12-2-2023

# A Generic Theory of Authorization to Support IS Practice and Research

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

# Access Control in the Era of Active Artefacts: A Generic Theory of Authorization 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

The term Authorization refers to a key element within the process whereby control is exercised over access to information and communications technology resources. It involves the assignment of a set of permissions or privileges to particular users, or categories of users. A description is provided of the conventional approach adopted to Authorization. The management of human users is still far from satisfactory, and devices and processes are posing additional challenges as they increasingly act directly on the real world. Applying a previously-published pragmatic metatheoretic model that provides a basis for information systems practice, this paper presents a generic theory of Authorization. The conventional approach to Authorization is re-examined in light of the new theory, weaknesses are identified, and improvements proposed.

**Keywords** Authorization, Enrolment, Authentication, Access Control

# 1 Introduction

Information and Communications Technology (ICT) facilities have become central to the activities not only of organisations, but also of communities, groups and individuals. The end-points of networks are pervasive, and so is the dependence of all parties on the resources that the facilities provide access to. ICT has also moved beyond the processing of data and its use of the production of information. Support for inferencing has become progressively more sophisticated, some forms of decision-making are being automated, and there is increasing delegation to artefacts of the scope for autonomous action in the real world. Humanity's increasing reliance on machine-readable data, on computer-based data processing, and on inferencing, decision and action, is giving rise to a high degree of vulnerability and fragility, because of the scope for misuse, interference, compromise and appropriation. There is accordingly a critical need for effective management of access to ICT-based facilities.

Conventional approaches within the ICT industry have emerged and matured over the last half-century. Terms in common usage in the area include identity management (IdM), identification, authentication, authorization and access control. The adequacy of current techniques has been in considerable doubt throughout the first two decades of the present century. A pandemic of data breaches has spawned notification obligations in many jurisdictions since the first Security Breach Notification Law was enacted in California in 2003 (Karyda & Mitrou 2016), and the resources of many organisations have proven to be susceptible to unauthorised access (ITG 2023).

I contend that many of the weaknesses in the relevant techniques arise from inadequacies in the conventional conception of the problem-domain, and in the models underlying architectural, infrastructural and procedural designs to support authorization. My motivation in conducting the research reported here has been to contribute to improved information systems (IS) practice and practice-oriented IS research. The method adopted is to identify and address key weaknesses, by applying and extending a previously-published pragmatic metatheoretic model.

The paper commences by reviewing the context and nature of the authorization process, within its broader context of identity management. This culminates in initial observations on issues that are relevant to the vulnerability to unauthorised access. An outline is then provided of a pragmatic metatheoretic model, highlighting the aspects of relevance to the analysis. A generic theory of authorization is proposed, which reflects the insights of the model. This lays the foundations for adaptations to IS theory and practice in all aspects of identity management, including identification and authentication, with particular emphasis in this paper placed on authorization and access control. That theory is then used as a lens whereby weaknesses in conventional authorization theory and practice can be identified and articulated.

# 2 The Conventional Approach to Authorization

A dictionary definition of authorization is "The action of authorizing a person or thing ..." (OED 1); and authorize means "To give official permission for or formal approval to (an action, undertaking, etc.); to approve, sanction" (OED 3a) or "To give (a person or agent) legal or formal authority (to do something); to give formal permission to; to empower" (OED 3b).

The remainder of this section outlines conventional usage of the term within the ICT industry, with an emphasis on the underpinnings provided by industry standards organisations, clarifies several aspects of those standards, and summarises the various approaches in current use.

## 2.1 ICT Industry Definitions

The authorization notion was first applied to computers, data communications and IS in the 1960s. It has of course developed considerably since then, both deepening and passing through multiple phases. However it has mostly been treated as being synonymous with the selective restriction of access to a resource, an idea usefully referred to as 'access control'. Originally, the resource being accessed was conceived as a physical area such as enclosed land, a building or a room; but, in the context of ICT, a resource is data, software, a device or a communications link.

The following quotations and paraphrases provide short statements about the nature of the concept as it has been practised in ICT during the period c.1970 to 2020:

> *Authorization is a process for granting approval to a system entity to access a system resource (RFC4949 2007, at 1b(I), p.29)*
>
> *Access control or authorization ... is the decision to permit or deny a subject access to system objects (network, data, application, service, etc.) (NIST800-162 2014, p.2)*

Josang (2017, pp.135-142) draws attention to ambiguities in mainstream definitions in all of the ISO/IEC 27000 series, the X.800 Security Architecture, and the NIST Guide to Attribute Based Access Control (ABAC). To overcome the problems, he distinguishes between:

- Authorization as the specification of access policies (p.137); and
- Access control as the application and enforcement of those access policies.

In standards documents, the terms 'subject' and 'system resource / object' are intentionally generic. NIST800-162 (2014, p.3) refers to an 'object' as "an entity to be protected from unauthorized use" . Examples of IS resources referred to in that document include "a file" (p.vii), "network, data, application, service" (p.2), "devices, files, records, tables, processes, programs, networks, or domains containing or receiving information; ... anything upon which an operation may be performed by a subject including data, applications, services, devices, and networks" (p.7), "documents" (p.9), and "operating systems, applications, data services, and database management systems" (p.20). For the present purposes 'actor' and 'IS resource' better convey the scope, and are adopted in this paper. Drawing on NIST800-162 (2014, pp.2-3):

> ***Actor*** *means any Real-World Thing capable of action on an IS Resource, including humans and some categories of artefact*
>
> ***IS Resource*** *means Data or a Process in the Abstract World, that an IS is capable of acting upon*

Permissions declare allowed actions by an Actor. (NIST uses the terms privileges and authorizations, and IETF uses the term authorizations). These are defined by an authority and embodied in policy or rules. In IETF's RFC4949 (2007), for example, a permission is "An approval that is granted to [an Actor] to access [an IS Resource]" (1a(I)). "... "The semantics and granularity of [permissions] depend on the application and implementation ... [A permission] may specify a particular access mode -- such as read, write, or execute -- for one or more system resources" (p.29).

The following are adopted as working definitions of the key terms, for refinement at a later stage in this paper:

> ***Authorization*** *is the process whereby a decision is made to declare that an Actor has Permission to perform an action on an IS Resource. The result of an Authorization process is a statement of the following form: <An Actor> has one or more <Permissions> in relation to <an IS Resource>*
>
> ***Access Control*** *is the process whereby (a) means are provided to enable an authorized Actor to exercise their Permissions, and (b) unauthorised Actors are precluded from doing so*
>
> ***Permission*** *means an entitlement or authority to be provided with the capability to perform a particular act in relation to a particular IS Resource*

Actions may take the form of operations on Data, in particular data access, data input, data amendment, data deletion, data processing, or data inferencing; or the triggering of a process in relation to IS Resources.

## 2.2 The Broad Field of Identity Management

Authorization processes depend on reliable information. Identity Management (IdM) and Identity and Access Management (IAM) are ICT-industry terms for frameworks comprising architecture, infrastructure and processes that enable the management of user identification, authentication, authorization and access control processes. IdM was an active area of development c.2000-05, and has been the subject of a considerable amount of standarisation, in particular in the ISO/IEC 24760 series (originally of 2011, completed by 2019). A definition provided by the Gartner consultancy is:

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

The process flow specified by NIST (2017, p.10) is in Appendix A, at Fig. A1. This is insufficiently precise to ensure effective and consistent application. Josang (2017, p.137, Fig. 1) provides a better-articulated overview of the functions, reproduced in Fig. A2. This distinguishes the configuration (or establishment) phase from the operational activities of each of Identification, Authentication and Access. This is complemented by a mainstream scenario (Josang 2017, p.143, Fig. 2) that illustrates the practical application of the concepts and is reproduced in Fig. A3.

The IdM industry long had a fixation on public key encryption, and particularly X.509 digital certificates. This grew out of single-signon facilities for multiple services within a single organisation, with the approach then being generalised to serve the needs of multiple organisations. The inadequacies of monolithic schemes gave way to federation across diverse schemes by means of common message standards and transmission protocols. Multiple alternative approaches are adopted on the supply side (Josang & Pope 2005). These are complemented and challenged by approaches on the demand-side that reject the dominance of the interests of corporations and government agencies and seek to also protect the interests of users. These include user-selected intermediaries, own-device as identity manager, and nymity services (Clarke 2004).

The explosion in user-devices (desktops from c.1980, laptops from c.1990, mobile-phones from 2007 and tablets from 2010) has resulted in the present context in which two separate but interacting processes are commonly involved. Individuals authenticate locally to their personal device using any of several techniques designed for that purpose; and the device authenticates itself to the targeted service(s) through a federated, cryptography-based scheme (FIDO 2022). The Identity Management model is revisited in the later sections of this paper.

## 2.3 Families of Authorization Models

Whether a request is granted or denied is determined by an authority. In doing so, the authority applies decision criteria. From the 1960s onwards, a concept of Mandatory Access Control (MAC) has existed, originating within the US Department of Defense. Instances of data are assigned a security-level, each user is assigned a security-clearance-level, and processes are put in place whose purposes are to enable user access to data for which they have a requisite clearance-level, and to disable access in relation to all other data. The security-level notion is not an effective mechanism for IS generally. Instead, the criteria may be based on any of the following (with particular models of Access Control listed for each of the alternatives, and outlined below):

- the identity of the actor (DAC, IBAC);
- the role performed by the actor (RBAC);
- attribute(s) of the actor, of the IS Resource, and/or of environmental variables (ABAC); or
- the task being performed (TBAC).

An early approach of general application was Discretionary Access Control (DAC). DAC matured into Identity Based Access Control (IBAC), with access control lists (ACLs) identifying which Actors are allowed to access which IS Resources. IBAC remains much-used. It scales poorly, however, and from 1992-96 onwards, Role Based Access Control (RBAC), became mainstream in large systems (Pernul 1995, Sandhu et al. 1996, Lupu & Sloman 1997, ANSI 2012). Each user's Permissions are based on a role they are assigned to. This offers efficiencies. See also ISO 22600 Parts 1 and 2 (2014).

To address weaknesses of RBAC, Attribute Based Access Control (ABAC) emerged from c.2000 (Li et al. 2002). This grants or denies user requests based on attributes of the subject and/or object, together with relevant environmental conditions. NIST800-162 provides, as examples of attributes of Actors, "name, unique identifier, role, clearance" (p.11), and "current tasking, physical location, and the device from which a request is sent" (p.23). Examples of IS Resource attributes include "document ... title, ... date of last edit, ... owning organization ..." (p.9). Environmental conditions include "current date, time, location, ... system status" (pp.24, 29). Task-Based Access Control (TBAC) associates permissions with a task, e.g. a case-number or incident-report identifier. See (Thomas & Sandhu 1997, Fischer-Huebner 2001, p.160), but appears to have achieved very limited adoption.

The next section outlines an abstract model that has been devised to support IS practice and practice-oriented IS research. The following section extends the model to the field of Authorization.

# 3 The Pragmatic Metatheoretic Model

In previously-published work (Clarke 2021, 2022, 2023a, 2023b), a model is proposed that reflects the viewpoint adopted by IS practitioners, and is designed to support understanding of and improvements to IS practice and practice-oriented IS research. The model embodies the socio-technical system view, whereby organisations are recognised as comprising people using technology, each affecting the other, with effective design depending on integration of the two. The model is '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. It is also 'metatheoretic' (Myers 2018, Cuellar 2020), on the basis that it builds on a working set of assumptions in each of the areas of ontology, epistemology and axiology.

As depicted in Figure 1, the Pragmatic Metatheoretical Model (PMM) 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. Abstract Worlds are depicted at two levels. The Conceptual Model level reflects the modeller's perception of Real-World Phenomena, with the notions of Entity and Identity corresponding to the category Things, and Transaction to the category Events. Authentication processes assess the reliability of the model's reflection of reality.

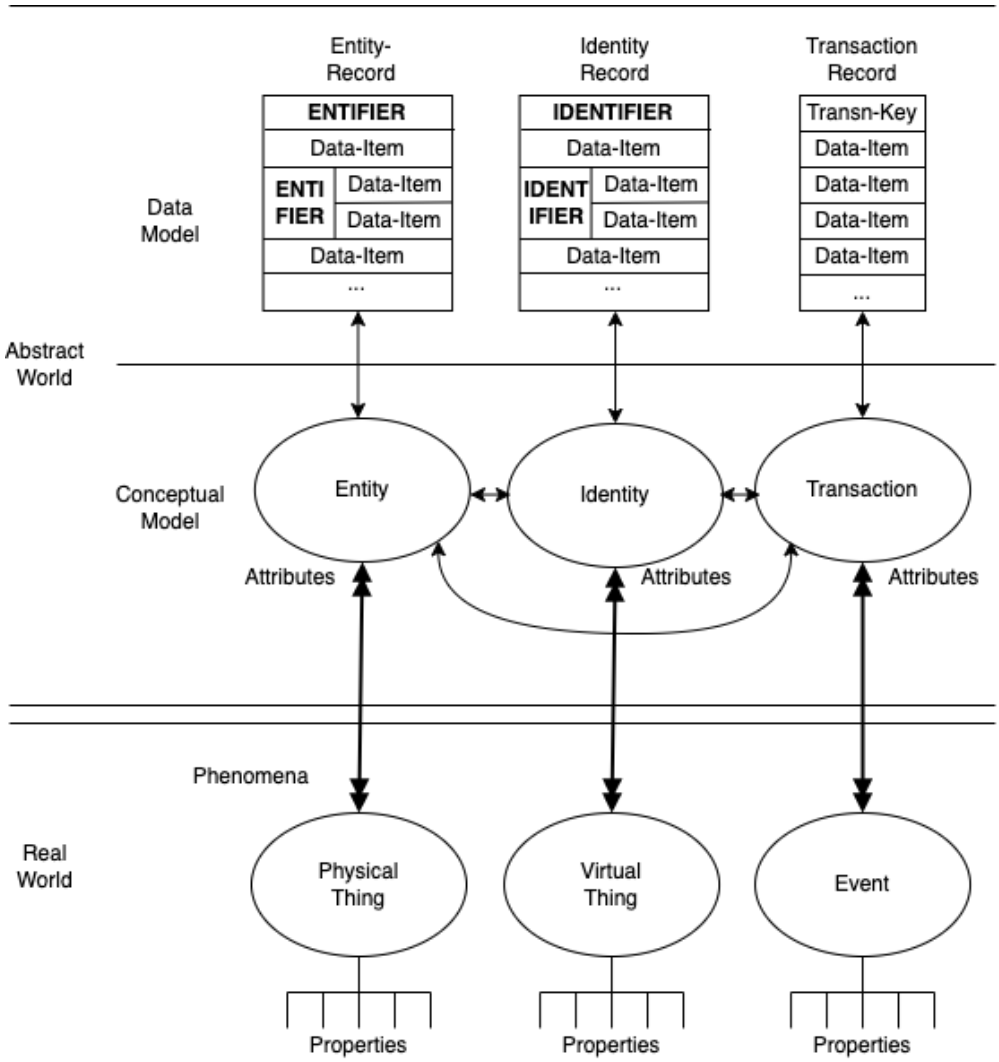


*Figure 1: A Pragmatic Metatheoretical Model (PMM)*

A vital aspect of the model is the distinction between Entity and Identity. An Entity corresponds with a Physical Thing. An Identity, on the other hand, corresponds to a Virtual Thing, which is a particular presentation of a Physical Thing, most commonly when it performs a particular role, or adopts a particular pattern of behaviour. For example, the NIST (2006) definition of Authentication

distinguishes a "device" (in the terms of this model, an Entity) from a "process" (an Identity), and the Gartner definition of IdM refers to "a digital representation [an Identity] of a user [an Entity]". An Entity may adopt one Identity in respect of each role it performs, or it may use the same Identity when performing multiple roles. For example, within a corporation, over time, different human Entity-Instances adopt the Identity of CEO, whereas the Identity of Company Director is adopted by multiple human Entity-Instances at the same time, each of them being an Identity-Instance.

The Data Model Level enables the operationalisation of the relatively abstract ideas in the Conceptual Model level through data management techniques and tools that support organised activity. The PMM uses the term Information specifically for a sub-set of Data: that Data that has value (Davis 1974, p.32, Clarke 1992, 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. Assertions are putative expressions of knowledge about one of more elements of the metatheoretic model.

The basic PMM was extended in Clarke (2022), by refining the Data Model notion of Record-Key to distinguish two further concepts: Identifiers as Record-Keys for Identities (corresponding to Virtual Things in the Real World), and Entifiers as Record-Keys for Entities (corresponding to Physical Things). A computer is an Entity, for which a Processor-ID may exist, failing which its Entifier may be a proxy, such as a the Network Interface Card Identifier (NIC ID) of, say, an installed Ethernet card, or its IP-Address. A process is an Identity, for which a suitable Identifier is a Process-ID, or a proxy such as its IP-Address concatenated with its Port-Number. For human Entities, the primary form of Entifier is a biometric, although the Processor-ID of an embedded chip is another possibility (Clarke 1994 p.31, Michael & Michael 2014). For Identities (whether used by a human or an artefact), a UserID or LoginID is a widely-used proxy Identifier.

This leads to distinctions between Identification processes, which involve the provision or acquisition of an Identifier, and Entification processes, for which an Entifier is needed. The acquired (Id)Entifier can then be used as the Record-Key for a new Data-Record, or as the means whereby the (Id)Entity can be associated with a particular, already-existing (Id)Entity-Record. The terms 'Entifier' and 'Entification' are uncommon, but have been used by the author since 2001 and applied in about 25 articles within the Google Scholar catchment, which together have over 400 citations.

Two further papers extend the PMM in relation to Authentication. In Clarke (2023a), it is argued that the concept needs to encompass Assertions of all kinds, rather than just Assertions involving (Id)Entity. That paper presents a Generic Theory of Authentication (GTA), defining it as a process that establishes a degree of confidence in the reliability of an Assertion, based on Evidence.

The second of those papers, Clarke (2023b), defines an Assertion of (Id)Entity as a claim that a particular (Virtual or Physical) Thing is appropriately associated with one or more (Id)Entity-Records. An Assertion of (Id)Entity is subjected to (Id)Entity Authentication processes, in order to establish the reliability of the claim. Also of relevance is the concept of a Property Assertion, whereby a particular Data-Item-Value in a particular (Id)Entity Record is claimed to be appropriately associated with, and to reliably represent, a particular Property of a particular (Virtual or Physical) Thing. Properties, and (Id)Entity Attributes represented by Data-Items, are of many kinds. One of especial importance in commercial transactions is an Assertion of a Principal-Agent Relationship, whereby a claim is made that a particular Thing has the authority to act on behalf of another particular Thing. An agent may be a Physical Thing (a person or a device), or a Virtual Thing (a person currently performing a particular role, or a computer process).

The theory reviewed in this section is extended in the following section to encompass Authorization, in order to lay the foundation for an assessment of the suitability of the conventional approaches to Authorization described earlier in this paper.

# 4 A Generic Theory of Authorization (GTAz)

This section presents a new Generic Theory of Authorization (GTAz), places it within the context of (Id)Entity Management (IdEM), and shows its relationships with the various other processes that make up the whole. The Theory applies the Pragmatic Metatheoretic Model (PMM) and the Generic Theory of Authentication (GTA), outlined above.

It is first necessary to present a generic process model of (Id)Entity Management as a whole, and define terminology in a manner consistent with the PMM and GTA. Wherever practicable, conventional terms and conventional definitions are adopted, or at least elements of conventional

definitions. However, the conventional model contains ambiguities, inconsistencies, and poor mappings to the Real World, all of which need to be avoided. As a result, many definitions and some terms are materially different from current industry norms and the current Standards documents.

## 4.1 (Id)Entity Management (IdEM)

Josang's (2017) Phase Model was reproduced in the Appendix, as Figure A2. In Figure 2 below, Josang's Model is further refined, to provide a diagrammatic overview of the field as a whole, for which the overarching term (Id)Entity Management is used, and within which Registration and Operational Phases are distinguished.

> ***(Id)Entity Management (IdEM)*** *means the architecture, infrastructure and processes whereby access to IS Resources is enabled for appropriate users, and otherwise denied*

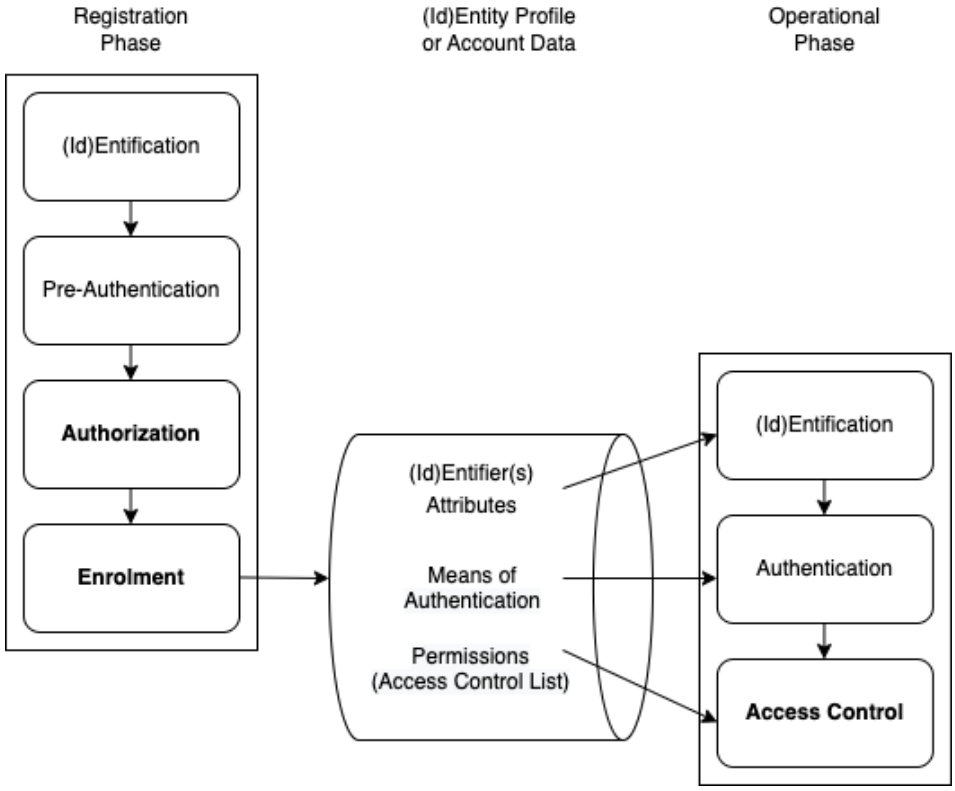


*Figure 2: A Generic Process Model of (Id)Entity Management (IdEM)*

The **Registration Phase** comprises:

- an (Id)Entification Process, in which Assertions are made, at least of (Id)Entity and of the appropriateness of providing that (Id)Entity with access to IS Resources;
- a Pre-Authentication Process, in which Evidence is acquired and evaluated, in order to assess the degree of confidence in the reliability of the Assertions;
- an **Authorization** Process, in which decision criteria are applied in order to determine what Permissions are to be made available to the (Id)Entity; and
- an Enrolment Process, in which Data is recorded to enable the Operational Phase to be conducted in an effective and efficient manner.

The **Operational Phase** comprises:

- an (Id)Entification Process, in which an Assertion of (Id)Entity is made, to the effect that the Entity (person or device) is the or an appropriate one to operate as that (Id)Entity;
- an Authentication Process, which utilises the recorded Means of Authentication to assess the degree of confidence in the reliability of that Assertion; and
- an **Access Control** process, which utilises previously recorded Permissions to establish a Session that enables an authorized user to exercise the appropriate Permissions.

The GTA outlined above explains the terms relevant to the first two of the four steps of the Registration Phase. Definitions of these terms are presented in Appendix B, including for the steps of (Id)Entification and Pre-Authentication, and for the supporting terms Evidence, Evidence of (Id)Entity, Authenticator, Credential, Token and Relying Party.

## 4.2 The Authorization and Enrolment Steps

The third step of the Registration Phase depicted in Figure 2, Authorization, is the primary focus of this paper. Adopting the modified definitions in the IETF and NIST standards proposed in Josang (2017), a clear distinction is drawn between the Authorization process (discussed in this section) and Access Control (discussed in the following section). The following is a refinement of the working definition presented earlier in this paper:

> ***Authorization*** *means a process whereby an Authorization Authority decides whether or not to declare that an Actor has one or more Permissions in relation to a particular IS Resource. A Permission may be specific to an Actor, or the Actor may be assigned to a previously-defined Role and inherit Permissions associated with that Role*
>
> ***Authorization Authority*** *means an Entity with legal or practical power (de juré or de facto) to determine whether and what Permissions a particular Actor has in relation to a particular IS Resource*
>
> ***Role*** *means a coherent pattern of behaviour performed in a particular context*

Categories of Role include:

- A job-description or appointment (CEO, call-centre operator, Company Director);
- An organisational function (fire warden, member of an appointment committee); and
- An external user, whether in another organisation or in a less formal setting (customer, applicant, enquirer, incident-reporter, consumer advocate, association meeting chair).

The operator of an Information System, as principal, or the operator of an (Id)Entity Management service acting as an agent for a principal, is generally assumed to be the Authorization Authority. Many other possibilities exist, however, such as a regulatory agency, a professional registration board, and an individual to whom personal data relates.

Actor was earlier defined to mean any Physical Thing or Virtual Thing capable of action on an IS Resource. Actors may take various forms. Many are human Entities, and many others are Identities intended for adoption by a human person. Others are human-made Entities, commonly referred to as artefacts, and Identities adopted by an artefact, such as a process running in computer. Another category is a legal person, by which is meant a virtual entity with no corporeal existence, such as an incorporated company or association, or a government agency.

An Actor needs the capability to perform actions in relation to IS Resources, or an agent that can do so on the Actor's behalf. Many artefacts lack suitable actuators, but devices are increasingly being provided with capacity to act in the real world. Legal persons such as corporations, associations and trusts have no capacity to act, and depend on agents acting on their behalf.

Generally, an Actor can perform as principal, or as an agent for a principal or for another agent. A qualification to this relates to artefacts and processes running in artefacts. Legal regimes generally preclude artefacts from bearing responsibility for actions and outcomes, and in particular they cannot be subject to provisions of the criminal law or bound by contract. Artefacts can be a tool for a human Actor or a legal person, but cannot act as principal where an action on an IS resource involves legal consequences, such as responsibility for due care, or liability for harm arising from an action.

IS Resource was earlier defined as Data or a Process in the Abstract World, that is capable of being acted upon. An IS Resource may be defined at various levels of granularity. In particular, Data may be defined as one or more data-holding(s), database(s), data-file(s), data-record(s), data-item(s) or document(s); and a Process may be defined as one or more service(s), application(s), function(s), program(s), transaction(s) or action-capability/ies.

The final step of the Registration Phase establishes the context in which the subsequent Operational Phase can be effectively but also efficiently performed:

> ***Enrolment*** *means a process that records Data to facilitate the performance of the Operational Phase of (Id)Entity Management*

> ***Account*** *means the data-holdings or profile associated with an Actor or (Id)Entity-Instance for which an Authorization process has created a Permission*

Depending on the approach adopted, the Enrolment process may need to perform some additional functions, such as the allocation of an Identifier, or the creation of an Authenticator.

## 4.3 The Operational Phase

The Registration Phase paves the way for Actors to be given powers to act, which are encapsulated in the entitlement called a Permission. The Operational Phase may be instigated at any time after Registration is complete, and as many times and as frequently as suits the circumstances. The first step in the Operational Phase, (Id)Entification, exhibits no material differences from the first step in the Registration Phase. The second step, Authentication, differs sufficiently from the Pre-Authentication process during the Registration Phase that a separate definition is needed:

> ***Authentication*** *means a process that evaluates Evidence in order to establish a degree of confidence in the reliability of an (Id)Entity Assertion, such as one communicated as part of a Login process*

The Authenticator(s) used in the Operational Phase may be the same as one or more of those used in the Pre-Authentication step of the Registration Phase. More commonly, however, an arrangement is implemented to achieve operational efficiency and user convenience. One approach of long standing is for a 'shared secret' (password, PIN, passphrase, etc.) to be nominated by the user, or provided to the user by the operator. Another mechanism is a one-time password (OTP) sent to the user when needed, via a separate and previously-agreed communications channel. A currently mainstream approach involves a one-time password generator installed on the user's device(s), or posted to them.

The third step, Access Control, is then able to be defined in a straightforward manner, as an element within the overall IdEM framework:

> ***Access Control*** *means a process that utilises previously recorded Permissions to establish a Session that enables a User to exercise the appropriate Permissions*
>
> ***Login*** *means a process whereby an Actor communicates a request to exercise Permissions that have been granted to a particular (Id)Entity, which triggers an Authentication process, and, if successful, an Access Control process*
>
> ***Session*** *means a period of time during which an authenticated Actor is able to exercise its Permissions in relation to IS Resources*
>
> ***User*** *means an authenticated (Id)Entity, commonly with an (Id)Entifier referred to as a userid, loginid or username, that is provided with the ability to utilise its Permissions to perform particular actions in relation to particular IS Resources*
>
> ***End User*** *means a User that is provided Permissions for application purposes*
>
> ***System User*** *means a User that is provided Permissions for system management purposes*

This section has applied and extended the Pragmatic Metatheoretic Model (PMM) and the Generic Theory of Authentication (GTA), in order to express a Generic Theory of Authorization (GTAz) intended to assist in IS practice and practice-oriented IS research.

# 5 Implications for Theory and Practice

This section applies GTAz as a lens through which to observe conventional approaches to authorization, and IdM more generally, and identify implications of the GTAz for theory and practice.

The first contribution of this work has been in the area of architecture and process flow. Depictions of conventional authorization theory exhibit many variants and inconsistencies. This unstable base results in very different renditions among Standards, text-books, the various models presented by consultancy firms, the various products and services, and the practices of various organisations. The GTAz model presented in Figure 2 separates the phases and steps, applies intuitive terms to them, defines all terms, and clarifies the categories of data necessary to enable the operational steps.

A second important feature of this work is the provision of clarity about Real-World Things. The distinction between an Entity, which models a Physical Thing, and an Identity, modelling a Virtual Thing, can be found in conventional theory and practice. However, even schemes that recognise the differences fail to express them clearly and/or fail to reflect the differences in their designs. Standards documents are particularly confused and confusing, including IETF (2007), ISO 24760-1 and NIST-800-63-3. Details are in Appendix C. The GTAz presented in this paper avoids or manages these problems. It thereby provides insights into how products and services developed using conventional approaches might be adapted to overcome those problems.

This work also actively avoids the assumption of accessible truth, and deprecates terms that derive from it, such as 'verification', 'proof' and 'correctness'. ISO 24760-1 uses inconsistent language, such as that authentication involves tests "to *determine [their correctness]*, **with the required level of assurance**" (p.3, emphasis added). The resultant ambiguities sow seeds of doubt, and cause confusions. The Generic Theory advanced in this work instead reflects real world complexities and uncertainties by building the definitions around the degree of confidence in the reliability of assertions.

The fourth area in which the Generic Theory embodies improvements is in relation to Roles and Attributes. RBAC was conceived at a time when most IS operated inside organisational boundaries, and the Standards are based on the assumptions that role means "a job function or employment position" (IETF, p.254), and that individuals have precisely one role. The GTAz presented here makes clear that Roles, and associated Identities, are relative to an IS, that they are not limited to organisational positions, and that individuals commonly perform many of them. It also enables consideration of Permissions being affected by Actors' Attributes and environmental factors. Further, it encompasses task-based approaches, such as Users declaring the reason for each exercise of a Permission, e.g. by cross-referencing to it a Case-Number, Email-Id, or other reference-number to a formal organisational register. A sufficiently rich log enables log-analysis to be undertaken, anomalies investigated, corrective action taken, and sanctions for misuse applied. Awareness by Actors that this is the case also acts as a substantial brake on the abuse of privileges.

A fifth area of contribution of the GTAz model is in the area of operational efficiency. Conventional approaches are resource-intensive, challenging to implement reliably, and intrusive and expensive. They encourage disaffected users to adopt countermeasures. GTAz encourages the evaluation of what Assertions need to be authenticated in order to satisfy the organisation's needs, and the development of a cost-effective strategy to manage the risks the organisation faces. Another facet is the volume of sensitive data involved in conventional IDM schemes. This is being increasingly perceived as a liability rather than as an asset. The GTAz approach leads to more sparing and targeted data collection and retention practices, reflecting both the 'data as asset' and 'data as liability' / 'toxic data' perspectives.

This section has identified weaknesses of conventional approaches to Identity Management (IdM) that are addressed by the IdEM framework presented in this paper. As a critical element within IdEM, the Generic Theory of Authorization (GTAz) enables the muddiness of thinking in existing theory to be identified and explained, avoids or resolves those confusions, and guides designers away from inappropriate designs and towards more suitable approaches to the field.

# 6 Conclusions

The purpose of the research reported in this paper was to contribute to improved IS practice and practice-oriented IS research in relation to the authorization process, within its broader context of identity management. The analysis has demonstrated that conventional theory relating to Identity Management (IdM) embodies inadequate modelling of the relevant real-world phenomena, internal inconsistencies, unhelpful terms, and confused definitions. It has demonstrated that by extending a previously-published pragmatic metatheoretic model (PMM), those inadequacies and inconsistencies can be overcome.

The practice of IdM since 2000 has been undermined by the many flaws in the underlying theory. The replacement IdEM framework defined in this paper provides the opportunity to review existing practices and designs and consider adaptations to address their weaknesses. To the extent that practices and designs are not capable of adaptation, the replacement theory supports the alternative approach of quickly and cleanly conceiving and implementing replacement products and services. This signals the need for wholesale replacement of defective Standards, both internationally (ISO/IEC) and nationally (e.g. NIST, FIPS 2022).

The benefits of substantial changes in this field would accrue to all stakeholders. Organisations can achieve greater effectiveness in their operations, and better manage business risks, and can do so in an efficient manner, by authenticating the assertions that actually matter. For this to be achieved, this research needs to be applied in the field, and the theory used as a lens by theorists, standards-producers, public policy organisations, designers and service-providers.

# 7 References

ANSI (2012) 'Information Technology - Role Based Access Control' INCITS 359-2012, American National Standards Institute, 2012

Clarke R. (1992) 'Practicalities of Keeping Confidential Information on a Database With Multiple Points of Access: Technological and Organisational Measures' Invited Paper for a Seminar of the Independent Commission Against Corruption (ICAC) of the State of N.S.W. on 'Just Trade? A Seminar on Unauthorised Release of Government Information', Sydney Opera House, 12 October 1992, at http://rogerclarke.com/DV/PaperICAC.html

Clarke R. (1994) 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' Information Technology & People 7,4 (December 1994) 6-37, PrePrint at http://www.rogerclarke.com/DV/HumanID.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. (2021) 'A Platform for a Pragmatic Metatheoretic Model for Information Systems Practice and Research' Proc. Austral. Conf. Infor. Syst, December 2021, PrePrint at http://rogerclarke.com/ID/PMM.html

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

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

Clarke R. (2023b) 'The Authentication of Assertions Relating to (Id)Entity' Working Paper, Xamax Consultancy Pty Ltd, March 2023, at http://rogerclarke.com/ID/IEA.html

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

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

FIDO (2022) 'User Authentication Specifications Overview' FIDO Alliance, 8 December 2022, at https://fidoalliance.org/specifications/

FIPS-201-3 (2022) 'Personal Identity Verification (PIV) of Federal Employees and Contractors' [US] Federal Information Processing Standards, January 2022, at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf

Fischer-Huebner S. (2001) 'IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms' LNCS Vol. 1958, Springer, 2001, at https://link.springer.com/content/pdf/10.1007/3-540-45150-1.pdf?pdf=button

IETF (2007) 'Internet Security Glossary ' Internet Engineering Task Force, RFC 4949, Version 2, August 2007, at https://tools.ietf.org/html/rfc4949

ISO 22600-1:2014 'Health informatics — Privilege management and access control — Part 1: Overview and policy management' International Standards Organisation TC 215 Health informatics

ISO 22600-2:2014 'Health informatics — Privilege management and access control — Part 2: Formal models' International Standards Organisation TC 215 Health informatics

ISO/IEC 24760-1 (2019) 'A Framework for Identity Management – Part 1: Terminology and concepts' International Standards Organisation SC27 IT Security techniques

ISO/IEC 24760-2 (2017) 'A Framework for Identity Management – Part 2: Reference architecture and requirements' International Standards Organisation SC27 IT Security techniques

ISO/IEC 24760-3 (2019) 'A Framework for Identity Management – Part 3: Practice' International Standards Organisation SC27 IT Security techniques

ITG (2023) 'List of Data Breaches and Cyber Attacks' IT Governance Blog, monthly, at https://www.itgovernance.co.uk/blog/category/monthly-data-breaches-and-cyber-attacks

Josang A. (2017) 'A Consistent Definition of Authorization' Proc. Int'l Wksp on Security and Trust Management, 2017, pp 134–144

Josang A. & Pope S. (2005) 'User Centric Identity Management' Proc. Conf. AusCERT, 2005

Karyda M. & Mitrou L. (2016) 'Data Breach Notification: Issues and Challenges for Security Management' Proc. 10th Mediterranean Conf. on Infor. Syst., Cyprus, September 2016

Li N., Mitchell J.C. & Winsborough W.H. (2002) 'Design of a Role-based Trust-management Framework' IEEE Symposium on Security and Privacy, May 2002, pp.1-17

Lupu E. & Sloman M. (1997) 'Reconciling Role Based Management and Role Based Access Control' Proc. ACM/NIST Workshop on Role Based Access Control, 1997, pp.135-141

Michael M.G. & Michael K. (2014) 'Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies' IGI Global, 2014

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 Infor. Syst. 49, 4 (November 2018) 11-14

NIST800-63-3 (2017) 'Digital Identity Guidelines' National Institute of Standards and Technology, 2017, at https://doi.org/10.6028/NIST.SP.800-63-3

NIST800-162 (2014) 'Guide to Attribute Based Access Control (ABAC) Definition and Considerations' NIST Special Publication 800-162, National Institute of Standards and Technology, updated to February 2019, at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

Pernul G. (1995) 'Information Systems Security – Scope, State-of-the-art and Evaluation of Techniques' International Journal of Information Management 15,3 (1995) 165-180

RFC4949 (2007) 'Internet Security Glossary, Version 2' Internet Engineering Task Force, FYI: 36

Sandhu R.S., Coyne E.J., Feinstein H.L. & Youman C.E. (1996) 'Role-Based Access Control Models' IEEE Computer 29,2 (February 1996) 38-47

Thomas R.K. & Sandhu R.S. (1997) 'Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management' Proc. IFIP WG11.3 Workshop on Database Security, Lake Tahoe Cal., August 1997, at https://profsandhu.com/confrnc/ifip/i97tbac.pdf

# Appendix A: Conventional Identity Management Frameworks

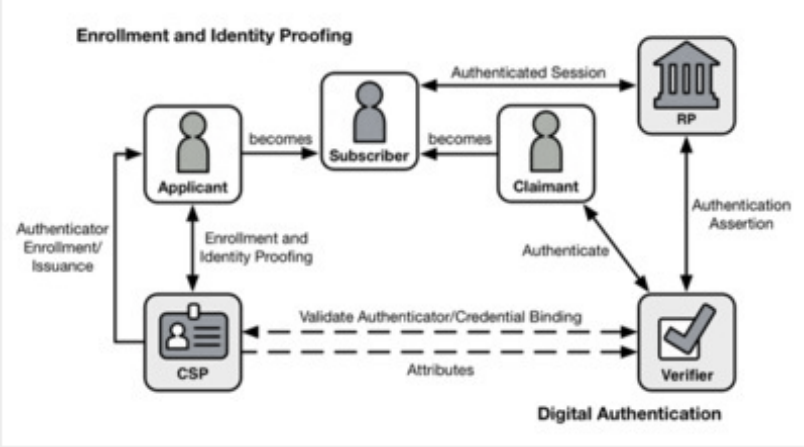


*Figure A1: NIST's Digital Identity Model*
Extracted from NIST-800-63-3 2017 (p.10)

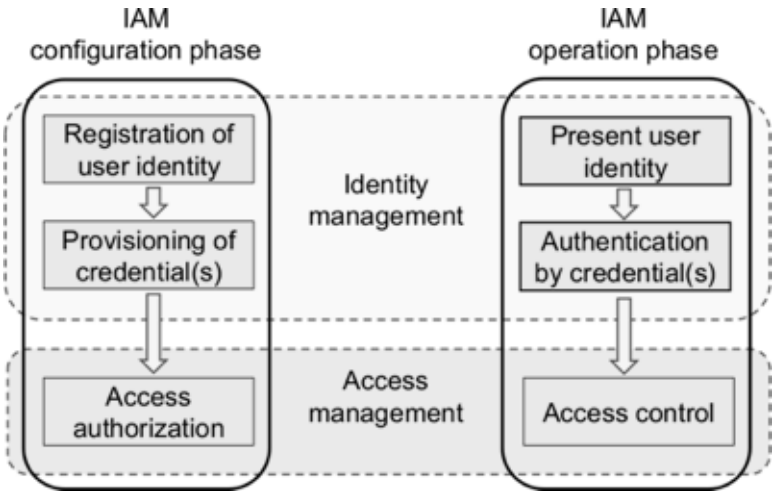


*Figure A2: Phase Model of Identity Management*
Extracted from https://en.wikipedia.org/wiki/File:Fig-IAM-phases.png
See also Josang (2017, p.137), Fig. 1

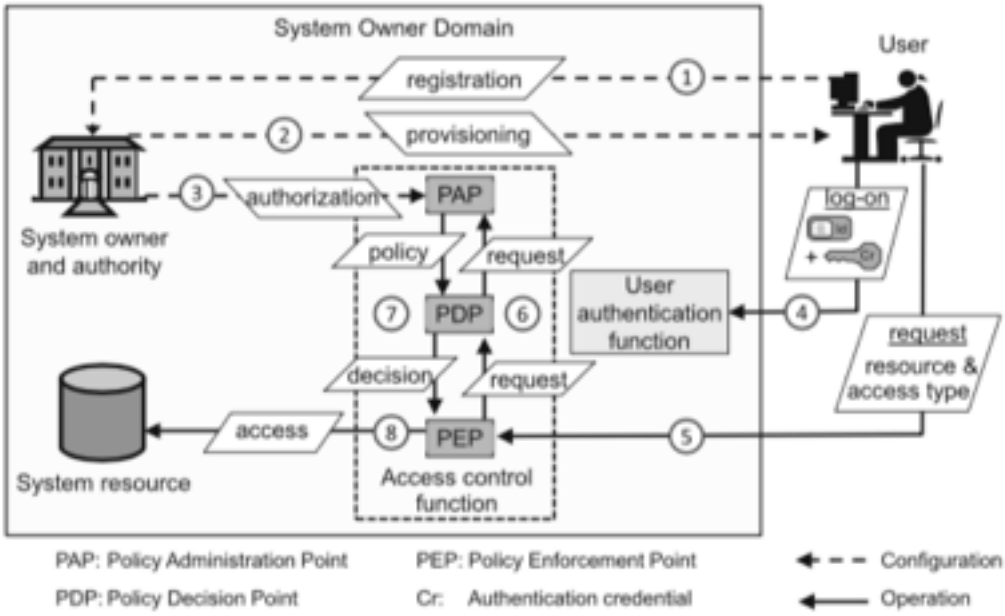


*Figure A3: Process Flow for Identity Management*
Extracted from Josang (2017, p.143), Fig. 2

# Appendix B: Definitions of Terms Relevant to Authentication

***Information System (or just System)*** *means a set of interacting Data and processes that performs one or more functions involving the handling of Data and Information, such as data creation, editing, processing, storage and deletion; and information selection, filtering, aggregation, presentation and use*

***(Id)Entification*** *means a process that necessarily involves the provision, acquisition or postulation of either an Identifier (for Identification) or an Entifier (for Entification); and that may also enable association with Data stored about that (Id)Entifier*

***(Id)Entifier*** *means a set of Data-Items that are together sufficient to distinguish a particular (Id)Entity-Instance in the Abstract World*

***(Id)Entity-Instance*** *means a particular instance of an (Id)Entity*

***(Id)Entity*** *means an element of the Abstract World that represents a Real-World Physical Thing (in the case of an Entity) or Virtual Thing (in the case of an Identity)*

***Nym*** *encompasses both an Identifier that cannot be associated with any particular Entity, whether from the Data itself or by combining it with other Data (an* ***Anonym****), and an Identifier that may be able to be associated with a particular Entity, but only if legal, organisational and technical constraints are overcome (a* ***Pseudonym****)*

***Pre-Authentication*** *means a process that evaluates Evidence in order to establish a degree of confidence in the reliability of Assertions of (Id)Entity and of the appropriateness of providing that (Id)Entity with a Permission*

***Evidence*** *means Data that assists in determining a level of confidence in the reliability of an Assertion*

***Evidence of (Id)Entity*** *means one or more Authenticators used in relation to (Id)Entity Assertions. The conventional term Proof of Identity (PoI) is deprecated*

***Authenticator*** *means an item of Evidence*

***Credential*** *means an Authenticator that carries the imprimatur of some form of Authority*

***Authority*** *means an Entity that is recognised as providing assurance regarding the reliability of an Authenticator. Examples of Authorities include government agencies that issue passports, drivers' licences and citizenship certificates; operators of databases of educational and trade qualifications and testamurs; and notaries*

***Relying Party*** *means an Entity that relies on Evidence that is purported to support an Assertion. An Entity that creates or provides Evidence may or may not have responsibility at law to ensure its reliability or integrity. This is more likely to be the case if the Entity is an Authority that issues a Credential. Where a responsibility exists, an Entity might incur liability to the Relying Party in the event that the Entity fails to fulfil that responsibility*

***Token*** *means a recording medium on which useful Data is stored, such as one ore more (Id)Entifiers, Authenticators and/or Credentials*

# Appendix C: Standards Documents' Misrepresentation of Things

The leading documents in the area during the decade 2000-2010 created a vast array of misunderstandings, and resulted in a considerable diversity of IdM theory and practice that ill-fitted organisational needs. For example, IETF (2007) defines **identification** as "an act or process that presents an **identifier** to a system so that the system can recognize a system **entity** and distinguish it from other **entities**" (p.145, emphases added).

A decade later, it is reasonable to expect that a revised version of an international Standard would provide a much clearer view of the concepts, and workable terminology and definitions. Instead, ISO 24760-1, even after a 2019 revision, defines **identification** as "process of recognizing an **entity**" (p.1), and verification as "process of establishing that ***identity*** *information* ... associated with a particular ***entity*** ... is correct" (p.3, all emphases added). This is despite the document having earlier distinguished 'entity' (albeit somewhat confusingly, as "item relevant for the purpose of operation of a domain [or context] that has recognizably distinct existence") from 'identity' ("set of attributes ... related to an entity ..."). Even stranger is the fact that, having defined 'identifier' as "attribute or set of attributes ... that uniquely characterizes an identity ... in a domain [or context]", the ISO document defines 'identification' without reference to 'identifier' (all quotations from p.1).

On this unhelpful foundation, the Standard builds further confusions. Despite defining the term 'evidence of identity', the document fails to refer to it when it defines credential, which is said to be "representation of an identity ... for use in authentication ... A credential can be a username, username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc." (p.4). This muddles all of evidence, entity, identity, attribute, identifier and entifier, and omits any sense of a credential being evidence of high reliability, having being issued or warranted by an authority. The confusion is further illustrated by the definition of **identity** proofing as involving "a verification of provided **identity** information and can include uniqueness checks, possibly based on **biometric** techniques" (p.5, emphases added). A biometric cuts through all of a person's identities, by providing evidence concerning the underlying entity.

The NIST documents, meanwhile, appear not to recognise any difference between entity and identity, with the only uses of 'entity' referring to legal or organisational entities rather than applicants / claimants / subscribers / users. NIST also refers to the "classic paradigm" for authentication factors (what you know/have/are), without consideration of the substantial difference involved in "what you are", and without distinguishing humans from active artefacts (NIST-800-63-3 2017, p.12). It also blurs the (id)entity notions when discussing biometrics: "**Biometric** characteristics are unique **personal attributes** that can be used to verify the **identity** of a person who is physically present at the point of verification" (pp.13-14, emphases added).

Beyond the basic definitions, conventional theory mis-handles **relationship cardinality**. Entities generally have multiple Identities, and Identities may be performed by multiple Entities, both serially and simultaneously. Consistently with that view, ISO 24760-1 expressly states that "An entity can have more than one identity" and "Several entities can have the same identity" (p.1, see also pp.8-9). Yet it fails to reflect those statements in the remainder of the document.

Authorization schemes built on models that fail to reflect realities inevitably deliver confusions and evidences errors and insecurities.

## Acknowledgements

This paper builds on prior publications by the author on the topic of identity authentication, including Clarke (1994, 2004, 2009). The comments and questions are acknowledged 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,