IDPro Taxonomy and Body of Knowledge DRAFT

# Introduction

A shared body of knowledge sits at the heart of any professional association.

For Identity Professionals, the body of knowledge will contain the information that is expected to be mastered, in their specific circumstances. So systems architects, security specialists, policy analysts, marketing representatives and business leaders should have knowledge of and possibly experience in specific subsections of information in the body of knowledge.

The ID Pro body of knowledge is structured around a taxonomy. The taxonomy is the organizational scaffolding used to categorize information. It has a regular structure within the different information domains to promote consistency. It is designed to be extendable to accommodate future authors’ needs and priorities. The taxonomy should allow the project teams to fill in portions of the body of knowledge piece by piece, without having to create a linear narrative.

The section in this document on representational models includes visualizations of the taxonomy that can be used by different audiences: practitioners in specific job roles; consultants; regulators; exam takers; educators; and learners in general.

The taxonomy and table of contents for the body of knowledge are being developed in the current work phase. The objective is to describe the boundaries of information for practitioners. In future work phases, citations to published work will be added, and then new content will be incorporated.

The work is challenging but we hope it will stand the test of time and become one of the central structures keeping ID professionals connected.

- any term used might not be perfect

-- The Editors

#

# Table of Contents

[Introduction 1](#__RefHeading___Toc844_1476289550)

[Table of Contents 2](#__RefHeading___Toc846_1476289550)

[High Level Concepts 3](#__RefHeading___Toc848_1476289550)

[Taxonomy 3](#__RefHeading___Toc850_1476289550)

[Body of Knowledge 3](#__RefHeading___Toc852_1476289550)

[Representational Models 4](#__RefHeading___Toc854_1476289550)

[Cake Model 5](#__RefHeading___Toc856_1476289550)

[The Layers of the Cake 5](#__RefHeading___Toc858_1476289550)

[The Sections of the Cake 6](#__RefHeading___Toc860_1476289550)

[The Slices of the Cake 7](#__RefHeading___Toc862_1476289550)

[ID Professional Body of Knowledge 8](#__RefHeading___Toc864_1476289550)

[Identities 9](#__RefHeading___Toc866_1476289550)

[Authentication 10](#__RefHeading___Toc868_1476289550)

[Authorization 12](#__RefHeading___Toc870_1476289550)

[Management 13](#__RefHeading___Toc872_1476289550)

[Citations and Bibliography 14](#__RefHeading___Toc874_1476289550)

[Additional Body of Knowledge Items 15](#__RefHeading___Toc876_1476289550)

#

#

# High Level Concepts

Identity Management is one of the most complex disciplines available in Information Technology. The reason for this complexity is driven by the fact that, whatever we do in IT, we always have some ‘subject-predicate-object’ situation. As soon as the subject or the object in this function represents an identifyable human being (or can be linked to one), we are talking about Identity Management.

This becomes more and more visible - and applicable – with the rise of the Internet of Things, where each and everything is connected and (at the very end) has most often a direct or indirect relation to ourself.

The consequences of this are manifold: apart from the tasks and processes that are to be taken into 7account with any IT operations, a couple of other aspects are to be considered: laws and regulations on data protection, interoperability, security and liability between disconnected systems, domains of responsibility and many more, not to forget ethical topics.

The Body of Knowledge for Identity Management Professionals (IDProBoK) seeks to provide a common framework which enables our industry to categorize areas of knowledge which are useful for anyone who is providing services within the area of management of identities.

The categories chosen for this are described in a ‘Taxonomy’, which we tried to build as universal and simple as possible. The content or information structured by the taxonomy is the Body of Knowledge itself. While the Taxonomy is supposed to be relative static, the Body of Knowledge itself is highly dynamic, and will - by definition - never be completed or ‘100% accurate’.

## Taxonomy

Taxonomy, in this context, refers to the overall scheme of classification used to describe the Digital Identity practices body of knowledge. Information is categorized into an initial layer which is used to separate specific areas of interest. These four areas are Identity, Authentication, Authorization and Management. Each of those four areas are described in the same four common sub sections of Concepts, Regulations, Best Practice and ‘Standards and Protocols’. By applying a consistent overarching categorization structure the Taxonomy becomes a device that can be depicted in numerous ways. This allows for an efficient means for the Identity Professional to expand and assess their level of knowledge.

## Body of Knowledge

Whilst the Taxonomy describes the structure, the Body of Knowledge is the categorized information within the Taxonomy itself. It is the detailed content in each category and sub-category that provides the guiding data for professionals. The IDProBoK is the living and breathing aparatus of the Taxonomy and will grow and contract based on the input of the Identity Professional community.

#

#

#

# Representational Models

The taxonomy and body of knowledge are intended to contain a structured repository of information that an ID Professional could be expected to master, depending on their role and specializations. This structured repository is essential as a means of organizing the information, however the repository will not be very usable unless careful attention is paid to creation of representational models and finding aids which are tailored to specific consumers.

We use the term Representational Model to describe how information can be structured and organized for use by a specific audience or consumer. For example, a hiring manager might want to see a list of job skills related to a certain role; an exam-taker might want a cross-referenced textbook; an instructor might want concepts grouped by credential lifecycle. The representational model or models make it possible to generate these different outputs or representations of the body of knowledge.

Although the taxonomy already tries to describe the concepts of identity, authentication, authorization and management, each of those have multiple dimensions or viewpoints: vertically as with concepts, regulations, best practice and standards/protocols and horizontally if applying operational concepts such as what can be seen in the COBIT ‘Process Reference Model’ or within Project Management Approaches.

The group’s goal was to find a representational model which is able to combine all the different axes and viewpoints in a consistent and logical way, while the model itself should be as complete as possible but still easy to understand.

Another challenge during the model development was the fact that we explicitly tried to avoid to concentrate on ONE standard for a given area, even if that standard is widely adopted: We think, a complete body of Knowledge should also include concepts and ideas which are not commonly applied throughout the topic of interest. Apart from the fact that there is no such standard.

Based on these considerations, we developed a ‘cake’ model with different layers.[[1]](#footnote-2)

##

##

## Cake Model

The idea of a ‘cake’ model is based on the sections we call ‘slices’. Additionally to the slices, cakes can be made of different layers, such as with more ‘complex’ ones. A good example for this could be a ‘wedding cake’.

### The Layers of the Cake

Identity Management can not be seen isolated. As with any other aspect in (professionalized) Information Technology areas, it is incorporated into a whole bunch of tasks and procedures and models already established. Depending on the environment that is investigated, those models might bring in a couple of viewpoints and governance models. As an example (and as a reference usage scenario), we have chosen COBIT, but the same idea applies to other models such as ISMS or Project Management Frameworks like PMI.

The wide topic and required definitions of “operations”, which includes delivery, service and support, is placed on the bottom of the model. On top of that, “implementation” aspects to build, acquire and implement IT Systems are representing the next layer. Non-technical or organizational perspectives are added with another layer for governance, strategy and planning. And finally, we need to add a layer dealing with the typical identity management aspects.

The order of these layers are not strict or fixed. It is important to understand that the model is not a ready to be used construction or action plan. One does not have to strictly apply all layers and slices available. But it makes definitely sense to take them into account if and how they might apply to the (identity mangement) topic which is investigated.

A cake like this consists of different levels; our reference cake has three levels representing typical operational areas known from Enterprise IT governance models and one level (on top) for IAM specific areas.

The ‘terms’ to be used to reference the elements of the model:

* ‘Layer’ for the 4 parts of the cake (from bottom to top)
* ‘Sections’ for the toplevel identity management areas
* ‘Slices’ for the sublevels within the sections
* ‘Rings’ as an additionally available dimension.

### The Sections of the Cake

Now imaging you would like to have a piece from this cake. Most likely, you will not try to cut a piece just from the lowest layer: you will get a slice which ‘covers’ all the layers. But which slice you will have?

If we have a look on this cake from the top, will you have the slice on the right or from the left? And where is right or left?

To answer the question, lets first split the cake into the four ‘Sections’, each representing the same ‘size’. These sections represent the four different basic knowledge areas, which we have identified to deal with the general **concepts** of….



* Identity
* Authentication
* Authorization
* Management

Each of these Sections do have a similar weight, and therefore size (a quarter). They are the most basic concepts you can think of in terms of ‘identity management’: Whatever you can think of, everything can be sorted into at least one of these sections.

### The Slices of the Cake

Each of the identified sections can be further subdivided into topics (slices) related to

* Concepts
* Regulations
* Best Practices
* Standards and Protocols

Again, the topic investigated is related to eat least one of these slices, while there is a kind of weight in it. The highest ones are obviously ‘Standard / Protocols’ and ‘Regulations’, while ‘Concepts’ and ‘Best/ Good Practices’ are less strict.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   |  **Concepts...** |  **Regulations...** |  **Best /Good Practices...** |  **Standard and Protocols...** |
|  **Identities /****Authentication /****Authorization /****Management** | ...that have evolved during time dealing with (digital) identities and their many facets.Concepts describes ideas, theories, procedures and common terms a ID-Professional should be aware of, even though the described concept might not be covered by regulations, best practices or standards. | ...and laws which are to be taken into account when dealing with (digital) identities, either in general or within a given industry | … are methods or techniques within the given field which have gained wide acceptance to be applied in preference to other methods and techniques.The superiority of a ‘best practice’ is commonly measured based on better results (in quantity, quality or manageability).This also includes ‘de-facto’ standards.  | ...are norms, requirements and conventions. This can be described as a general principle to be followed (canon), as industry standard such as RFC and ISO or technically as communication protocol describing the interaction between two or more computer systems. |

##

# ID Professional Body of Knowledge

These tables contain the topics that an an ID Professional should know *something* about and eventually master. The depth of knowledge and experience will vary by individual and role.

The bulleted items in the tables are topic labels, not wordy descriptions of the topic itself. The detailed elaboration of each topic label will occur in a future revision.

The examples and content of the tables do not claim completeness. In much the same way they are not written in stone: for many details you will find contradicting information in other publications. This does not mean the IDProBok is wrong or right: It simply means that the given topic is widely discussed. And that is just another aspect of identity management and the knowledge you need.

##

##

## Identities

The term or concept of ‘identity’, and what it means exactly is subject to discussion since the very beginning of science and scholarship, especially in philosophy. In much the same way, a single, reliable definition of the term is still debated extensively and internationally.

Much simplified, an identity can be seen as **one** subject which is **uniquely** identifiable, to a given level of certainty (or ‘assurance’) in a given set of **many** subjects. A ‘digital identity’ is a cybernated representation of this subject. This definition includes human and non-human subjects - although generally, the discipline of ‘Identity Management’ most often deals with human subjects, or at least subjects that are directly or indirectly related to human beings. This relation to a human being (a real person) is what makes ‚identity management‘ so special within information technology. Personal Identifiable Information (PII) is protected by several laws and regulations, they demand ethical behavior and they generally have a direct (or indirect) impact on our self.

|  |  |
| --- | --- |
| Identities | Examples (collection, not meant to be complete) |
| Concepts | * Identities and their digital representations and types in their respective context.
* Identity Relationships
	+ Business (reports-to / reports-to-me)
	+ Social (Foaf)
	+ Asset Ownership
	+ Customer (‘know-your-’)
	+ Patient (medical)
	+ Other non-human entities
* Ethics
* Identifiers and uniqueness in populations
* Aggregation and Verification, Levels of assurarance
* (Self)-Sovereign (authority)
* Attributes and properties
	+ Static, dynamic
	+ Assigned and self-asserted
	+ Mandatory and optional
 |
| Regulations | * EU-GDPR
* EU-eIDAS
* US-ESIGN
 |
| Best Practice | * Contextual Identity Management
	+ Privileged Identity Management
	+ Customer Identity Management
* Master Data Management
	+ Relationship Hierarchies
	+ Relationship Management
* Privacy Protection and consent management
	+ Selective and minimal disclosure
	+ Pseudonymity and anonymity
* Identity Proofing
	+ Evidence requirements
	+ Process requirements
	+ Thresholds, statistical nature, sampling, relation to source documents
 |
| Standards and Protocols | * ISO/IEC 24760
* ITU-T X.1252
* NIST 800-63-3
 |

## Authentication

The term ‘Authentication’ has many meanings and usage contexts for ID Professionals.

The Merriam-Webster dictionary definition is: “*Authentication (verb): to prove or serve to prove to be real, true, or genuine*”[[2]](#footnote-3). In the domain of ID Professionals, this definition can be used as a starting point.

Some of the contexts which ID Professionals will encounter Authentication include:Look we are either talking about Identity Proofing OR authentication (with the factors POST enrollment) can we please please please not conflate these things. Just read NIST 800-63-3 or Sarah Squire’s talk from RSA. authentication is not prooving you are who you say you are.

**Credential authentication:** can include a) a form of document verification where the credential is a controlled document issued by an authority; or b) a form of user login where a credential and authenticator are used to prove that the credential is presented and controlled by the true owner.

**Federated authentication:** entity authentication where the authentication verifier is remote or separate from the resource being requested and the verifier and relying system use the same standards for confidence in authentication. The authentication verifier communicates, or asserts, the result of the authentication to the system that is relying on the authentication decision.

**Entity authentication:** synonym for ID Proofing and Verification OR a form of login using credentials and authenticators. This form deliberately avoids specification of human entities versus non-person entities.

**Document verification[[3]](#footnote-4):** checking that data is correct and valid by corroboration or source verification; checking that any document security features are intact; searching for duplicates. Often used in ID Proofing and Verification processes.

These contexts and usages have similar operations: presentation of evidence, sometimes known as ‘authenticators’ to a verifier; verification of the evidence either as-presented or against a data repository; optional corroboration of data related to the evidence; decision; action resulting from decision.

In entity authentication systems for system access, credentials are created and issued to enrolled system users. Credentials for authentication conform to specifications of the authentication mechanism or technology for those credentials. The authenticators specified in an authentication system are presented to the authentication verifier such that the verifier is able to determine the nature of and characteristics of and perhaps the identity of the entity which aims to use the credential for authentication. For example, for username and password credentials, the authenticator is often a cryptographic hash of the password. The verifier can determine that the hash received matches that on record for the username, but cannot know if the human that originally controlled the username is still the same human. Qualities of authentication systems should include security, reliability and usability qualities. Authentication systems are critical for identification of human and non-person entities to a degree of confidence. Identification is an early step in processes related to authorization policy evaluation, and control of information or system access.

The ID Pro Taxonomy and Body of Knowledge includes concepts of authentication and widely-used authentication methods and techniques, depending on the context.

Regulations and standards are emerging for the public sector and regulated industries. Standards for the determination of relative authentication ‘strength levels’ are under development. Standards and guidance for evaluation of confidence in authentication exist and are being improved over time.

|  |  |
| --- | --- |
| Authentication | Examples (collection, not meant to be complete) |
| Concepts | * What are the commonly-used frames of reference for the term ‘Authentication’?
	+ Document verification
	+ Person fact verification
	+ Recognition of a prior encounter
	+ Identification (in different contexts)
	+ Verification of authenticators bound or contained in Credentials
* What is the relationship of Authentication to Identification
* Authenticators (Credentials)
	+ Categories and characteristics
	+ Single- and multi-factor authenticators: objectives, threat mitigation
	+ Verification mechanisms
	+ Cryptographic mechanisms
	+ Lifecycle management
	+ Misuse and impersonation detection
	+ Usability considerations
* Authentication Architectures
	+ Federated authentication
	+ Single sign-on
	+ Challenge-response
* User interaction techniques
	+ Forms-based
	+ Image based
	+ Operating system pop-up
	+ Out of band techniques
* Impersonation
	+ Authorized
	+ Fraudulent
 |
| Regulations | * US Government MFA mandatory
* State-level regulation - some have these regulations
* US Health IT
* US Financial Services Industry
* EU-PSD2 (explicit authentication requirements)
* EU-GDPR (implicit authentication requirements)
 |
| Best Practice | * Methods to choose appropriate authentication techniques
	+ Risk evaluation considerations
	+ Cost considerations
	+ Usability
	+ Manageability
	+ Attack Resistance
	+ Models of Authentication ‘levels’
* ‘Binding’ of authenticators to entity records
	+ Uniqueness within a population scope or ‘namespace'
* Decision factors to determine if authentication is needed, and to what degree and what appropriate mechanisms
* Privacy matters
	+ Correlation across multiple transactions
	+ Decoupling of personal information to authentication events
 |
| Standards and Protocols | * OpenID Connect
* SAML and WS-Federation
* Shibboleth?
* PKI-based
* Kerberos
* FIDO Universal 2nd Factor, Universal Authentication Framework protocols
* RADIUS
 |

## Authorization

Authorization is one of the primary purposes of any identity management system.

The Merriam-Webster dictionary definition is: “*Authorize (verb): to […] permit by [...] some recognized or proper authority (such as custom, evidence, personal right, or regulating power)*”[[4]](#footnote-5).

The processes of deciding whether some requested activity is allowed are the processes of authorization. Authorization usually happens after the requesting party is already authenticated and the subject requesting a ressource is identified.

However, once entering the authorization phase it is also possible to link back into the authentication and request additional proofs of authenticity.

When discussed in the context of information systems, access control is preceded by an authorization decision process. When discussed in the context of information exchange, authorization is often called ‘consent’.

|  |  |
| --- | --- |
| Authorization | Examples (collection, not meant to be complete) |
| Concepts | * Relationship to Identification, Authentication, Access Control
* Access control models
	+ RBAC, ABAC, PBAC, ID-BAC
	+ ACL-based
	+ Centralized, decentralized
* Authorization and obligation
* Prerequisites and Duties
	+ Trust elevation (e.g. re-authentication, step-up authentication, claims gathering) - items done before access is granted
	+ Duties - items that are requested to be performed after authorization
 |
| Regulations |  |
| Best Practice | * Authorization policy evaluation
	+ Proofs of assertion (tokens, tickets, cookies, cryptographic methods)
		- Bearer methods v proof of possession methods
	+ Access control policy, authorization policy,
	+ Static evaluation, dynamic evaluation
* Considerations for choosing specific models, protocols
	+ Risk based authorization
	+ Context based authorization
	+ Centralized v decentralized decision
	+ Segregation of authorization policy decision and access control decision
 |
| Standards and Protocols | * OAuth
* UMA
* XACML
 |

## Management

Management at it’s broadest sense defines how the life cycle of identity records, physical things and relationships are managed. For Identity Management we define this as the administrative tasks associated with the handling of Identities and their entitlements. It refers to the processes that ensure the maintenance and fidelity of associated data of the identities and their relationship to entitlements within and of systems, applications and devices.

Management consists of initial tasks that include defining requirements, creating policies and implementing base technological systems to ensure alignment with business requirements and security needs.

Once base systems and processes are in place, maintenance tasks are carried out which include auditing, reconciliation, reporting and process improvement tasks. A core component of this maintenance is also the ongoing validation of the relationship between identities and their entitlements via access certifications.

Overall, Management seeks to set a clear set of engagement rules for the control of Identities and what they are entitled to.

|  |  |
| --- | --- |
| Management | Examples (collection, not meant to be complete) |
| Concepts | * Identity Technologies
* Entitlement Dictionary
* Identity Governance
* Least Privilege
* JIT and other forms of Provisioning
* Identity Store and associated Identity data
* Segregation of Duties and Toxic Combinations
* Identity Life Cycles, Joiner-Mover-Leaver
* Auditing and Logging
 |
| Regulations | * PHI / HIPAA
* PII
* PCI DSS
* GDPR
 |
| Best Practice | * Requirements Definitions
	+ Clearly define Joiners/Movers/Leavers Management
	+ Establish clear ownership of all identity types, attributes and properties
	+ Establish policies for the lifecycle (Joiner/Movers/Leavers)
	+ Establish policies and processes for non-human identities/accounts (e.g. Service Accounts)
	+ Align with required regulations especially around entitlement revalidation periods
	+ Define a Privileged Identity Policy and processes
	+ Authentication credentials management and policies.
* Self Service scenarios and self-sovereign identities.
* Certification and re-validations
* Program Buy-In - Management Support
* Reconciliation
* Establish Metrics - KPI, KRI’s & KTI’s
* Management of Physical components supporting identity information recording, assertion, integrity, verification
* Management of information related to identity records
* Management of linking identifiers (relationships) between information assets and/or physical assets
 |
| Standards and Protocols | * SCIM
 |

# Citations and Bibliography

1. EU-GDPR
<http://eur-lex.europa.eu/eli/reg/2016/679/oj>
2. EU-eIDAS
<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN>
3. US-ESIGN
<https://www.law.cornell.edu/uscode/text/15/chapter-96>
4. ISO/IEC 24760-1
<http://standards.iso.org/ittf/PubliclyAvailableStandards/c057914_ISO_IEC_24760-1_2011.zip>
5. NIST 800-63-3 (DRAFT)
<https://www.nist.gov/itl/tig/special-publication-800-63-3>
6. Best Practices
<https://en.wikipedia.org/wiki/Best_practice>
7. Canon
[https://en.wikipedia.org/wiki/Canon\_(basic\_principle)](https://en.wikipedia.org/wiki/Canon_%28basic_principle%29)
8. Government of Canada: ‘Directive on Identity management’
<https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577>
9. Web of Trust, Identity Crisis
<https://github.com/WebOfTrustInfo/ID2020DesignWorkshop/blob/master/final-documents/identity-crisis.pdf>
10. [ISO/IEC 24760-1:2011(en) Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts](https://www.iso.org/obp/ui/%22%20%5Cl%20%22iso%3Astd%3Aiso-iec%3A24760%3A-1%3Aed-1%3Av1%3Aen)
11. [ISO/IEC 24760-2:2015(en) Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements](https://www.iso.org/obp/ui/%22%20%5Cl%20%22iso%3Astd%3Aiso-iec%3A24760%3A-2%3Aed-1%3Av1%3Aen)
12. [ISO/IEC 29100:2011(en) Information technology — Security techniques — Privacy framework](https://www.iso.org/obp/ui/%22%20%5Cl%20%22iso%3Astd%3Aiso-iec%3A29100%3Aed-1%3Av1%3Aen)
13. [ISO/IEC 29115:2011](https://www.oasis-open.org/committees/download.php/44751/285-17Attach1.pdf)
14. Bla
15. Bla
16. Bla
17. Bla
18. Bla
19. Bla
20. BlaBla
21. Bla
22. Bla
23. Bla
24. Bla
25. Bla

# Additional Body of Knowledge Items

….Before you add stuff to this section. Think if that is not already covered ‘in some way’ in the taxonomy!

1. During the work on this models, we also had ‘dartboard’ and ‘fishbone’ models, which we skipped in favour of the ‘cake’ [↑](#footnote-ref-2)
2. <https://www.merriam-webster.com/dictionary/authenticate> Accessed 2017-03-22 [↑](#footnote-ref-3)
3. Verification and validation are very similar in meaning and usage. Verification of information leans toward comparison of the presented information against a known authoritative source. Validation of information leans towards providing proof or corroboration to substantiate the information. [↑](#footnote-ref-4)
4. https://www.merriam-webster.com/dictionary/authorize Accessed 2017-03-22 [↑](#footnote-ref-5)