Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2023 Proceedings | Australasian (ACIS)

12-2-2023

A Generic Theory of Authentication to Support IS Practice and Research

Roger Clarke
Xamax Consultancy Pty Ltd / ANU Computer Science / UNSW Law, Australia, roger.clarke@xamax.com.au

Follow this and additional works at: https://aisel.aisnet.org/acis2023

Recommended Citation
Clarke, Roger, "A Generic Theory of Authentication to Support IS Practice and Research" (2023). *ACIS 2023 Proceedings*. 9.
https://aisel.aisnet.org/acis2023/9

This material is brought to you by the Australasian (ACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ACIS 2023 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

How Confident are We in the Reliability of Information? A Generic Theory of Authentication to Support IS Practice and Research

Full research paper

Roger Clarke
Xamax Consultancy Pty Ltd, 78 Sidaway St, Chapman ACT 2611
School of Computing, Australian National University, Canberra
Faculty of Law, University of NSW, Sydney
Email: Roger.Clarke@xamax.com.au

Abstract

This paper addresses a yawning gap in IS theory and practice. In the information systems (IS) discipline and profession, the concept of authentication is commonly limited in scope to the checking of assertions relating to identity. The effective conduct of organised activities depends on the authentication of not only assertions of those kinds, but also many other categories of assertion. The paper declares its metatheoretic assumptions, and outlines a pragmatic metatheoretic model whose purpose is to establish a workable framework for IS practitioners, and for researchers oriented to IS practice. Within this frame, a generic theory of authentication is proposed, encompassing not only commonly discussed kinds of assertions, but also other important categories relating to real-world properties, asset-value and content-integrity. This surfaces unaddressed opportunities for IS researchers in content-integrity authentication at the semantic level, relating to assertions of fact.

Keywords Assertion, Authentication, Evidence, Verification, Fact-Checking

1 Introduction

Use of the term 'authentication' in contexts relevant to information systems (IS) practice and research is almost always limited to what is referred to here as '(id)entity authentication'. For example, in the large family of standards documents published by the Internet Engineering Task Force (IETF 2022), a device, or a process running in a device, 'authenticates itself' to another device or process. This is commonly done by declaring the entifier of a device, or the identifier of a process running on a device, and demonstrating that the device or process has access to a secret that only that device or process is expected to know. The US government standards document extends beyond artefacts to encompass human entities and their identities, defining authentication as "Verifying the identity of a *user*, process, or device, often as a prerequisite to allowing access to resources in an information system" (NIST 2006, p.6, *emphasis added*). Magnusson (2022) provides a straightforward, commercial explanation of the NIST notion, using the definition "the process of verifying a user or device before allowing access to a system or resources".

However, (id)entity is far from the only thing that needs to be authenticated (Clarke 2001, 2003). Hence, limiting the scope of the term has serious drawbacks. Examples of other things that need to be authenticated include claims of value, declarations by an agent of its authority to act on behalf of a principal, and statements of fact. These are crucial to processes of business, governments and societies. The author contends that many of the ongoing weaknesses in identity management, and in information reliability more generally, arise from an inadequate conception of authentication. The purpose of the work reported both in this paper and in others published within the broader project, is to establish a comprehensive theoretical basis to support reliability assessment. The intent also exists to broaden the scope of IS, enabling it to contribute to the currently fraught area of misinformation and disinformation.

The proposition that authentication needs to be interpreted broadly is unusual in the IS literature, to the extent that few explicit sources can be readily identified. An inspection of the first 200 hits using a Google Scholar search on <authentication "information systems"> detected almost no uses other than in relation to identity authentication. Exceptions include a small body of work on watermarking for image provenance authentication (a topic currently enjoying a resurgence in the context of generative AI), and a single throwaway sentence in a mainstream IS journal: "Authentication can be used to verify either *the content of the message, the origin of the message*, or the identity of the user" (Altinkemer & Wang 2011, p.394, emphasis added). Other examples found in the AIS electronic Library (AISeL) are Mattke et al. (2019) and Thomas & Negash (2023) who refer to transaction and asset authentication in the context of blockchain implementations, and Lausen et al. (2020) who discuss the authentication of claims made by financial professionals in relation to their previous employment and licences held.

In the IS literature generally, even the common, narrow interpretation as '(id)entity authentication', while clearly within-scope, is not a particularly lively topic-area. For example, the string <authentication> is found in Title or Abstract in only 37 of over 17,000 refereed papers in the AIS electronic library (AISeL), with the positivist term <verification> used in a further 13. (All hits provided by the AISeL search-engine require inspection, because of generic uses, specific usages distinct from the one relevant here, and an over-generous synonym-table, which treats 'authentic' and 'authenticity' as equivalents to 'authentication'). Searches across all of the Basket of 8 IS journals produced a count of 12 out of >10,000 articles with 'authentication' in Title or Abstract. Searches for at least a single occurrence of the term in full-text finds 324 in Basket of 8 corpus, and 1,331 in AISeL. On inspection, however, fewer than two dozen of them make a contribution to the work reported here. It is contended that the narrowness of the conventional conception gives rise to important deficiencies in IS practice, which IS researchers have failed to identify and address.

This paper's purpose is to express a general theory of authentication that encompasses not only (id)entity authentication but also the many other circumstances in which the reliability of claims is assessed. The theory is intended for use to support both IS practice and research. To achieve that end, the analysis applies a previously-published, pragmatic metatheoretic model, comprising a working set of assumptions in each of the areas of ontology, epistemology and axiology (Clarke 2021).

The paper commences by briefly presenting the underlying pragmatic metatheoretic model. It then discusses the abstract notion of 'authentication', placing it within that model, and defining it as a process that establishes a level of confidence in an assertion. A number of kinds of assertion are

distinguished, and descriptions are provided of the processes and criteria necessary to enable their authentication. The categories in which (id)entity plays a key role require article-length treatment which has been presented elsewhere (Clarke 2023). This paper reviews those ideas only briefly, and has its focus instead on the categories that are currently short-changed in the IS literature. Implications are drawn for IS practice and for IS research.

2 The Underlying Pragmatic Metatheoretic Model

The analysis of authentication presented in this paper builds on previous work that proposed a pragmatic metatheoretic position and model to support IS practice and research (Clarke 2021). This section provides a recapitulation of key aspects of that work. The model is referred to as 'metatheoretic' (Myers 2018, Cuellar 2020), on the basis that it draws on relevant areas of philosophy in which IS practitioners and theorists alike make 'metatheoretic assumptions', often implicitly, and sometimes consciously. Where the assumptions are both conscious and intentional, a more appropriate term for them is 'metatheoretic commitments'.

A first area in which this work has a metatheoretic commitment is in the conception of an IS as "a set of interacting artefacts and human activities that performs one or more functions involving the handling of data and information" (Clarke 1990), or "a system which assembles, stores, processes and delivers information ... a human activity (social) system which may or may not involve the use of computer systems" (Avison & Fitzgerald 2006, p. 23). Since the mid-20th century, information technology (IT) has become pervasive. A largely technical view of IS may be legitimate in the case of highly-automated decision-and-action systems. On the other hand, for that large majority of IS that are concerned with data, information and decision support, the interweaving of artefacts with human activity means that neither a wholly technical nor a wholly social view can provide a sufficient basis for understanding.

Key aspects of the socio-technical view are that organisations comprise people using technology, that each affects the other, and that effective design depends on integration of the two (Mumford 2006, Boell & Cecez-Kecmanovic 2015, Abbas and Michael 2022). Adopting the socio-technical view, "[t]he social and the technical should be apportioned comparable emphases" and treated as "as two mutually interacting components" (Sarker et al. 2019, pp.697, 698). Yet those authors' study of works in MISQ and ISR concludes that "about 87% of the studies reviewed focused solely on instrumental outcomes" (p.704), by which the authors mean "higher productivity" for the benefit of the system sponsor (p.698), and that "by losing sight of humanistic goals, the IS discipline risks facilitating the creation of a dehumanized and dystopian society" (p.705). As a remedy for that particular ill, calls have been made for IS researchers to adopt the perspectives of salient stakeholders, as well as, and in some cases even instead of, those of the system sponsor (Clarke 2020).

A further commitment that I bring to this work is that IS research is concerned with advancing IS practice. However, this is even more unfashionable than the socio-technical view of IS: "while everyone pays lip service to the importance of applied research, when it comes time to publish it, the mainstream journals are generally unwilling participants ... Papers are routinely rejected from our journals because they fail to make a sufficient theoretical contribution" (Hirschheim 2019, pp.1349, 1351). The approach I have adopted, the model I have proposed, and the analyses based on that model, may therefore be relevant only to that sub-set of readers who subscribe to, or at least tolerate, both a socio-technical view of IS and a practice orientation.

The model is also 'pragmatic', as that term is used in philosophy, that is to say it is concerned with understanding and action, rather than merely with describing and representing. The author's intention is instrumentalist, in this case not economically motivated but to achieve change in the worldviews of IS practitioners and researchers, and hence changes in professional behaviour patterns and in the management of data. So the model needs to speak to IS practitioners, and to those IS academics who intend the results of their research to do the same.

The deepest-rooted metatheoretic assumptions of the model are in three areas of philosophy. The ontological approach adopted here is that a reality exists, outside of and independently of the human mind, where Phenomena exist – a position commonly referred to as 'realism'. Humans cannot directly know or capture those Phenomena. They can, however, sense and measure those Phenomena, can create data reflecting them, and can construct models of them – an assumption related to the ontological assumption referred to as 'idealism'. This is reflected in Figure 1, which distinguishes a Real World from an Abstract World. The Real World comprises 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.

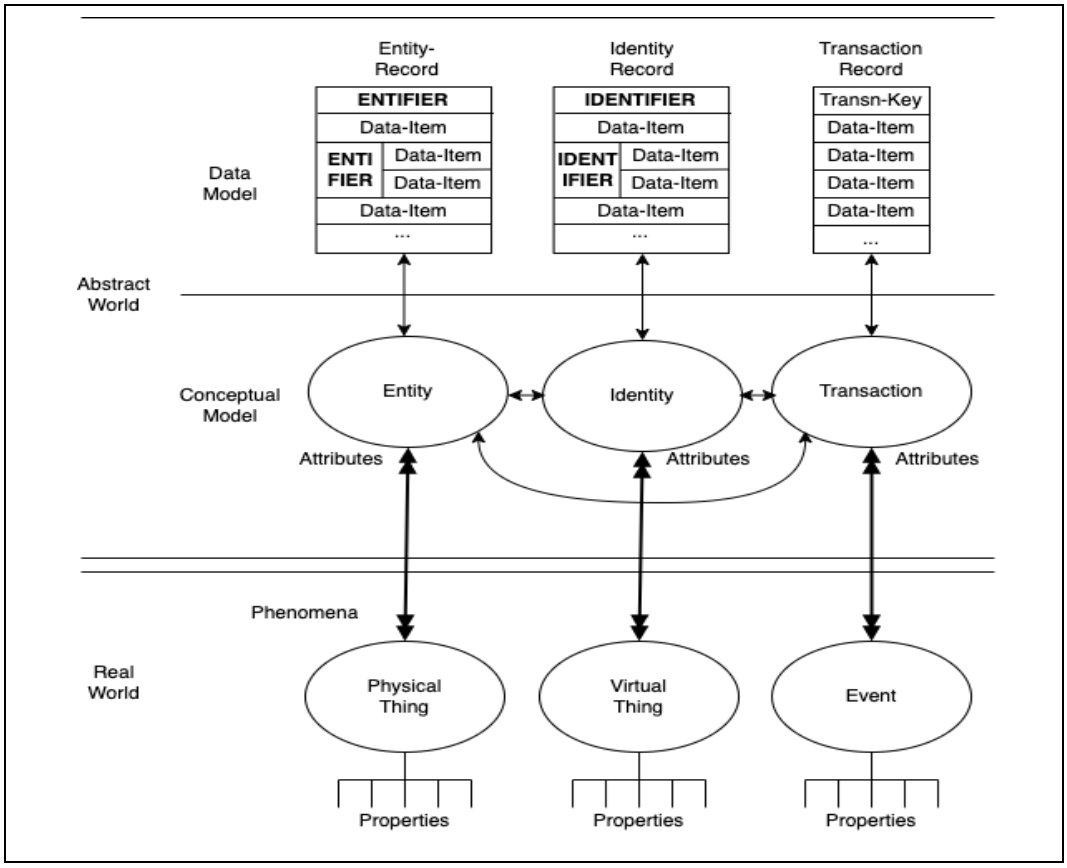

Figure 1: A Pragmatic Metatheoretic Model
From Clarke (2021)

In epistemological terms, a pragmatic metatheoretic approach must support practice and research not only in contexts that are simple, stable and uncontroversial, but also where there is no expressible, singular, uncontested 'truth'. The assumption adopted here is that the empiricist view is applicable (perceiving knowledge as a body of facts and principles derived from sensory experience and accumulated by humankind over time, that is capable of being stored in the equivalent of a warehouse – Becker & Niehaves 2007, p.202), but that so too is the apriorist epistemological view (that knowledge is internal and personal, and the concept is not applicable outside the mind of an individual human). The two different views are applicable in different circumstances, and many variants of those circumstances arise in IS practice.

Humans create Abstract Worlds. Some are imaginary, variously tenable and simply fantasy. Those of primary relevance here are empirically-based, in the sense of being intended to model relevant aspects of the Real World. In Figure 1, Abstract Worlds are depicted as being modelled at two levels. The Conceptual Model level reflects the modeller's perception of the Things, the Events and their Properties, providing a general idea of the Phenomena**.** The notions of Entity and Identity at the Conceptual Model level correspond to categories of Things, and Transaction to the category of Events.

A key difference in this Model from mainstream approaches is the clear distinction made between Identities and Entities. The abstract concept of Identity corresponds to a particular presentation of a Thing, as arises when it performs a particular role, that is to say, a pattern of behaviour adopted by an Entity. For example, the NIST (2006) definition of Authentication distinguishes a "device" (in this model, an Entity) from a "process" (an Identity). An Entity may adopt one Identity in respect of each Role, or may use the same Identity when performing multiple Roles. Within a corporation, over time, different human Entities adopt the Identity of CEO, whereas the Identity of Company Director is adopted by multiple human Entities at the same time, each of them being an Identity-Instance.

The Data Model Level enables the operationalisation of the relatively abstract ideas at the Conceptual Model level. This moves beyond a design framework to fit with data-modelling and data management techniques and tools, and to enable specific operations to be performed to support organised activity. Central to this level is the notion of Data. The term, used variously as a plural and as a generic noun, refers to a quantity, sign, character or symbol, or a collection of them, that is in a form accessible to a person and/or an artefact. A Data-Item is a storage-location in which a discrete Data-Item-Value can be represented.

The term Information is used in many ways (Boell 2017). Frequently, even in refereed sources, it is used without clarity as to its meaning, and often in a manner interchangeable with Data. The pragmatic model adopted in this paper uses the term Information specifically for a sub-set of Data: that Data that has value (Davis 1974 p.32, Clarke 1992b, Weber 1997 p.59). Data has value in only very specific circumstances. Until it is in an appropriate context, Data is not Information, and once it ceases to be in such a context, Data ceases to be Information.

An Assertion (per OED 5, "a positive statement; a declaration, averment") is a putative expression of knowledge about one of more elements of the metatheoretic model. Signifiers that make up Assertions may involve particular elements of the Real World (e.g. 'A physical item was delivered to a location'); or they may relate to particular elements of an Abstract World (e.g. 'A delivery Transaction caused changes in the states of Entities representing stock-holdings and a customer order', or 'A delivery Transaction-Record caused changes in Data-Items in the Entity-Records reflecting a particular stock-item and a particular customer order'). Alternatively, they may map between particular elements in both the Abstract and Real Worlds (e.g. 'The Data-Record that contains a particular Record-Key [all of which is in the Abstract World] relates to a particular Thing [which exists in the Real World]').

The third relevant branch of philosophy is Axiology. This deals with 'values', in the sense of "the relative worth, usefulness, or importance of a thing" (OED II 6a). The values dominant in most organisations are operational and financial. However, many contexts arise in which there is a pressing need to recognise broader economic interests, and values on other dimensions as well, particularly the social and the environmental. 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 1992a, Fischer-Huebner & Lindskog 2001, Baumer 2015).

Several approaches exist to the question of how to determine what values to apply. In simple contexts, virtue-based evaluation (ethically or morally good/bad) may be applicable. In some circumstances, deontic approaches are appropriate, recognising an obligation, and constraining behaviour to achieve compliance with some externally-imposed norm (March & Allen 2014). Other contexts are teleologically-driven or utilitarian, with the determination of appropriate actions dependent on the degree of alignment of impacts and outcomes with the designer's purpose. The axiological approach adopted here is aligned with IS practice. It is teleological and instrumentalist, seeking to support the development and maintenance of effective, efficient and adaptable IS.

In respect of any particular IS, there are one or more system sponsors, and multiple stakeholders, all with differing value-sets (Freeman & Reed 1983). The value-conflicts that arise may all be of an economic nature, particularly between the system-sponsor's operational and financial objectives and the financial interests of users. However, a range of factors can give rise to much greater complexity in the assessment of utility. Important examples are where:

- there are multiple stakeholders with materially different value-sets;
- stakeholder groups are sufficiently heterogeneous that they do not speak with a single voice, e.g. where meaningful minorities exist along such lines as ethnicity, religion, sexual preferences, and physical and mental dis/diff/abilities;
- some stakeholders exhibit high intensity of desire to achieve their aims;
- stakeholder interests extend beyond economic factors to include, in particular, social, environmental and political objectives;
- one or more stakeholders have sufficient power that progress is unlikely without accommodation by the system sponsor, and some degree of tolerance, negotiation and compromise among the participants (Achterkamp & Vos 2008); and/or
- reference-points exist other than humans, such as animals, plants, natural ecologies or the biosphere as a whole.

In summary, the model and work undertaken applying it are founded on meta-theoretic commitments to a socio-technical view of IS, an orientation to practice and practice-relevant IS theory, and a pragmatic concern with understanding and action. Consistently with those commitments, the ontological position adopted is to treat realism and idealism as being reconcilable. Both the empiricist and apriorist epistemological views are seen as being applicable to various circumstances within the scope of IS. The axiological approach is teleological and instrumentalist, seeking to support the development and maintenance of effective, efficient and adaptable IS.

This section has drawn on the pragmatic metatheory described in Clarke (2021) to identify aspects of it that are relevant to the generic notion of authentication.

3 Authentication in Theory

Authentication is a process applied to Assertions. This section first outlines the elements evident in dictionary definitions, and then proposes a working definition. The concept is then considered within the context of the pragmatic metatheoretic model outlined in the previous section, and other sources of insight.

The richest dictionary source records a wide range of interpretations of the verb to authenticate, and of the object of the action or process of authentication (OED 1, 3a, 3b, 4a, 4b, 5, 6). The interpretations can be summarised as follows:

> *to { validate, approve, prove, confirm, establish as genuine/authentic, verify }*
> *{ something/anything, a statement, an account, truth, existence, a reputed fact, a document, an artefact, an artwork, a user identity, a process identity }*

IS practice and research has narrower scope than a dictionary needs to encompass. There are, however, considerable variations in the contexts that need to be addressed. This paper's aim is to establish a metatheoretic foundation for Authentication in IS practice and research. A fundamental assumption of this work, that a socio-technical view of IS is essential, has the corollary that it is untenable to assume that each, or any, assertion can be resolved by reference to a singular, accessible truth. It could be feasible to do so if the more extreme forms of positivism are adopted; but design science research, interpretivism and critical theory research appear highly unlikely to be able to accommodate an uncompromising assumption of the existence of accessible truth. That leads to a strong preference to avoid language that implies truth, such as 'verification' or 'validation'. Instead, there is a need for fuzziness, or at least degrees of likelihood or reliability, quite possibly contingent on multiple factors. The following is accordingly proposed as an operational definition:

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

At the Real-World Level, Assertions are expressed in terms of Things that are postulated to exist, and Events that are postulated to occur and to have impacts on the Properties of Things. Hence 'A delivery of Things called stock-items was received by a category of Things called customers' or 'There are no relevant Things (stock-items) in the Thing (a storage-bin) that is allocated to that particular category of stock-items'. The Real-World level is best conceived as the external point-of-reference of the IS, rather than as part of the IS.

At the Abstract Level, some Assertions are expressed in terms of (Id)Entities and Transactions and their Attributes. For example, 'A Transaction has occurred that affects the stock-count Attribute of that Entity-Instance'. Other Assertions are expressed in terms of the Data Model level, such as 'A Transaction-Record gives rise to changes in (Id)Entity-Records'. At this level, reasoning can be applied to Assertions in order to infer further Assertions. Classical logic, such as the propositional calculus, only supports conclusions of right or wrong / true or false. Many-valued and fuzzy logics are of greater value, because they recognise that propositions can have degrees of truth (Gottwald 2001).

Some logics support qualitative data that makes nominal, imprecise distinctions among categories. Some other logics are appropriate to data on an ordinal scale (e.g. unborn, young, old, dead), and yet others require discrete quantitative values on an ordinal scale (such as the non-linear Richter scale for intensity of earthquakes), or on an interval scale (with equal distances between consecutive values, cf. Celsius for temperature). A ratio scale has the further requirements of a natural zero (cf. Kelvin for temperature). See Stevens (1946). Powerful inferencing tools are applicable to data on ratio scales. Assertions and inferences from them are of value to decision-making. On the other hand, the Authentication of Assertions in the Abstract World can provide only limited assistance in assuring reliability, because it implicitly assumes that the Assertions, and inferences from them, are

representative of the Real World. Logics offer little assistance to the tasks of testing the relationship between Data and the Real World, and enabling assessment of the degree of confidence in the Real-World reliability of Assertions.

The forms of Assertion that are most critical to the effectiveness of an IS are those that bridge between the Real-World and Abstract-World Levels. They represent empirical linkages, and assurance is needed that decision-makers can rely on those linkages. In Figure 1, interactions or mappings between Real-World and Abstract World elements are denoted by double-headed arrows. An example of such an Assertion is 'A physical stock-count of Things in a particular storage-bin identified a mis-match between that count and the relevant Data-Item-Value'. This presents supporting evidence for the reliability or otherwise of an Assertion of stock-holding counts, and, by inference, of monetary value.

4 Authentication in Practice

The previous section declared foundational theory about the Authentication of Assertions. This section further articulates those basic ideas, to enable its practical application. Assertions at the Abstract Level can be evaluated. One form this can take is a check of compliance with the rules of logic, to detect whether a flaw exists in the chain of argument. Another is checks of the language used, to ensure that no misunderstandings have arisen from ambiguous language. More valuably, Assertions that straddle the Real World and the Abstract World can be authenticated. Data-Item-Values can be compared with available observations of the Real World, purpose-designed observation and measurement can be conducted, and checks can be devised to ensure that the observations are of sufficient quality.

The degree of confidence in an Assertion that is desirable, and the extent to which that degree can be achieved, vary widely, depending on the circumstances. The term Evidence is used here to mean Data that assists in determining the level of confidence in an Assertion's reliability. This is closely related to OED's definition of Evidence III, 6: " ... facts or observations adduced in support of a conclusion or statement; the available body of information indicating whether an opinion or proposition is true or valid".

An individual item of Evidence is usefully referred to as an Authenticator. A common form of Authenticator is a Document, by which is meant content of any form and expressed in any medium, often text but possibly tables, diagrams, images, video or sound. Content on paper, or its electronic equivalent, continues to be a primary form.

Some Authenticators carry the imprimatur of an authority, such as a registrar or notary. Such Authenticators are usefully referred to as Credentials ("any document used as a proof of identity or qualifications", OED B2). Common examples of Credentials for human Identities are a birth certificate, certificate of naturalisation, marriage certificate, passport, driver's licence (and, in some jurisdictions, non-driver's 'licence'), employer-issued building security card, credit card, club membership card, statutory declaration, affidavit, and letter of introduction.

The term Token refers to a recording medium on which useful data is stored. Tokens are applied to the storage of machine-readable copies of (Id)Entifiers, such as identity cards (especially 'photo-id'), turnaround documents, sequentially-numbered tickets issued to people required to wait in a queue, machine-readable visual images (such as bar-codes or QR-codes) and machine-readable data-storage (such as a magnetic-stripe, solid-state memory, or transmission from an RFID-tag). Tokens may also contain Authenticators generally, and Credentials in particular. Security features are necessary, in order to provide confidence in the validity of the Token and its contents, such as hidden graphic features to guard against forged Tokens, and cryptographic features to guard against manipulation of the content. If a particular Entity is intended to be a Token's exclusive user, measures may also be needed to reliably associate the Token with that Entity.

Where the subject of the Assertion is a passive natural object, animal or artefact, the Authentication process is limited to checking the elements of the Assertion against Evidence already held, or acquired from, or accessed at, some other source considered to be both reliable and independent of any party that stands to gain from masquerade or misinformation. On the other hand, humans, organisations (through their agents), and artefacts capable of acting in the Real World, can be participants in the Authentication process, by means of a 'challenge-response' sequence. This involves a request to the relevant party for an Authenticator, and an answer or action in response. Examples of Authenticators relevant to each of the important categories of Assertion are provided in the following section.

In legal proceedings, distinctions are drawn among testimony (verbal evidence), documentary evidence, and physical evidence. The term probative means "having the quality or function of proving or demonstrating; affording proof or evidence; demonstrative, evidential" (OED 2a). In the law of evidence, "'probative value' is defined to mean the extent to which the evidence could rationally affect the assessment of the probability of the existence of a fact in issue" (ALRC 2010, 12.21). At law, a court is required to treat some kinds of Assertion as rebuttable presumptions, to be treated as being reliable unless and until case-specific evidence is presented that demonstrates otherwise. This makes clear on which party the onus of proof lies. In civil jurisdictions, the standard of proof is 'preponderance of the evidence' or 'preponderance of the probabilities', whereas in criminal jurisdictions the threshold of proof is generally 'beyond a reasonable doubt'. The law also recognises that economic constraints apply to evidence-collection and authentication processes: "a decision is better if it is less likely to be erroneous, in light of the actual (but unknown) outcome of the decision that would be known if there were perfect information. The quality of the decision takes into account the magnitude of ... harm from making the erroneous decision [and] the probability of doing so" (Salop 2017, pp.12-13).

In the context of investigations by a law enforcement agency, the term 'evidence' is used in a somewhat different sense. An investigator seeks patterns or relationships within data, which at best will point firmly towards the resolution of a case, but which will desirably at least close off an unproductive line of enquiry and even lead the investigator towards more promising lines. A degree of protection against spurious results is desirable, but the disincentives have to do with resource efficiency rather than a wrong result in a civil process or a criminal trial. Linked with this looser form of evidentiary standard is the concept of confirmation bias, which describes the tendency to take notice of evidence that supports a hypothesis rather than that which conflicts with it, and the even more problematic tendency to actively look for evidence that will support rather than refute a currently favoured proposition (Nickerson 1998).

A range of risk factors impinge on the quality of Authentication processes. Of especial importance is the need to achieve an appropriate balance between the harm arising from false positives, which are Assertions that are wrongly accepted; and false negatives, which are Assertions that are wrongly rejected. Sources of poor quality include accidental mistakes, and intentional mistakes which generate intentionally false positives, e.g. masquerade or 'spoofing' or intentionally false negatives, e.g. avoidance, undermining or subversion of (Id)Entification. Where quality shortfalls occur, additional considerations come into play, including the means whereby a party can contest or repudiate an assertion; which party bears the onus of proof; which party bears the risk, cost and inconvenience; and what avenues are available for challenge, adjudication and redress.

Quality is a substantially greater challenge where relevant parties are motivated to contrive false positives or false negatives. Safeguards are needed to limit the extent to which such parties may succeed in having Assertions wrongly accepted or wrongly rejected, in order to gain advantages for themselves or others. The level of assurance of an Authentication mechanism depends on the extent of safeguards against abuse, and hence on whether an Assertion can be effectively repudiated by the relevant actor. It is conventional to distinguish multiple quality-levels of Authentication, such as unauthenticated, weakly authenticated, moderately authenticated and strongly authenticated. Organisations generally adopt risk management approaches, accepting lower levels of assurance in return for processes that are less expensive, more practical, easier to implement and use, and less intrusive (Altinkemer & Wang 2011).

5 Categories of Assertion

The analysis to date has considered the generic concept of Authentication of a generic notion of Assertions. In practice, there are many kinds of Assertions, and a theory to support IS practice and research needs to be sufficiently articulated to encompass them and to reflect their differences. This section identifies key categories of Assertion, drawing on the practice and theory of, in particular, identity management, but also the well-established techniques of Entity-Relationship Modelling. The categories are described in sufficient detail to enable the theory to be applied, and to demonstrate its effectiveness and usefulness, in a variety of contexts.

5.1 Assertions Involving (Id)Entity

It was noted earlier that assertions that involve an Entity or Identity are the sole focus of almost all discussions of Authentication in both IS practice and research. The primary category in practice is:

> *A particular Real-World Thing is appropriately associated with a particular (Id)Entity-Instance at the Conceptual Level of an Abstract World and/or with one or more particular (Id)Entity-Records at the Data Level*

Multiple other categories exist, which are complex to describe and to understand, and challenging to implement effectively. The complexities are such that this is the topic of two separate full-length papers on (Id)Entities and (Id)Entification (Clarke 2022) and their Authentication (Clarke 2023). In the case of human Entities, they are also inevitably invasive of personal space. Because of those characteristics, it is highly advantageous to all concerned for Authentication activities to focus on other kinds of Assertions if they are capable of satisfying the need.

5.2 Property Assertions

Another important category is Property Assertions. In this context, the word 'property' refers not to ownership, but rather to a feature of a Real-World Thing. A simple Property Assertion is of the form:

> *A Real World Thing has a Property that is appropriately represented in the Abstract World by an Entity-Instance-Attribute-Value and/or an Entity-Record-Data-Item-Value.*

If the Real-World Thing is a gem, its Property of 'weight in carats' can be tested by independent measurement. Alternatively, some kind of Credential may be inspected, such as a jeweller's valuation. A party that accepts a Credential as being sufficient Evidence is referred to as a Relying Party. A Relying Party may have recourse against the issuer of the Credential, under consumer protection or contract law.

Objects, and many artefacts, do not act in the Real World, and most of those that do act are not trying to further their own interests. In contrast, job-applicants may make unjustified Property Assertions in relation to their qualifications, experience and previous employment. Their claims in relation to qualifications can be tested against a testamur or by look-up of an educational institution's database. To guard against masquerade, the association between the person and the qualification-evidence may also need to be tested.

Many Properties evidence complexity that needs to be reflected in multiple data-items and interpretation rules. An important kind of complex Property is the capacity to act on behalf of another party, i.e. as an agent for a principal. High-reliability authentication of this kind of Property Assertion is vital to commercial activities. Clarke (2023) describes how the Authentication of Property Assertions may or may not involve assurances relating to Identity.

On the basis of the author's decades of consultancy experience in this area, IS practice does not place sufficient emphasis on the Authentication of Property Assertions. IS theory needs to provide additional intellectual and practical tools to support practice.

5.3 Asset-Value Assertions

Commerce, whether electronic, mobile or entirely physical, depends on the reliable transfer of value to the seller, most commonly of money ("Any generally accepted medium of exchange which enables a society to trade goods without the need for barter", OED 1; "Means of payment considered as representing value or purchasing power", OED 2a). Hendershott et al. (2021) remark that "financial services are fundamentally about authenticating identity and value ..." (p.1).

Examples of Value Authentication for liquid assets include checking a banknote for forgery-resistant features, comparing a newly-executed written signature with one previously executed, checking the validity of a card-identifier (identifying a card, not a person) and a PIN (evidencing that the person presenting the card knows a 'secret' that the intended card-user should know and others should not), and receiving a message from a trusted third party stating that funds have been transferred from the sender's account to the recipient's account with a trusted third party. In the case of a blockchain-based digital currency, authentication depends on the receipt of an electronic message into an electronic currency wallet, together with confirmations of the transaction from multiple sources (Miscione et al. 2018).

Commerce also depends on confidence by each transacting party in the value of goods and services being offered by the other. The previous paragraphs dealt with transactions in which money is traded for money, e.g. depositing and withdrawing cash, and currency-conversion transactions. The other categories are a non-monetary tradable item traded for money, and barter transactions. Examples of

tradable items include consumer durables, livestock, artworks, motor vehicles and 'collectibles', but also invisibles such as shares, loan agreements, and insurance.

The Value Assertion is that the tradable item has economic value, or has Properties that underpin economic value. Examples of Authenticators applicable to Assertions relating to such tradable items include tickets for entry to entertainment venues (Huang et al. 2014), warranty cards for consumer durables, valuation reports in relation to real estate, inspectors' reports on livestock and breeding stock (Clarke & Jenkins 1993), and share registry entries. Chua et al. (2007) focus on Assertion unreliability as a basis for fraud in Internet auction spaces, and note the challenges involved in establishing "whether a stamp [that is being traded is] authentic or fake" (p.771).

In the case of valuable artworks, Authenticators are sought that document the work's origins, nature, provenance (in particular, chain of ownership), and current ownership. The preference is for a Credential from a highly-reputed intermediary (such as a document uttered on a company's letterhead, a physical signature, a company seal, or a digital signature). Ownership of some real estate assets and goods in transit by sea are attested to by a chain of contracts relating to transfers between successive owners (Karamitsos et al. 2018).

5.4 Content Integrity Assertions

Messages over wired and wireless telecommunications infrastructures involve risk of accidental corruption and of content compromise resulting in falsification. Beyond email and chat, this applies to downloads of documents, images, video-files, transactions and software. Authentication techniques include checks that the message-hashes are the same (NIST 2015). Mechanisms for software content integrity authentication may utilise encryption (Sander 2021), and, for transactions, encryption coupled with multiple, independent storage locations (Dai & Vasarhelyi 2017).

Those examples relate to the simple, syntactical aspects of content integrity, At the semantic level, a pattern of Assertion that arises frequently is:

> *A Real World Thing is reliably represented by an Abstract World Entity-Instance-Attribute-Value or an Entity-Record-Data-Item-Value*

Practical examples are 'This customer qualifies for a discount', and 'The number of Widgets Class A that we have in stock is 37, as recorded in the Current-Stock-Count Data-Item in the stock file'. The function of Authentication is to establish a degree of confidence in the reliability of such Assertions. 'This customer qualifies for a discount' might be accepted as legitimate because the customer's face is recognised at the checkout. Alternatively, it may be established at the Abstract-World level, entirely within the IS, because the customer logs in online and their profile has the loyalty-program indicator set, enabling the Assertion to be authenticated automatically.

It was noted earlier that the most critical kinds of Assertions are those that map between Real-World and Abstract-World elements. An Assertion such as 'We have 37 of that item in stock' may be accepted simply because the inventory IS is regarded as reliable, or (particularly if the stock-item in question is subject to pilfering or breakages) the bin-contents may be checked for at least rough equivalence with the number recorded in the stock-file. In the case of 'This customer qualifies for a discount', Data or a Credential can be sought from some external source to provide assurance that the claim is justifiable. All Assertions involve the provision of Data, and its quality is at issue when Assertions are evaluated. In relation to well-structured data, a framework for assessing quality was consolidated from the literature in Clarke (2016, pp.77-80).

Not all assertions are in terms readily relatable to structured data like loyalty-flags and stock-counts. Some depend on audio, image or video content. Many are expressed in text. Consider the notion of email authentication. This encompasses at least three distinct assertions: the identity of the sender and/or recipient, and content integrity firstly syntactically, and secondly at the semantic level.

The IS discipline has largely avoided authentication of textual, audio, image and video content at the semantic level, that is to say the assurance of the reliability of the message-content's expression or meaning. The contemporary world is adjusting from analogue to mostly-digital publication of those forms of information. Assertions of Fact are a major battleground, as evidenced by the prevalence of misinformation, propaganda, rumour-mongering, disinformation, 'false news', 'alternative facts', and hence 'fact checkers' and 'explainers'. The scope for the concoction of text, image, video and audio has exploded in the digital era, as has the capacity to massage, adapt and falsify information content. I contend that the authentication of Assertions of Fact is a new frontier that the IS discipline and profession must explore and conquer.

At this stage, there is a paucity of published IS research in these areas, but it is emergent. Ziolkowski et al. (2020) and Zhang et al. (2021) are concerned with the Authentication of documentary claims, by means of distributed mirroring using blockchains. Georgea et al. (2021) consider "originator authenticity" in the context of unmasking fake news. The focus of their study is the process of mitigation by "resistors", who "identify deceit and disinformation" (p.1080). The authors provide no clues as to what Authenticators to use to test the authenticity of either messagers or messages, but cite Duffy et al. (2020) and Torres et al. (2018). Far more contributions are needed in the area of authentication of the content integrity at the semantic level.

6 Implications and Conclusions

This paper has presented a generic theory of Authentication to support IS practice and practice-oriented research. It reflects a pragmatic metatheoretic model comprising assumptions about the Real World, and a two-layer view of the Abstract World. It defines Authentication as a process whereby a level of confidence is achieved in an Assertion. It provides a framework for the design of processes, with exemplars of its application, and articulates that framework by identifying and describing categories of Assertions that are relevant to IS design.

The generic theory of Authentication is relevant to IS practice, uses terms familiar to practitioners, is understandable by practitioners, and can provide guidance in relation to the design and refinement of business processes that perform Authentication. Among its important implications for practice is the focus on Assertions that are relevant to the need, whose reliability can provide the necessary assurance, and that can be the subject of practical, effective, efficient and inexpensive Authentication processes. It encompasses the Authentication of Assertions of (Id)Entity, but recognises the challenges, expense and intrusiveness inherent in that undertaking, and encourages IS designers to pause and consider whether other categories of Assertion are a more appropriate focus.

The theory has multiple implications for research. It outlines a large domain in which theory has been lacking. It identifies many sub-domains in which articulation of the theory is needed, which can contribute to more efficient and effective designs by IS practitioners. One important area of contribution is in formalisation of value-authentication, both in relation to assets designed for fungibility (i.e. cash and its proxies) and capital and consumer goods and services. In various circumstances, value authentication can be much less expensive, much quicker and much less intrusive than (id)entity authentication, The work presented here invites the development of contingency theories that define the circumstances under which each of the various categories of assertion needs to be prioritised for consideration by designers.

A further contribution of this theory is to point the way towards a new IS research domain: the authentication of the semantic content integrity of Assertions of Fact. The scope of IS was initially limited to relatively structured data, that is to say quantitative data, and qualitative data on ordinal scales. In addition to audio, image and video, IS now deals with a vast volume of highly unstructured text. Moreover, enormous concerns exist about misinformation and disinformation, and about the impacts of generative AI. The theory of authentication presented in this paper provides a springboard for IS practitioners and theorists to provide support to business, governments and societies in relation to the assessment of the reliability of information of all kinds.

7 References

Abbas R. & Michael K. (2022) 'Socio-Technical Theory: A review' In S. Papagiannidis (Ed), 'TheoryHub Book', TheoryHub, 2022

Achterkamp M.C. & Vos J.F.J. (2008) 'Investigating the Use of the Stakeholder Notion in Project Management Literature: A Meta-Analysis' Int'l Journal of Project Management 26 (2008) 749-757

ALRC (2010) 'Uniform Evidence Law' Australian Law Reform Commission, Report 102, August 2010

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

Baumer E.P.S. (2015) 'Usees' Proc. 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI'15), April 2015

Becker J. & Niehaves B. (2007) 'Epistemological perspectives on IS research: a framework for analysing and systematizing epistemological assumptions' Info Systems J 17 (2007) 197–214

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

Boell S. & Cecez-Kecmanovic D. (2015) 'What is an Information System?' Proc. 48th Hawaii Int'l Conf. on System Sciences, 2015, at http://bölls.de/publications/2015-HICSS-Boell,Cecez-Kecmanovic-What_is_an_IS.pdf

Boell S. K. (2017) 'Information: Fundamental positions and their implications for information systems research, education and practice' Information and Organization 27,1 (2017) 1-16

Clarke R. (1990) 'Information Systems: The Scope of the Domain' Xamax Consultancy Pty Ltd, 1990, at http://www.rogerclarke.com/SOS/ISDefn.html

Clarke R. (1992a) '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. (1992b) 'Fundamentals of 'Information Systems'' Xamax Consultancy Pty Ltd, September 1992, at http://www.rogerclarke.com/SOS/ISFundas.html

Clarke R. (2001) '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. (2003) '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 Consultancy Pty Ltd, , March 2004, ISBN 0-9589412-3-8, 66pp., at http://www.xamax.com.au/EC/IdMngt.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. (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) 'The Authentication of Assertions of (Id)Entity' Working Paper, Xamax Consultancy Pty Ltd, January 2023, at http://rogerclarke.com/ID/IEA.html

Clarke R. & Jenkins M. (1993) 'The Strategic Intent of On-Line Trading Systems : A Case Study in National Livestock Marketing' Journal of Strategic Information Systems 2,1 (March 1993) 57-76, PrePrint at http://www.rogerclarke.com/EC/CALM.html

Chua C.E.H., Wareham J. & Robey D. (2007) 'The Role of Online Trading Communities in Managing Internet Auction Fraud' MIS Quarterly 31,4 (December 2007) 759-781

Cuellar M.J. (2020) 'The Philosopher's Corner: Beyond Epistemology and Methodology - A Plea for a Disciplined Metatheoretical Pluralism' The DATABASE for Advances in Information Systems 51, 2 (May 2020) 101-112

Dai J. & Vasarhelyi M.A. (2017) 'Toward Blockchain-Based Accounting and Assurance' Journal of Information Systems 31,3 (Fall 2017) 5-21

Davis G.B. (1974) 'Management Information Systems: Conceptual Foundations, Structure, and Development' McGraw-Hill, 1974

Duffy A., Tandoc E. & Ling R. (2020) 'Too good to be true, too good not to share: the social utility of fake news' Information, Communication & Society 23,13 (2020) 1965-1979

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

Freeman R.E. & Reed D.L. (1983) 'Stockholders and Stakeholders: A New Perspective on Corporate Governance' California Management Review 25,3 (1983) 88-106

Georgea J., Gerhartb N. & Torresc R. (2021) 'Uncovering the Truth about Fake News: A Research Model Grounded in Multi-Disciplinary Literature' Journal Of Management Information Systems 38,4 (2021) 1067–1094

Gottwald S. (2001) 'A Treatise on Many-Valued Logics', January 2001

Hendershott T., Zhang X.M., Zhao J.L. & Zheng Z.E. (2021) 'FinTech as a Game Changer: Overview of Research Frontiers' Information Systems Research 32,1 (March 2021) 1–17

Hirschheim R. (2019) 'Against Theory: With Apologies to Feyerabend' Journal of the Association for Information Systems 20, 9 (2019) 1340-1357

Huang J., Newell S., Huang J., Pan S.-L. (2014) 'Site-shifting as the source of ambidexterity: Empirical insights from the field of ticketing' Journal of Strategic Information Systems 23 (2014) 29–44

IETF (2022) 'RFCs' Internet Engineering Task Force (IETF), December 2022

Karamitsos I., Papadaki M. & Al Barghuthi N.B. (2018) 'Design of the Blockchain Smart Contract: A Use Case for Real Estate' Journal of Information Security 9,3 (July 2018)

Lausen J., Clapham B., Siering M. & Gomber P. (2020) 'Who Is the Next 'Wolf of Wall Street'? Detection of Financial Intermediary Misconduct' Journal of the Assoc. for Information Systems 21, 5 (2020)

Magnusson A. (2022) 'The Definitive Guide to Authentication' Strong DM, September 2022

March S.T. & Allen G.N. (2014) 'Toward a Social Ontology for Conceptual Modeling' Commun. Assoc. for Infor. Syst. 34,70 (2014) 1347-1358

Mattke J., Maier C., Hund A. & Weitzel T. (2019) 'How an Enterprise Blockchain Application in the U.S. Pharmaceuticals Supply Chain is Saving Lives' MIS Quarterly Executive 18, 4 at 6

Miscione G., Ziolkowski R., Zavolokina L. & Schwabe G. (2018) 'Tribal Governance: The Business of Blockchain Authentication' Proc. Hawaii International Conference on System Sciences (HICSS-51), 3-6 January 2018

Mumford E. (2006) 'The story of socio-technical design: reflections on its successes, failures and potential' Info Systems J 16 (2006) 317–342

Myers M.D. (2018) 'The philosopher's corner: The value of philosophical debate: Paul Feyerabend and his relevance for IS research' The DATA BASE for Advances in Information Systems 49, 4 (November 2018) 11-14

Nickerson R.S. (1998) 'Confirmation Bias: A Ubiquitous Phenomenon in Many Guises' Review of General Psychology 2, 2 (1998)

NIST (2006) 'Minimum Security Requirements for Federal Information and Information Systems' Federal Information Processing Standard (FIPS) PUB 200, National Institute of Standards and Technology Gaithersburg, March 2006

NIST (2015) 'hashing' Computer Security Resource Center, [US] National Institute of Standards and Technology, 2015

Salop S.C. (2017) 'An Enquiry Meet for the Case: Decision Theory, Presumptions, and Evidentiary Burdens in Formulating Antitrust Legal Standards' Georgetown University Law Center, 2017

Sander R. (2021) 'What is a Code Signing Certificate? How does it work?' IEEE Comp. Soc., August 2021

Sarker S., Chatterjee S., Xiao X. & Elbanna A. (2019) 'The Sociotechnical Axis of Cohesion for the IS Discipline: Its Historical Legacy and its Continued Relevance' MIS Qtly 43, 3 (September 2019) 695-719

Stevens S.S. (1946) 'On the Theory of Scales of Measurement' Science 103, 2684 (7 June 1946)

Thomas D. & Negash S. (2023) 'Emerging Technology IS Course Design: Blockchain for Business Example' Communications of the Association for Information Systems, 52 (2023)

Torres R., Gerhart N. & Negahban A. (2018) 'Epistemology in the Era of Fake News: An Exploration of Information Verification Behaviors among Social Networking Site Users' ACM SIGMIS Database 49,3 (July 2018), 78–97

Zhang W., Wei C.-P., Jiang Q., Peng C.-H. & Zhao J.L. (2021) 'Beyond the Block: A Novel Blockchain-Based Technical Model for Long-Term Care Insurance' Journal Of Management Information Systems 38,2 (2021) 374–400

Ziolkowski R., Miscione G. & Schwabe G. (2020) 'Decision Problems in Blockchain Governance: Old Wine in New Bottles or Walking in Someone Else's Shoes?' Journal Of Management Information Systems 37,2 (2020) 316–348

Acknowledgements

This paper builds on a long series of refereed publications by the author on the topic of authentication, including Clarke (1994, 2003, 2009). The author acknowledges comments and questions of the reviewers of these previous papers, both formal and informal. In addition, the comments of the reviewers of the present paper provided valuable input,

Copyright © 2023 Roger Clarke. This is an open-access article licensed under a Creative Commons Attribution-Non-Commercial 3.0 Australia Licence, which permits non-commercial use, distribution, and reproduction in any medium, provided the original author and ACIS are credited.