Words of Identity

A pragmatic guide to the confusing terms and words of Identity and Access

By Espen Bago

Table of Contents

A PRAGMATIC GUIDE TO THE CONFUSING TERMS AND WORDS OF IDENTITY AND ACCESS..........1

ABSTRACT..1

INTRODUCTION..2

WORDS..3

NOTES ON SPECIFIC WORDS AND TERMS IN IDENTITY AND ACCESS TO BE AWARE OF 3

CAUSES AND CONSEQUENCES...8

SHORT-TERM SOLUTIONS 9

CONCLUSION 10

AUTHOR BIO 11

Abstract

Identity and Access is a complex topic covering a wide range of topics and sub-areas. Getting a grasp on this is difficult for anyone; understanding the subject well enough to explain it to others and collaborate is even more challenging.

A natural starting point for understanding a complex topic or area is to seek to learn the native language, such as the professional jargon of the area. And many of us start precisely that way, by searching out dictionaries containing words and terms of "IAM" and its sub-components.

There are many such dictionaries to be found. And the subtle—and not-so-subtle—differences in the definitions found in these illustrate the challenge this article aims to alleviate. We may have a de facto "*language of Identity and Access*," but this language has no formal structure to its semantics.

Our area of technology and business is characterized by an abundance of words having multiple meanings. These are confusing or frustrating for beginners and experienced practitioners alike.

This article is intended as a guide for keeping track of ambiguous words and terms often encountered in our industry, as well as to show that this deficiency in understanding may be even more significant in Identity and Access than in other places.

The article offers examples of where terms are ambiguous and definitions seem to vary across the industry. These examples serve as an aid both to lessen confusion and encourage better and clearer usage of the terms. This article also discusses reasons for the differences and offers some suggestions on countering this challenge in the line of work.

Introduction

None of us in this industry work with bricks and mortar or other tangible, real objects. Everything we do—in IT, not just in Identity and Access—is instead a digital representation, an abstraction, of something that might exist in the real world.

Identity and Access are the glue for many of those digital representations. This puts a lot of responsibility on our representations to be extra reliable, understandable, and able to be proven correct. This concept of representation may be the most important thing to understand when considering, interpreting, and choosing between the different possible meanings of words.

Practitioners new to Identity and Access quickly realize that many of the words they encounter have different meanings than they first thought. One of the first words encountered is “identity” itself. Some will think they know what it means, and others will stop and think and ask. Does “identity” mean the same as “user”? Does “user” mean a person, or does it mean some digital object within IT systems (like a “user account”)? The difference is often obvious to the author or originator, but less so for the rest of us.

But since many people—newcomers and old hands alike—are reluctant to show (perceived) weakness in front of perceived experts, questions are too often not being asked when they are unsure. As in any industry, a typical consequence of miscommunication is that the end product or project is of lower quality or takes longer to deliver.

Another aspect of the problem is the differences in dialects between separate companies and organizations. Learning the local dialect may be achievable, but realizing that other organizations and products have divergent definitions can be a surprise.

There is no quick fix available for the ensuing confusion, but it may help to be aware of the most commonly diverging meanings and their context. The following list is a sample of words and terms where Identity Professionals have experienced significant ambiguity.[i]

Words

Notes on Specific Words and Terms in Identity and Access

This terminology section highlights how common terms are defined differently within the same industry. It is not intended to suggest definitive language for any term included—the focus here is on showing existing usage variations.

Access Right, Entitlement, Permission, Privilege, Profile, Role (and More)

There are multiple words that (mostly) mean almost the same as the term *access right* or simply *access*. One challenge is that sometimes they are used interchangeably as pure synonyms. At other times, each word is ascribed a slightly different meaning, often denoting different granularity of access in a hierarchy when one word is meant as being a subtype of another. But such usage is only defined by local customs rather than universally. Often, we see such specific usage as part of a specific vendor terminology or in a particular standard. The suggestion here is to by default assume these words to be synonyms, and if there is a need for them to have distinct and significant meanings, describe these meanings locally and make certain the description follows the text wherever it is used. Each potential synonym listed above has separate entries below, noting some of their possibly distinct meanings in particular contexts.

Account

The word *account* has its origin in the act of counting something. Identity and Access often denotes "*user account,"* as in an IT system's digital user object or user record. But *accounts* in a bank, insurance company, or customer relationship system differ from the *user accounts* an IT department might speak of.

In such situations, using "account" in documentation and description will cause confusion unless it is made unambiguously clear how to understand it.

But user accounts and accounts do not exist isolated from each other. Financial systems exist where "users" (or persons) can have one or more "accounts." Similarly, Customer Relationship Management (CRM) systems exist where customers (or persons in general) can have one or more "accounts." Both need to interact with Identity and Access systems. CRM and finance are just two examples of a word taking on a different meaning when the context changes or varies.

Authentication

Authentication is often described as "the process or action of proving or showing something to be authentic, true, genuine, or valid." Note that this does not necessarily mean the entity is mapped to a known, verified, natural person. This is often a prerequisite to *allowing* access to *resources* in an information system. In that context, authentication is often confused with authorization, as in many erroneously thinking that if someone authenticates successfully to a protected resource, they should also have access to it. The *authorization* process does not follow automatically from *authentication*, and each of the process steps needs to be clearly and distinctly described.

Authentication Factor

Continuing from *authentication* above, further potential for confusion is related to the varying understanding of the individual building blocks or elements of that process. For example, *authentication* often requires multiple "factors in Identity and Access." But "factor" is often interchangeably used to mean both "categories of factors" and "specific or individual factors." This ambiguity tends to make understanding harder. Descriptions of *authentication* also often contain confusing usage of components such as *identifier* (e.g., the identifying key, text string, numeral) and *authenticator* (e.g., the password, hardware key, biometric fact) of the process.

Authorization

Authorization is, as indicated above, sometimes confused with *authentication,* although they are different processes. Even in the IDPro Body of Knowledge, the definitions diverge slightly based on the context of the article.[ii] Apart from this, the complexity and lack of one standard for authorization gives rise to confusion. For more examples and information, see the IDPro blog post, The State of the Union of Authorization.

Entitlement

Entitlement is often used as a synonym for *access rights,* as mentioned above. Since "being entitled" in general means inherently having a right to something, as opposed to having been granted a privilege, the terms are sometimes used in Identity and Access to denote different levels of access rights in a hierarchy. Such usage is discouraged because it relies on subtle differences that are hard to understand, especially for non-native speakers of English. If the context of the situation requires such a hierarchy, it is better to explicitly describe and explain it than to depend on minute implicit differences in meanings.

Identification

Identification is listed here mainly to complement the words authentication and authorization*,* as it is a process related to those two terms but is often conflated with *authentication.* These processes may be implemented in very different ways depending on the context and requirements, so identification, authentication, and authorization are sometimes merged and implemented as one. But in another context, keeping identification separate and distinctly defined might be essential. In some contexts, there might not even be a need for identification at all (meaning there is no need for an identifier to be used in the *authentication* and *authorization* processes). That might be the case if the only requirement for granting access to a resource is that payment has been made. For the sake of completeness: Other sub-processes are also related to and often required by those discussed above, such as (identity) validation, proofing, vetting, etc.

Identity

First: *Identity is almost never a synonym for* just *identifier.* But the word is often used as if it were.

In almost every case*,* *identity* in our industry is shorthand for *digital identity.* It is often a representation of a real, natural person or something that acts like a person, such as a robot, or something that acts on behalf of a person, such as many Internet of Things (IoT) entities. Anything that requires *authorization* or *authentication* must have an *identity*, even though it does not always *have to* be reliably linked to an actual person. But what it means "to have" an *identity* in a specific context or situation is often not explained. And *identity* is often used interchangeably to mean different things that are not immediately apparent to the reader or audience. The difference often lies in the level of complexity intended for the given *identity* object. For example, sometimes *identity* needs to mean a very specific set of required data attributes that together—completely, for that given context—make up the *identity*. At other times, *identity* refers to a user object in a digital system, possibly including corresponding data attributes as well. And sometimes, *identity* is used for just referring to the *identifier* or *username* itself, without any notion of further complexity.

It may seem useful to have the word *identity* be so flexible, but when it switches back and forth between meanings, for example, "the person using the service" and "the user object representing them," readability suffers. The mix-up of *identity* and *user*—neither of which are clearly defined terms—is very common in the industry. At the time of writing, several examples can be found, for instance, in the Microsoft Azure AD documentation, if searching for both the words *identity* and *user* and seeing how they are used.[iii] Microsoft is no worse than any other party in this regard, unfortunately.

The NIST definition of identity also demonstrates this uncertainty about what it means to "have an identity."[iv] It states that a (digital) identity is "The set of physical and behavioral characteristics by which an individual is uniquely recognizable." The word "individual" here leads us to think about a person since there is nothing else following. Still, the definition is unclear about what it means for identities not directly intended to uniquely represent an actual, physical individual person.

It bears mentioning that there is no such thing as a "human digital identity" versus a "non-human digital identity." In digital systems, any identity is a digital object, which with varying degrees of certainty and through several layers of abstraction, might represent a real person, or it might not.

This problem of not distinguishing *identity* from *identifier* becomes even harder when using the widespread abbreviations ID and ident. These started out as shorthand for *identification* but now often mean either *identity* or *identifier* or both at the same time, making it easier to write a text about them but much harder to understand what it means. It is strongly advised to only use these abbreviations with clear guidance on their intended meaning in the given context. And whenever encountering them, it is advisable to investigate what exactly they stand for instead of guessing.

Owner

Most of the words in Identity and Access are used to *represent* something physical in the digital realm. As such, there is always the concept of relation and linking, which is often accompanied by the concept of ownership. A person may “own” an Identity, which may in turn “own” various user accounts/objects, which may, in turn, be assigned (ownership of) individual Access rights directly or grouped via Roles. In these cases, “ownership” and what it means will not be self-explanatory and needs to be clarified.

Permission

Permission is one of the common synonyms of access or access rights. In Identity and Access, permission has the same general meaning as entitlement and privilege (see below). However, it may also denote the lowest level in a hierarchy of access rights.

Person

For some vendors, *user* denotes the actual human accessing the service, while others use *person* for this. Others again do both at the same time. See User and Identity.

Privilege

As a synonym for entitlement, access rights, and so on, *privilege* is discussed above. In general usage, *privilege* is not a synonym for *right*, which is worth noting. Think of the sentence: “Education is a right, not a privilege.” In Identity and Access, where *entitlement*, *access right,* and *privilege* represent further digital abstractions of something, such distinctions are seldom practical nor constructive.

Privilege in Identity and Access is associated with an even more common challenge. It is used both, as in the above, to denote any access right because any access right is a privilege granted. What causes confusion is when *privilege* is additionally used to mean *special access rights that imply an extra high level of privilege.* A whole specialty area of Identity and Access deals with such special access rights, including administrative access, access to sensitive information, accesses that can cause extra harm if misused, etc. This area has taken the name “Privileged Access Management,” abbreviated PAM.

Where *privilege* sometimes refers to special access and sometimes to *any* access, it is advisable to make this distinction very clear by other means than just the word itself.

Along the same line, it may sometimes be better to use a different term, such as Higher Privilege Management or Higher Privilege Governance, for situations covering only a defined set of *special* access rights to emphasize the focus on special or “higher in importance than the others.”

A related concept is the principle of “least privilege,” used both in general in information security and risk management as well within the Zero Trust security model. Determining what constitutes the “least privilege” necessary for doing a particular job or task will also require being able to group and distinguish between different access rights (privileges) according to the corresponding risk.

Profile

Profile (and the similar *group* as used in Active Directory Security Group) is typically used for describing a collection of something, often a set of access rights or attributes about an entity. In Identity and Access, there is often no significant difference between using a group, profile, label, type, category, or a similar word to mean “a grouping” of, for example, access rights. But often the developer, the designer, or the author of the text had a distinction or special meaning in mind, so it is important to determine and describe what special characteristics or dependencies that specific grouping is intended to have.

Role

Role is often used to represent a grouping of something. This has become the general meaning of *role*. But *role* can generally group *anything* from individual access rights to people, tasks, and responsibilities. All these different meanings are relevant in Identity and Access, but exactly what things a given *role* groups, and under which rules, is rarely spelled out. When using the word *role,* it is almost always necessary to specify how that role is different from all other places the word is used. If, for example, using a term such as “Business role,” “Technical role,” or “Application role,” always supply a precise definition for the term.

Token

There are many tokens in use in Identity and Access since most of the work relates to creating digital representations or symbols of something else—something which may also be abstract. Whether it is *explicitly* a token or just *implicitly* a representation—like a token can represent a valid and authenticated user, or an identity can represent an actual, physical person as well as a non-physical robot—the description of what is being represented and how cannot be implicit. Care must be taken to ensure that the reader or audience understands the relationship and what is represented by what.

An example from standards is the difference between a SAML token and a hardware token such as a FIDO security key. In NIST 800-63-3, the latter was changed to be an authenticator, and the former is still a token to help avoid confusion.

User

The meaning of the word *user* often overlaps with Identity and Person. It is often used to represent a person, such as the physical person who is meant to use a specific digital service, as well as simply representing the *identifier* or *username* of a digital object in the system. Without keeping these two meanings clearly apart, it will be hard for an audience to understand when it means one or the other. Another distinction that needs to be made clear for *user* is when it represents both internal *users* of software systems as well as external *users*. The former are often, but not always, administrative users or employees, and the latter are often, but not always, customers. Context determines the correct usage, but since the context is often not known, it needs to be specified.

The list above primarily aims to showcase the most common ways typical words in Identity and Access are used confusingly. Other lists aim to provide commonly used definitions - one of these is the *Terminology in the IDPro Body of Knowledge*, the list of words and terms used in articles of the Body of Knowledge, describing how they are used and maintained by the IDPro.

Causes and Consequences

An understanding of sources of ambiguity may be useful here, as this can make it easier to detect potential misunderstandings as well as manage their impact.

As noted above, Identity and Access have a language of their own. It is a language consisting of technical terms and abbreviations, but it also includes many *common* words that have taken on *special* meanings. These commonly known words comprise one such source of ambiguity. This organic growth of potential meaning stems from the fact that adding extra meanings to a word is much easier than taking it away. Consequently, the original meaning of the word is, for most people, still present in their minds. Unfortunately, they must also guess what exact interpretations have been added. The lack of a single, authoritative vocabulary for Identity and Access means that such extra meanings may and will diverge over time.

Whether one has learned these meanings from a list—found by searching on the Internet—or learned them from a mentor, colleagues, or presentations at conferences, they are valid in one or more specific contexts. If there are different possible contexts, there will also be multiple possible meanings.

One reason this is plaguing the area of Identity and Access is that this is an industry, not a discipline of science, and a young industry. It's an industry where practice is developing faster than standards and theory.

There is also the fact of multiple stakeholders. Identity and Access are relevant across various sectors (e.g., finance, healthcare, education, government), and each sector brings its own needs and interpretations to terms used in their environments.

But the stakeholder type probably most useful to be aware of is Marketing. For every term, technical or not, there is a risk that, in the end, "Marketing owns everything."[v]
No one has enough bandwidth to fight a battle for every term, so regarding which terms and concepts we find essential to retain ownership and definition power over, we must prioritize; we "have to choose our battles."[vi]

The relevance and viability of Identity and Access across sectors drive financial investment in vendors and products, resulting in companies' desire to put their stamp on Identity and Access terms and have their specific words correspond to their specific product or expertise. This desire leads to a multitude of competing words and/or meanings for terms like "privileged access rights" or "zero trust" or creates new terms overlapping with old, such as "IdM" vs. "IGA" vs. "CIEM," or "UEBA" vs. "ITDR."

The proliferation of such terms, created primarily to distinguish products from others, or attempt to take the name of a method or framework and connect it to a product, is something Identity Professionals get used to seeing over time. That does not mean it is necessarily a sustainable situation for the industry, and investigations into potential long-term solutions might be constructive to pursue. A discussion of potential longer-term solutions and the change the industry might go through is outside of the scope of this article.

On the other hand, it is within the scope to highlight the issue for the sake of better understanding and suggest how to approach the issue in the short term.

Short-term Solutions

To begin with, the best thing that Identity and Access practitioners can do is be *aware* that the terms used in the industry are confusing and ambiguous. When *hearing or reading* words of Identity and Access, this means:

- Continuously being aware of the problem.
- Setting aside time and patience for questioning.
- Questioning everything that:
    - Seems to have a different meaning than expected.
    - May have a meaning not immediately understood.
    - Seems ambiguous.

When *using*—writing or speaking—words of Identity and Access, awareness means consciously practicing clear and precise language.

- One important guideline is to always think about which of the chosen words may be understood differently if read or heard by persons from different backgrounds. If so, further explanation may be necessary. The list of words in this article is a good reference point for potential confusion.

- Consider whether a word is chosen because it can convey a fact or concept clearly, or whether it just looks good on paper.
- Imagine a theoretical difference between an identity *engineer* and an identity *evangelist*, the former needing to be unambiguous, the latter needing to be convincing.[vii]
- See also the note on Marketing above.

Create and maintain *local sources of truth (definitions)* where needed and when the universal terminologies do not precisely fit your local purpose.

- Use such lists to maintain a local authority to clarify in which context the meanings are valid.
- Try to keep the use of these words to only the intended local context.
- When it is necessary to collaborate with someone *outside* of the local area**:** Describe and explain the local context and purpose of the list.

In addition to the general awareness noted in the first bullet point, maintain an additional awareness of *specific words* within Identity and Access.

- These are regular words whose specific meanings get confused more often than others.
- See the Terminology section for examples of such words.

Conclusion

The specific context of a word is often unclear or unknown. And very few of these words and terms have exact, universally agreed-upon meanings. Consequently, unresolved debates about correctness or truth are common in Identity and Access. In many more cases, no one wants to admit that they are unsure about the meaning, and there isn't even room for a debate that might lead to resolution.

With so much opportunity for misunderstandings and miscommunication, the language of the industry is unnecessarily complex. This complexity hurts the recruitment and diversity efforts of the industry, as the impression individuals come away with is that one must be an expert in the field to participate. At the same time, there are no authoritative places to become an expert since the meanings are not universally agreed upon. And as practice develops faster than standards, individual actors in the industry tend to further develop standards in different ways, leading to competing versions. One example is the ISO 18013-5:2021 for Mobile driving license (mDL) application, where different vendors have been building solutions based on different draft versions of the standard.

Even being experienced and an ‘insider’ does not ensure correct understanding. Despite years of experience, individuals will find that words such as *user* or *identity* have multiple and contradicting meanings in a sentence.

There are potential solutions for this chaotic ambiguity of terms, some of which are immediately available and might be applied in the short term**.** Possible solutions for the long term**,** however**,** require more planning and coordination by the industry and affected parties.

In summary: The vocabulary of Identity and Access is vague and contradictory, and as such is not the best possible tool to build reliable Identity and Access solutions. It is a problem that only the smallest startup companies can ignore if they will never have any customers.

Awareness and carefulness around ambiguous words and terms—and knowledge about them—can help in the short term.

Author Bio

Espen Bago realized in 2002 that as system administrator, he’d been working in identity already for a while and decided from there to fully explore what this Identity thing was all about. He’s been an independent Identity Advisor and coordinator to large enterprises for the last few years, but in 2021 became Identity Manager for the Norwegian Labour and Welfare Administration. As such, his goal is to make certain that identities – and the real persons this represents – are not forgotten when governments inevitably go all-in digital. He’s also a founding member of IDPro and a member of the IDPro Body of Knowledge Committee and the IDPro Certification Committee.

[i] Based on conversations and questions about the issue in the IDPro Slack channels and in the industry in general.

[ii] Flanagan (Editor), H., (2022) “Terminology in the IDPro Body of Knowledge”, *IDPro Body of Knowledge* 1(9). doi: https://doi.org/10.55621/idpro.41

[iii] https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad

[iv] https://csrc.nist.gov/glossary/term/identity

[v] Vittorio Bertocci at the Identity at the Center podcast episode #167 - https://www.identityatthecenter.com/listen/episode/24656bde/167-2022-gartner-iam-summit-vittorio-bertocci-with-auth0

[vi] Ibid.

[vii] It’s sometimes necessary to do both at the same time—the point being made is to prioritize clarity over seeming convincing.