ***Evidence*** *is Data that assists in determining the level of confidence in the reliability of an Assertion.*

An individual item of Evidence is usefully referred to as an Authenticator. A common form of Authenticator is a Document, in any form and expressed in any medium. Some Authenticators carry the imprimatur of an authority, such as a registrar or notary, and are referred to as Credentials. The term Token refers to a recording medium on which useful Data is stored, in the present context (Id)Entifiers, Authenticators and/or Credentials.

The preliminary sections of this paper have drawn on prior work to define a pragmatic metatheoretic model to support IS practice and practice-relevant research, and to establish basic theory in relation to Assertions and their Authentication. The following section applies those ideas to the specific context of assertions in which Entities and Identities figure prominently.

3 Assertions Relating to (Id)Entity

This section applies the theory of Authentication outlined above to Assertions that involve Entities or Identities. The first sub-section identifies the kinds of Assertion that are relevant. The later sub-sections discuss the process whereby such Assertions can be authenticated, and the nature of the Evidence that can be used in that process.

3.1 Introduction

The pragmatic metatheoretic model avoids the idea that an accessible truth exists, and articulates the relativistic notion of a degree of confidence in the reliability of Assertions. Reflecting this, a key term in the category descriptions below is defined as follows:

> ***Appropriately*** *means with a level of confidence commensurate with the reliance placed on the Assertion and the severity of the consequences if the reliance is misplaced*

This sub-section identifies a set of Assertion categories. Almost all of the IS and related literature on Authentication is concerned with a limited mainstream mode of thought in which the focus is on what are referred to here as (Id)Entity Assertions – categories (1) and (2) below.

(1) An Identity Assertion

An assertion of a relationship between a Virtual Thing and a Record takes one of the following forms:

- 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'

Expression of such Assertions is facilitated by the industry standard Security Assertion Markup Language (SAML), which includes an assertion-type called an 'authentication statement', which asserts that 'a particular remote Virtual Thing is appropriately associated with a particular Identity' (OASIS 2005).

(2) An Entity Assertion

An Assertion of a relationship between a Physical Thing and a Record takes one of the following forms:

- A particular Physical Thing is appropriately associated with one or more Entity-Records
  'This felon's profile information is displayed on the screen in front of me'
- The Data-Item-Values in a particular Entity-Record are appropriately associated with a particular Physical Thing
  'The data displayed on my screen relates to this particular stock-item'
- This Physical Thing is the Physical Thing with which this particular Entity-Record is appropriately associated
  'This is the shipping-container we were looking for'

'This person is Wanted Person No.1'

A contention of this paper is that a serious deficiency exists in the existing literature in the form of the conflation of Entity and Identity Assertions and their Authentication. An important example is the statement within the IT industry, frequently adopted in the research literature, that Authentication is based on 'what you know, what you have, and what you are'. See, for example, Elgarah & Falaleeva (2005), Witman (2006), Carpenter et al. (2008) and Hewitt (2009). The third category ('what you are') differs fundamentally from the other two.

A recent UNHCR plan reported on by Madon & Schoemaker (2021) calls for "a self-managed digital wallet [that] would allow refugees to store a variety of different forms of *identification* such as biometric registration, individual ID documentation, attestation card and already-existing authenticated paper documents that have been digitised and uploaded" (p.938, emphasis added). Authenticators for Identity Assertions (such as 'I have this Accredited Refugee Code') are combined into a single Token along with a biometric Authenticator for an Entity Assertion ('I am s/he'). Biometrics strikes through a person's multiple Identities to the Entity. Physical and Virtual Things differ enormously, as do the contexts, the impacts on values, and hence the design processes and the ethicality and public acceptability of those designs. It is therefore very important to distinguish between the two Assertion categories.

(3) A Simple Property Assertion

Assertion categories (3)-(5) are concerned with Properties. The descriptions here use the abbreviated form (Id)Entity to encompass both sub-categories. A straightforward Assertion takes the following form:

- 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'

This category of assertion is at an atomic level and of high granularity, and relates to a Property that is represented by a single Data-Item. More complex circumstances are the subject of the following category. The UNHCR plan discussed by Madon & Schoemaker (2021) includes in the envisaged "self-managed digital wallet [for] refugees" the inclusion of "education credentials" (p.938). The Token would therefore assist with the Authentication of Property Assertions (e.g. 'I have a High School Certificate from ...').

A Property Assertion is frequently assumed to be dependent on an accompanying (Id)Entity Assertion; but, subject to some conditions, it is feasible to perform Property Assertion Authentication without (Id)Entity, and may be far preferable to do so (e.g. for cost, confidentiality or privacy reasons).

To facilitate expression of Property Assertions, the industry standard SAML includes an assertion-type called an 'attribute statement', which asserts that a particular remote Virtual Thing has a particular Property (OASIS 2005).

(4) A Complex Property Assertion

A more complex assertion depends on an inference drawn from multiple Data-Items, and takes the following form:

- 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'

Reliance on Property Assertions needs to be based on careful analysis, because each Assertion's reliability depends on data quality, and because of the wide array of quality factors that need to be satisfied to ensure that the level of confidence in the Assertion is appropriate – defined above as meaning 'commensurate with the reliance placed on the assertion and the severity of the consequences if the reliance is misplaced'.

Kambil & van Heck (1998) describe Authentication as one of the five 'Basic Trade Processes' in Online Auctions, used "to verify [1] the quality and [2] features of the product offered [both of which are Complex Property Assertions], [and] [3] the authenticity of the trading parties [a combination of Identity and Attribute Assertions] ..." (p.5). This was revisited in Fairchild et al. (2007), who argued that Authentication is "central to the design of multi-attribute markets [with the market operator performing] extensive pre-qualification of suppliers by intermediary to ensure the integrity of the auction process" (pp.291-292, involving both Identity Assertions and Complex Attribute Assertions).

However, where this category is evident in the IS literature, there is often a lack of clarity as to what the Assertion is, or Assertions are, whose reliability is being investigated. One example of simple mis-phrasing is "He pays for this transaction online using BankID to authenticate his payment" (Eaton et al. 2014), when what is meant is 'He authenticates himself to his bank as a person authorised to operate on that account', i.e. it is an Identity not a Value Assertion. Another is the expression 'authenticity of Internet-sourced information' (e.g. Haider 2008), which conflates source (an Identity Assertion) and content (a Fact Assertion).

(5) A Principal-Agent Assertion

A special case of a complex Property Assertion is of considerable commercial significance, and hence is dealt with here as a separate category. An Assertion relating one Thing's ability to act on behalf of another Thing takes the following form:

- 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'

This Assertion-category involves a chain of Virtual and Physical Things, and hence requires multiple Authentication processes to be performed: "The claims of a business intermediary to be acting on behalf of another intermediary need to be subjected to testing. Moreover, the claims of a person to be acting on behalf of a business entity (which may itself be acting as an intermediary for another business entity) also need to be tested. Authentication needs to be undertaken of a particular attribute or credential that reflects the agency relationship, such as a power of attorney, or some other form of delegation of power to sign contracts" (Clarke 1999, p.9). A comprehensive study of Principal-Agent Authentication is in Basul & Muylle (2001).

(6) (Id)Entity Match Assertions

A further cluster of Assertion Categories are entirely within the Abstract World. Authentication of these categories is not merely valuable, but actually essential to the conduct of IS. They differ from the earlier categories, however, in that Authentication of these Assertions alone, while contributing to the level of confidence, does not satisfy all of the necessary conditions, and hence complementary Assertion Authentication processes are needed, to reliably link these Assertions within the Abstract World with Things in the Real World.

Match Assertions take one of the following forms:

- *This Identity-Record is appropriately associated with this other Identity-Record*
  Within a particular insurance company: 'This record in the Motor Vehicle Insurance database matches to this record in the Home & Contents database'
  In a government context, and subject to legal authority: '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'
  Subject to legal authority: 'This DNA sample data from { a crime-scene, a crash-site } is from the same person as is represented by this DNA sample data from a particular family history database'

- *This Identity-Record is appropriately associated with this Entity-Record*
  'This process is running in this computing device'
  In a law enforcement context: 'The record containing this client-number corresponds to this fingerprint-based criminal record'

The contexts in which matching of human Entities is undertaken often have potentially very serious consequences for the person concerned. This calls for a very high degree of confidence in the reliability of the Assertion.

3.2 The Authentication Process

Assertions are depended upon as a basis for inferencing, decision and action. They need to be authenticated, to protect against risks of error and fraud. Sources of poor quality include:

- Accidental mistakes; and
- Intentional mistakes, including:
- intentional false positives, e.g. masquerade or 'spoofing' to enable a person or process to exercise a power that should only be exercised by some other (Id)Entity; and
- intentional false negatives, e.g. avoidance, undermining or subversion of (Id)Entification.

Few sources have been located that identify criteria for evaluating the quality of Authentication processes. Zviran & Erlich (2006) identify as relevant factors: effectiveness, ease of implementation, ease of use, and user attitude and acceptance. Way & Yuan (2009) provide a more substantial list, comprising Accuracy, Robustness, User Acceptance, Accessibility, Feasibility, Applicability, Responsiveness, Non-reputability [sic: Non-Refutability] and Maintainability. Those authors also note different priorities for the criteria among stakeholders, which they categorise as Management, IT Support and Users. Both are useful contributions, but are mostly technical in their orientation. Most IS require a socio-technical approach, and hence additional considerations need to be factored in, such as transparency (from user and usee perspectives) and costs and risks (from the viewpoint not only of the system sponsor, but also of users and usees).

Quality is a substantially greater challenge where other parties are motivated to achieve false positives or false negatives. Safeguards are needed to limit the extent to which such parties may succeed in undermining authentication quality. Techniques such as channel encryption (in particular SSL/TLS) and one-time password schemes are applied to these purposes. Each safeguard has vulnerabilities, and is subject to threats. It is common to distinguish multiple quality-levels or 'strengths' of Authentication, such as unauthenticated, weakly authenticated, moderately authenticated and strongly authenticated. Business enterprises and most government agencies generally adopt risk-managed approaches, accepting lower levels of assurance in return for processes that are less expensive, more practical, easier to implement and use, and less intrusive.

3.3 Evidence in Support of the Authentication Process

In section 2.2, the concepts of Authenticators, Credentials and Tokens were introduced. These notions are much applied in the Authentication of Assertions involving (Id)Entity. The central form of such Assertions is category (1), an Identity Assertion, of the form:

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

Each such association is achieved by means of an Identifier. The conventional term used in government circles for Authenticators designed to support Authentication of such Assertions is 'Proof of Identity' (PoI). This is a disingenuous term, implying infallibility of the Authenticator and the Authentication process that uses it. The notion of accessible truth in such complex circumstances lacks credibility. The appropriate term is accordingly Evidence of Identity (EoI).

Several different categories of Authenticator are used as EoI. The notions of 'what you know' (i.e. Data of some kind) and 'what you have' (a Credential or a Token containing one) are useful summaries. A reasonable degree of confidence in an Assertion of Identity can only be achieved, however, if:

- A Virtual Thing appropriately associated with that Identity can be relied upon to have access to suitable Evidence, to be willing to provide that Evidence, and to do so; and
- The party performing the Authentication (or the technology on which that party depends) has access to a copy of relevant Data, or some other means of being satisfied that the proffered Evidence supports the Assertion and is trustworthy.

Common examples of knowledge-based EoI are passwords and PINs. Further instantiations are private keys generated by (or sometimes issued to) individuals' own devices (workstations, mobile phones, tablets, smartcards, etc.), and one-time passwords, whether generated by a separate device issued to the relevant individual, or communicated to them at the appropriate time over a separate and secure transmission channel. Tokens are usefully applied to the storage of human-visible and/or machine-readable copies of (Id)Entifiers. The same Token may also be used as EoI, by containing one or more Authenticators, which may be Credentials. Forms of Tokens include sequentially-numbered tickets issued to people required to wait in a queue; a credit-card-sized plastic card carrying a chip, sometimes called a smartcard; machine-readable visual images (such as bar-codes and QR-codes); and machine-readable data-storage (such as a magnetic-stripe, solid-state memory in such artefacts as a thumbdrive or 'USB key', and transmissions from an RFID-tag).

In some circumstances, the provision of an Identifier may represent EoI. For example, if a Token is used, and not even the artefact or the individual is aware of the Data-Value that is their Identifier, but the authenticating party (or its technological artefact) knows that Data-Value, the Identifier itself can represent reliable EoI. Generally, however, an Identifier is not a secret, and most schemes use Data-Item(s) other than Identifiers.

The next Assertion category (2), an Entity Assertion, is of the form:

- A particular Physical Thing is appropriately associated with one or more Entity-Records

The Record-Key, in this case an Entifier, by definition reliably distinguishes that Entity-Instance from all other Instances of the same Entity. An Authenticator for this purpose, Evidence of Entity (EoE), differs from EoI, in that it is required to provide strong support for the proposition that the Physical Thing is a specific object, artefact or human.

An example is a Token installed in a device that provides the relevant Data to, and only to, the party doing the Authentication. Subject to careful design of the EoE creation, installation and storage, and of the communications protocols including transmission security features, a considerable degree of confidence can be designed into such a scheme. In the case of living things, a biometric measure may be used. Alternatively, a plant or an animal, including a human being, can be subjected to implantation of a Token in the same manner as installation of a Token into an artefact (Michael & Michael 2009).

Assertion categories (3) to (5) all involve Property Assertions. Simplifying:

- A particular Thing has a particular Property, based on one or more particular
  Data-Item-Values in one or more particular (Id)Entity Records

Two alternative approaches to the Authentication of Property Assertions are possible. Reliance may be placed on Evidence in such forms as Assertions containing sufficient detail that can be checked against one or more other sources (e.g. a claim of a qualification against a testamur, or against a database listing graduates).

The alternative approach is for the party performing the Authentication to rely on Data that they already hold. The relevant (Id)Entity Record may contain a directly-relevant Data-Item, such as a flag for 'Trade Customer' or 'Old-Age Pensioner', or for some category of disablement such as 'legally blind'. In other cases, it will be necessary for the organisation to apply logical processes to its Data to assess the claim. This applies, for example, to a claim of being owed a refund for a failed delivery; and to having reached a particular age or period of association with an organisation.

3.4 Data Quality's Role in the Authentication Process

Little material has been found that identifies criteria for data quality in support of Authentication processes. It is therefore necessary to got back to basic principles and work forward from there. Whether Data is a 'reliable representation' of the relevant phenomena depends on the factors listed in Table 1, comprising Data Quality factors (which are assessable at the time of creation and subsequently) and Information Quality factors (which are assessable only at the time of use).

The generic categorisation of quality factors in Table 1 needs to be applied to each circumstance. For example, an Identity Authenticator for a role may be vital to the signing of a large contract, in which case D7 (Temporal Applicability) looms as a high priority for careful checking. Another concern, causing people to be justifiably wary of government agencies sharing data, is that D3 (Appropriate Property Association) and D4 (Appropriate Property Signification) differ greatly, depending on context. The number of children a person declares to an agency depends on that agency's definition of 'a child of a person' (and definitions may even differ between programs administered by the same agency, and over time). The same holds for marital status, and for gender. More complex examples are legion, such as a person's income, which can be measured differently, and can be accumulated and/or averaged over periods as diverse as daily and annually.

Quality assurance measures needs to be layered. Safeguards must be designed into authentication processes, and implemented. Controls must be designed, implemented and monitored, to ensure that the safeguards are operational and effective.

When concern arises that an Authentication process may have been malperformed or may have delivered a wrong result, it is necessary to conduct an audit. This depends on reviewability, replicability, auditability, accountability, and action. For any of these measures to be feasible, Data needs to be available that document the basis on which each decision was made.

Table 1: Quality Factors

Data Quality Factors Assessable when created and later	**Information Quality Factors** Assessable only at the time of use
D1 Syntactical Validity Conformance of the Data-Item-Value with the Domain on which the Data-Item is defined	**I1 Theoretical Relevance** Demonstrable capability of the Data-Item to, in principle, make a difference to the inferencing process in which the Data-Item is to be used
D2 Appropriate Phenomenon Association A high level of confidence that the Data-Item-Value is associated with the particular Real-World Thing or Event it is intended to represent	**I2 Practical Relevance** A demonstrable capability of the Data-Item-Value to, in practice, make a difference to the inferencing process in which the Data-Item-Value is to be used
D3 Appropriate Property Association A high level of confidence that the Data-Item-Value is associated with the particular Property of the Real-World Thing or Event that it is intended to represent	**I3 Currency** The absence of a material lag between a Real-World Event and the recording of the corresponding Data-Item-Values
D4 Appropriate Property Signification A high level of confidence that the Data-Item-Value represents the state of the particular Property of the Real-World Thing or Event it is intended to represent	**I4 Completeness** The availability of sufficient contextual information that the data is not liable to be misinterpreted
D5 Accuracy A high level of correspondence of Data-Item-Value with the particular Real-World Thing or Event that it is intended to represent	**I5 Controls** The application of business processes that ensure that the Data Quality and Information Quality factors are satisfied
D6 Precision The level of detail at which the data is captured, reflecting the Domain on which the Data-Item is defined	**I6 Auditability** The availability of Metadata that evidences the Data Quality and Information Quality factors
D7 Temporal Applicability The absence of ambiguity about the date and time, or period, when the Data-Item-Value represents a particular Real-World Thing or Event	

Adapted from Clarke (2016), Table 1

This section has articulated the basic theory of Authentication in contexts relevant to identity management activities in IS. It identifies a range of needs. Areas in which IS practice and theory evidence shortfalls include the widespread error of conflating Identity and Entity, failure to be clear about what Assertions need what strength of

Authentication, failure to evaluate threats, and ineffectiveness of relevant safeguards, resulting in inability to rationally select a good-enough approach to Assertion Authentication.

4 Implications

The analysis presented above has important implications for IS practitioners, and for practice-oriented IS research. Some of these relate to the quality of IS design, while others reflect the importance of the human-values aspects of IS activities.

(1) The Effectiveness of Identity Management

Attention has been drawn to the significant differences between Entities that reflect Physical Things and Identities that reflect Virtual Things. The ability of an IS to support organisational activities is undermined if the model on which it is built conflates an Entifier such as a device-id with an Identifier of one of many processes running within that device. In such circumstances, users of a cybersecurity-monitoring system, for example, would be hampered in their efforts to detect runaway, rogue and compromised processes. Similarly, confusion could arise between a non-corporeal principal (such as a corporate trustee) and the individual person or software-process acting as the agent for that principal.

In the case of humans, the failure to distinguish Entities from Identities means there is an implicit assumption that a person whose Assertion of Identity is authenticated is necessarily a single, particular instance of *homo sapiens*. This flies in the face of many real-world practices. Employees routinely share passwords. The Authenticators used by older family members continue to be provided to younger members, so that payments can be made. Commercial terms may well provide organisations with legal assurance that they can repudiate responsibility for transactions conducted in such ways (if they can gather evidence). On the other hand, all of the organisation's work on risk assessment and risk management, including distinguishing between abuse of commercial terms by the principal and abuse by another party through unauthorised masquerade, lie outside the model, and hence are unsupportable by the IS.

Another technical problem masked by conventional, inadequate identity management models is the risk of biometrics being compromised, such that convincing biometrics-based masquerade is able to be committed. The Properties of Physical Things that are used for biometrics (fingerprints, iris-patterns, password-capture dynamics, gait, DNA, etc.), are not capable of being tightly protected. They can be captured and replicated, then simulated sufficiently well that Entity Authentication can be duped. Each advance in liveness-testing stimulates countermeasures.

The value of biometrics-based Entification may fall and/or governments may move to limit its use to tightly-controlled, priority circumstances. This would be tantamount to imposing a licensing scheme and heavily-sanctioned legal prohibitions on retention and transmission of biometric data. PIN-pads were designed to prevent capture, retention, replay and transmission of PINs. The same design approach can be applied to biometrics, by implementing a secure stored-biometric measure in a personal card, and installing a secure capture and processing module in the authentication device (Clarke 2003a). This has recently become more common in the form of separation of Authentication of an individual's Entity Assertion to their personal device (e.g. mobile phone, tablet) from Authentication to a remote service of the device's Entity Assertion and/or of each process's Identity Assertion.

(2) The Effectiveness of Other Business Processes

The widespread availability of high-capacity information infrastructure since the 1990s has had impacts on many aspects of organisational and individual activity. One key aspect is greatly increased institutional distance. For example, until the turn of the century, consumer credit business processes embodied a blend of Authentication of both category (2) and category (3) Assertions, because they were 'high-touch' in nature. Since then, most business enterprises have abandoned such labour-intensive approaches, and are now remote from their clients, making their decisions on the basis of a Digital Persona rather than the person (Clarke 1994a, 2014). Moreover, the recent fashions of big data, data analytics and AI/ML, by increasing the volume and diversity of data being used, and decreasing the transparency of the decision process, have greatly increased the scope for erroneous inferences. Authentication of category (3) Assertions are curtailed or dropped, and the much weaker form of Authentication of category (2) Assertions relied upon instead, because they are easily automated and inexpensive and quick.

These factors have given rise to greatly increased scope for faulty business decisions. These are not limited to the example used in the previous paragraph, consumer credit, but pervade many other application areas as well. Some of the harm directly affects the organisation sponsoring the system, e.g. through faulty evaluations of loan-worthiness. In many cases, however, the harm is suffered by users and usees. The infliction of harm may not come to the organisation's attention for some time, resulting in reputational risk. Imprecisions in the models underlying identity management schemes exacerbate these risks, and hence far greater care is needed in IS design than in the past. There are few signs, however, that appropriate changes are being made to safeguards, controls and mechanisms for redress.

(3) The Economics of IS Design

Ineffective identity management can have efficiency and financial impacts. Reduced reputation harms market-share and sales volumes, and hence increases the gross profit margin needed to cover the overheads. In industry sectors in which consumer protection and other regulatory mechanisms exist, the scope exists for customer complaints numbers to rocket, and with that complaints-handling costs. Restitution and redress to individual complainants can be greatly exceeded by even the legal costs of a class action, and swamped by a class action damages settlement.

The previous sub-section also noted the concerns of individuals about Entification processes and biometrics, about a consolidated Digital Persona, and about the risks of data-leakage and and manipulation that both give rise to. Identification processes are of particular concern where organisations have the capacity to inter-link multiple of a person's many Identities. This results in tensions between the organisation and individual users, both employees of the sponsoring organisation and external users. Those tensions play out in avoidance, obfuscation, falsification, and lowered ethicality of behaviour and loyalty among individuals with whom the organisation interacts, and in many cases on which it depends.

Identity Authentication, and particularly Entity Authentication, are expensive, both in terms of financial costs and negative impacts on users and usees. This raises the question as to whether the Authentication of other forms of Assertion may be able to deliver sufficient assurance to an organisation, and to be performed materially less expensively. Property Authentication can be achieved in many contexts without having to perform (Id)Entification and (Id)Entity Authentication processes. In addition, the prior paper which presents a generic theory of authentication identifies several other Assertion-categories that can be effective in satisfying organisations' needs, and can be at the same time more efficient. These are Fact Assertions, Content Integrity Assertions, Liquid-Asset Value Assertions and Non-Liquid-Asset Value Assertions (Clarke 2023).

Remarkably few sources have been located that give systematic consideration to the Authentication of Assertions other than of (Id)Entity. Exceptions include Clarke (2001), which argued that "parties [need to] know what is being authenticated" (p.148), and gave examples of Value and Attribute Assertions; Rauniar et al. (2002), which distinguished user authentication, smartcard authentication and card-reader authentication; and Clarke (2003b), which listed "Assertions important to eBusiness" as extending to organisational and artefact Entities and Identities, Attributes, Agency (referred to in this paper as a Principal-Agent Assertion), Location and Value. The absence of serious treatment in the literature is remarkable given the relative ease and inexpensiveness of Authentication of some of the other categories of Assertion, at least in a proportion of the circumstances in which activities are conducted.

(4) Stakeholder Interests

The primary focus in the first three sub-sections above has been the interests of the organisational sponsor of the particular IS. This final sub-section broadens the view to encompass stakeholders generally.

Many circumstances arise in which Authentication of any category of Assertion, and Authentication of (Id)Entity Assertions in particular, involve clashes of values between the system sponsor and individual users and usees. In some of those circumstances, the tension is intrinsic and largely unavoidable. For example, in both the lending and the insurance sectors, the contracting organisation is unlikely to be able to protect their financial interest unless key Assertions by the other party can be reliably authenticated. Similarly, government agencies that make transfer payments to the needy have an obligation to authenticate the claims made by each applicant. There are many circumstances, however, in which an appreciation of the full range of Authentication possibilities may enable the discovery of scope for the organisation to adopt less intrusive process designs. Individuals live their lives in enormously varied circumstances. Organisations that understand particular customer segments may be able to offer alternative Assertion-Authentication channels for, say, the seriously sight- or mobility-impaired, or for victims of domestic violence who are currently taking great care not to disclose their whereabouts.

More generally, many people are concerned about the conflation of their separate Identities. Some have reasons that derive from a desire for physical safety, others because of an enclosed disposition, some because of embarrassing personal histories, and of course some for reasons that may deleteriously affect the interests of an organisation they deal with. All such categories of people are likely to be concerned about the conflation of roles that they perform on behalf of an employer, with their roles on behalf of associations, clubs, their families, and their friends. Some people are even more concerned about the conflation of their Identities with multiple consumer marketing corporations, and even more so as public-private partnerships proliferate, government agency databases are compromised, and a movement gathers steam that began as a gleam in the eye of a Google CEO and Chair: the high-tech, corporatised-government State (Schmidt & Cohen 2013). This risk is inherent in Entifiers, but also increasingly common with Identifiers, where governments and consumer marketing corporations alike invest heavily in the consolidation of personal data into a singular Digital Persona. Many individuals are very concerned about the enablement of surveillance and manipulation, the creation of 'honey-pots' that attract third parties, the inevitable abuse of insider privileges, and leakage of sensitive personal information.

Arguments can be advanced for organisations to take individuals' interests into account for ethical, consumer rights or social responsibility reasons. Leaving those aside, however, organisational self-interest may well be best served by recognising the extent to which individual user behaviour, especially among employees and contractors, and usee behaviour, may not be what the organisation prefers. Specifically, individuals' behaviour may include objections, non-adoption, noncompliance, avoidance, obfuscation, falsification, quiet sabotage, and whistleblowing. These drive up an organisation's costs, and drive down its internal morale and its external reputation. Opportunities exist to apply insights from the model and analysis presented in this paper to envision and implement satisfactory forms of Authentication that are less burdensome and intrusive for individuals and less expensive and otherwise harmful for organisations.

The focus of this paper has been, throughout, on IS practice and practice-relevant IS research. Mention also needs to be made, however, of the broader issues that arise from the application of the pragmatic metatheoretic model to (id)entity. The axiological aspects of the model highlight the inadequate attention paid by both IS practice and research to values, and particularly the interests of users and usees. Further work is needed to draw out the implications of this work for professionally responsible IS design.

5 Conclusions

This paper has built on a previously-published pragmatic metatheoretic model, that is intended to reflect the Real World and the Abstract Worlds as they are understood, manipulated and applied in IS practice and practice-oriented IS research. It has drawn further on a previously-published extension of that model into the identity management space, and a generic theory of Authentication of Assertion categories relevant to IS.

The first contribution of this paper is a body of theory that identifies categories of Assertion that involve (Id)Entity, outlines key requirements of processes for the Authentication of those Assertion categories, describes the forms that may be taken by Evidence that can support those processes, and provides a framework for the evaluation of Data Quality and Information Quality of that Evidence.

A second area of contribution is the discussion of the implications of this body of theory for IS practice, and for the organisations that depend on the products of IS practitioners. Proposals are made for improvements in effectiveness and efficiency within the frame of reference used by the organisations that utilise IS. Further proposals are made that reflect the somewhat different worldviews of those organisations' employees, customers and suppliers, and of usees, who are affected by but do not directly participate in the system.

The analysis presented in this paper also identifies a number of weak spots in IS and practice, and points towards ways to address them. The most significant weakness, visited at multiple points in the paper, is the conflation of the concepts of Identity and Entity, and how that plays out in faulty business models and ineffective, inefficient and unpopular business processes. Another area in which considerable scope exists for insightful work is the ways in which organisations, as Virtual Things, are represented within IS models, and how the reliability of Assertions relating to them can be evaluated. For example, see Eriksson & Ågerfalk (2022).

Beyond these implications for IS practice, new directions for practice-oriented IS research are opened up. More illustrations and applications of the model will deliver deeper insights that offer value in particular contexts. Some industry sectors deal in natural objects and passive artefacts, both physical and virtual, whose Properties may demand refinements and extensions of a model and theory that are intentionally somewhat generic.

Active artefacts, again both physical and virtual, are increasingly being conceived and injected into IS. There is current controversy concerning the extent to which active artefacts can reliably be delegated the power to infer, decide and act in isolation, or need to be oriented towards decision support roles, working closely with humans. The elements of the above analysis of (Id)Entification, and of the Authentication of (Id)Entity Assertions, provide what may prove to be valuable perspectives on that problem-domain.

Acknowledgements

This work reflects feedback from many colleagues who have participated in seminars and panels, and formally and informally reviewed the many working papers and refereed papers on which the present work is built. It has also benefited from the thoughtful and informed comments of the Bled Conference reviewers.

References

Abbas R. & Michael K. (2022) 'Socio-Technical Theory: A review' In S. Papagiannidis (Ed), 'TheoryHub Book', TheoryHub, 2022, at https://open.ncl.ac.uk/theories/9/socio-technical-theory/

Altinkemer K. & Wang T. (2011) 'Cost and benefit analysis of authentication systems' Decision Support Systems 51 (2011) 394-404

Avison D. & Fitzgerald G. (2006) 'Information Systems Development - Methodologies, Techniques & Tools' McGraw Hill, 4th ed., 2006

Basul A. & Muylle S. (2001) 'Achieving Authentication in Electronic Markets: A Principal-Agent Perspective' Proc. 8th Research Symposium on Emerging Electronic Markets, Maastricht, The Netherlands, September 2001, at https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=538ce0bbebb44ce0159 95e3e5122092a3fa93171

Baumer E.P.S. (2015) 'Usees' Proc. 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI'15), April 2015, at http://ericbaumer.com/2015/01/07/usees/

Berleur J. & Drumm J. (Eds.) (1991) 'Information Technology Assessment' Proc. 4th IFIP-TC9 International Conference on Human Choice and Computers, Dublin, July 8-12, 1990, Elsevier Science Publishers (North-Holland), 1991

Brands S.A. (2000) 'Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy' MIT Press, 2000

Breward M., Hassanein K. & Head M. (2017) 'Understanding Consumers' Attitudes Toward Controversial Information Technologies: A Contextualization Approach' Information Systems Research 28,4 (2017) 760-774

Brown A.D. (Ed.) (2020) 'The Oxford handbook of identities in organisations' Oxford University Press, 2020

Carpenter D.R., McLeod A.J. & Clark J.G. (2008) 'Using Biometric Authentication to Improve Fire Ground Accountability: An Assessment of Firefighter Privacy Concerns' Proc. AMCIS 2008, at 11

Chaum D. (1985) 'Security Without Identification: Transaction Systems To Make Big Brother Obsolete' Communications of the ACM 28, 10 (October 1985) 1030-1044, at https://dl.acm.org/doi/pdf/10.1145/4372.4373

Clarke R. (1992) 'Extra-Organisational Systems: A Challenge to the Software Engineering Paradigm' Proc. IFIP World Congress, Madrid, September 1992, PrePrint at http://www.rogerclarke.com/SOS/PaperExtraOrgSys.html

Clarke R. (1994a) 'The Digital Persona and its Application to Data Surveillance' The Information Society 10,2 (June 1994) 77-92, PrePrint at http://www.rogerclarke.com/DV/DigPersona.html

Clarke R. (1994b) 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' Information Technology & People 7,4 (December 1994) 6-37, PrePrint at ://www.rogerclarke.com/DV/HumanID.html

Clarke R. (1999) 'Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice' Proc. Conf. User Identification & Privacy Protection Conference, Stockholm, June 1999, PrePrint at http://www.rogerclarke.com/DV/UIPP99.html

Clarke R. (2001a) 'The Fundamental Inadequacies of Conventional Public Key Infrastructure' Proc. Conf. ECIS'2001, Bled, Slovenia, 27-29 June 2001, PrePrint at http://www.rogerclarke.com/II/ECIS2001.html

Clarke R. (2001b) 'Authentication: A Sufficiently Rich Model to Enable e-Business' Xamax Consultancy Pty Ltd, 19 October 2001, at http://www.rogerclarke.com/EC/AuthModel.html011019.html

Clarke R. (2002a) 'Personal Notes on Computers, Freedom & Privacy 2002' CFP'22, San Francisco, Xamax Consultancy Pty Ltd, 16-19 April 2002, at http://rogerclarke.com/DV/NotesCFP02.html

Clarke R. (2002b) 'Why Do We Need PKI? Authentication Re-visited' Xamax Consultancy Pty Ltd, Presentation at the 1st Annual PKI Research Workshop, at NIST, Gaithersburg MD, April 24-25, 2002, at http://www.rogerclarke.com/EC/PKIRW02.html

Clarke R. (2003a) 'The Scope for Privacy-Sensitive Biometric Architecture' Xamax Consultancy Pty Ltd, February 2003, at http://www.rogerclarke.com/DV/BioArch.html

Clarke R. (2003b) 'Authentication Re-visited: How Public Key Infrastructure Could Yet Prosper' Proc. 16th Bled eCommerce Conf., June 2003, PrePrint at http://www.rogerclarke.com/EC/Bled03.html

Clarke R. (2004) 'Identity Management: The Technologies Their Business Value Their Problems Their Prospects' Xamax Consultancxy Pty Ltd, March 2004, 66 pp., at http://www.xamax.com.au/EC/IdMngt-Public.pdf

Clarke R. (2008) 'Dissidentity: The Political Dimension of Identity and Privacy' Identity in the Information Society 1,1 (December, 2008) 221-228, PrePrint at http://www.rogerclarke.com/DV/Dissidentity.html

Clarke R. (2009) 'A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation' Proc. IDIS 2009 - The 2nd Multidisciplinary Workshop on Identity in the Information Society, LSE, London, 5 June 2009, at http://www.rogerclarke.com/ID/IdModel-090605.html

Clarke R. (2014) 'Promise Unfulfilled: The Digital Persona Concept, Two Decades Later' Information Technology & People 27, 2 (Jun 2014) 182-207, PrePrint at http://www.rogerclarke.com/ID/DP12.html

Clarke R. (2016) 'Big Data, Big Risks' Information Systems Journal 26, 1 (January 2016) 77-90, PrePrint at http://www.rogerclarke.com/EC/BDBR.html

Clarke R. (2021) 'A Platform for a Pragmatic Metatheoretic Model for Information Systems Practice and Research' Proc. Austral. Conf. Infor. Syst. (ACIS), December 2021, PrePrint at http://rogerclarke.com/ID/PMM.html

Clarke R. (2022) 'A Reconsideration of the Foundations of Identity Management' Proc. 35th Bled eConference, June 2022, pp.1-30, PrePrint at http://rogerclarke.com/ID/IDM-Bled.html

Clarke R. (2023) "A Generic Theory of Authentication to Support IS Practice and Research' Xamax Consultancy Pty Ltd, January 2023, at http://rogerclarke.com/ID/PGTA.html

Clarke R. & Davidson R.M. (2020) 'Through Whose Eyes? The Critical Concept of Researcher Perspective' J. Assoc. Infor. Syst. 21, 2 (March-April 2020) 483-501, PrePrint at http://rogerclarke.com/SOS/RP.html

Coneybeare F.C. (1892) 'Professor Clifford on the Soul in Nature' The Monist 2,2 (January 1892) 209-224, at https://www.jstor.org/stable/27896942

Eaton B., Hallingby H.K., Nesse P.-J. & Hanseth O. (2014) 'Achieving Payoffs from an Industry Cloud Ecosystem at BankID' MIS Quarterly Executive 13,4 at 6

Elgarah W. & Falaleeva N. (2005) 'Adoption of Biometric Technology: Information Privacy in TAM' Proc. AMCIS 2005, at 222

Eriksson O. & Ågerfalk P.J. (2022) 'Speaking things into existence: Ontological foundations of identity representation and management' Information Systems Journal 32,1 (2022) 33-60, at https://onlinelibrary.wiley.com/doi/full/10.1111/isj.12330

Fairchild A.M., O'Reilly P., Finnegan P. & Ribbers P.M. (2007) 'Multi-Criteria Markets: An Exploratory Study of Market Process Design' Electronic Markets 17,4, (Nov 2007) 286-297, at http://www.electronicmarkets.org/fileadmin/user_upload/doc/Issues/Volume_17/Issue_04/V17I4_Multi-Criteria_Markets__An_Exploratory_Study_of_Market_Process_Design.pdf

Fischer-Huebner S. & Lindskog H. (2001) 'Teaching Privacy-Enhancing Technologies' Proc. IFIP WG 11.8 2nd World Conf. on Information Security Education, Perth, Australia

Gottwald S. (2001) 'A Treatise on Many-Valued Logics', January 2001, at https://www.researchgate.net/profile/Siegfried-Gottwald/publication/259645593_A_Treatise_on_Many-Valued_Logics/links/00b7d5324ce793473c000000/A-Treatise-on-Many-Valued-Logics.pdf

Haider A. (2008) 'Believable Unbelievable Internet Based Information' Proc. ACIS 2008, at 93

Halperin R. & Backhouse J. (2008) 'A roadmap for research on Identity in the information society' Identity in the information society journal 1,1 (2008) 71-87, at https://link.springer.com/article/10.1007/s12394-008-0004-0

Hewitt B. (2009) 'Using a Hybrid Technology Acceptance Model to Explore How Security Measures Affect the Adoption of Electronic Health Record Systems' Proc. AMCIS 2009, at 328

IETF (2022) 'RFCs' Internet Engineering Task Force (IETF), December 2022, at https://www.ietf.org/standards/rfcs/

Kambil A. & van Heck E. (1998) 'Reengineering the Dutch Flower Auctions' Information Systems Research 9,1 (March 1998) 1-19

Magnusson A. (2022) 'The Definitive Guide to Authentication' Strong DM, September 2022, at https://www.strongdm.com/authentication

Michael K. & Michael M.G. (2009) 'Innovative Automatic Identification and Location-based Services: From Bar Codes to Chip Implants' Information Science Reference, 2009

Mumford E. (2006) 'The story of socio-technical design: reflections on its successes, failures and potential' Info Systems J 16 (2006) 317-342, at https://executiveinsight.typepad.com/files/the-story-of-socio-technical-design.pdf

Nyst C., Makin P., Pannifer S. & Whitley E. (2016) 'Digital identity: Issue analysis: Executive summary' Consult Hyperion, 2016

OASIS (2005) 'SAML V2.0 Standard' OASIS, March 2005, at https://wiki.oasis-open.org/security/FrontPage

Rauniar R, Rauniar D., Shakya S. & Urcuyo C. (2002) 'A Mutual Authentication Scheme for Low Cost Smart Card Applications' Proc. AMCIS 2002, at 265

Ryan T.W. & Marett K. (2010) 'The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived' Journal of Management Information Systems 27,1 (Summer 2010) 273–303

Schmidt E. & Cohen J. (2013) 'The New Digital Age: Reshaping the Future of People, Nations and Business' Knopf, 2013

Stevens S.S. (1946) 'On the Theory of Scales of Measurement' Science 103, 2684 (7 June 1946), at https://psychology.okstate.edu/faculty/jgrice/psyc3120/Stevens_FourScales_1946.pdf

Way S.C. & Yuan Y. (2009) 'Criteria for Evaluating Authentication Systems' Proc. AMCIS 2009, at 338

Witman P. (2006) 'Anti-Phishing Strong Authentication Technology Options' Proc. AMCIS 2006, at 131

Zviran M. & Erlich Z. (2006) 'Identification and Authentication: Technology and Implementation Issues' Commun. Assoc. Infor. Syst. 17,4 (2006) 90-105

Supplementary Materials

Glossary, at http://rogerclarke.com/SOS/FDI.html#G
'The Authentication of Assertions Relating to (Id)Entity',
a comprehensive Working Paper from which the present paper is drawn, at
http://rogerclarke.com/ID/IEA.html