Education 3.0 Base Document

Peter Sibley

Education 3.0 Base Document

Table of Contents

Education 3.0 Base Document

The contents of this document are exploratory and intended to be in the public domain. This is draft material not for distribution beyond the study group and contributors or for citation.

Our intent is the following:

1. ILR Hub Inventory and Ed 3 Base Doc provide a foundation for standards alignment and harmonization
2. CEDS + TLA will integrate in IEEE CM4LTS
3. IEEE CM4LTS will integrate with ISO/IEC JTC1 SC 36
4. IEEE ILR and W3C VC Edu will integrate with each other and incorporate CLR/CASE and other record types leveraging the the public domain ILR Wrapper and Learner Wallet Specification and Modeling Educational Verifiable Credentials
5. IEEE P7004 will integrate MIT Privacy Principles

A primary reference implementation for this work will be:

1. The Broward Algebra Project CLR C-Lab demonstrating linked data pathways and verifiable competency assertions.
2. Credential Engine: Making Learner and Worker Records More Meaningful, Relevant, and Actionable: The Value of the Credential Transparency Description Language - Post
3. T3 SSI Report, Summary

Objectives:
The goal of this document is to establish a common starting point for alignment and harmonization between relevant standard specifications. A Resource Inventory is being gathered in partnership with the T3 Innovation Network, EdMatrix.org, and Project Unicorn.

Education 3.0 Base Document

One initial objective of this work is to update the IEEE's 2003 Learning Technology Systems Architecture 1484.1 standard and publish a recommended set of practices and publish a crowd-maintained, updated, conceptual/logical meta model with linked alignments to relevant data, technical, policy, and achievement standards. In addition, we intend to publish a clear set of recommended practices for integrated, interoperable, and international learner and worker records. The IEEE ILR will result in a recommended practices guide to harmonize learner record standards. The goal of this work is to align many standards into a unified framework. The goal of this work is not a new standard, but rather points to existing standards and practices (with proper IP protocols), providing a guide to bridge learner records between standards for better translation and exchange.

This Base Document is being assembled to provide a strong straw man starting point for the work. It is not a polished static document to be published on its own. It is a dynamic collection of thought leadership contributed by individuals not organizations. All content herein is public domain and can be used without restriction to develop derivative work.

Components

Section 1. Learning Contexts and Models

1.1. Transition from Traditional Education Models

1.2 Learner-Centered Model

Section 2. Information Models

2.1 CEDS Conceptual Model - **Jim Goodell**

2.2 ADL TLA Logical Model - **Jerry Gordon**

Section 3. Guiding Principles

3.1 Contract for the Web - **Tim Berners-Lee**

3.2 T3 Innovation Network Self-Sovereign Identity Principles, **Kim Hamilton**

3.3 Collaboration on Open standards - **Open Pledge**

Section 4. Technical Meta Model

Section 5. ILR Technical Implementation Guidance

5.1 W3C DID Identity and Trust - **Drummond Reed**

5.2 T3 Open Ontology References - **Brandt Redd**

5.3 W3C VC with IMS CLR Verifiable Assertions - **Nate Otto**

Section 6. Mutually Exclusive Collectively Exhaustive (MECE) Use Cases - Greg Nadeau

Section 7. Standards Alignment & Harmonization

7.1 Proposed Relationship of CM4LTS to other LTSC Groups

7.2 Proposed Relationship of CM4LTS to open, published technical standards outside of LTSC

Primary Authors and Facilitator Steering Committee

- **Jim Goodell**, QIP - *Common Education Data Standards (CEDS) Conceptual Model*
- **Jerry Gordon**, ADL - *Total Learning Architecture (TLA) Logical Model*
- **Kim Hamilton**, MIT Digital Credentials Consortium - *Self-Sovereign Identity (SSI) Principles*
- **Drummond Reed**, Evernym, Sovrin Foundation - *Distributed Identity (DID) and Trust*
- **Greg Nadeau**, PCG - *IMS Global Comprehensive Learner Record*
- **Nate Otto**, Concentric Sky - *Open Badge and Verifiable Credentials*

- **Brandt Redd**, MatchMaker Labs - *Open Ontology References*
- **Chris Purifoy**, Learning Economy Foundation - *Market Adoption*
- **Alex Jackl**, Bardic Systems - *Standards Coordination*

IP Protocols

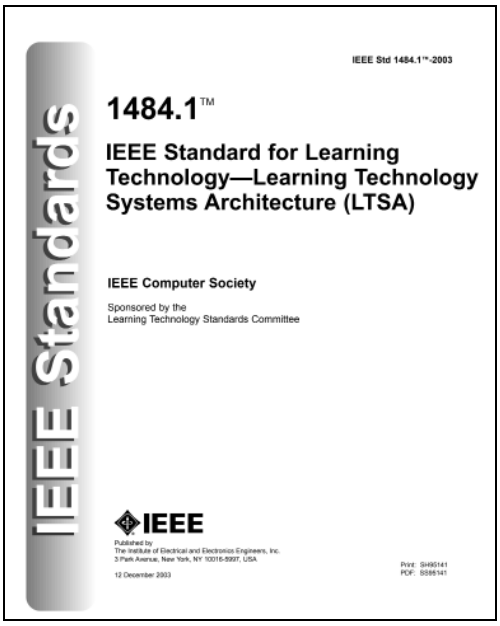
The contents of this document are exploratory and intended to be in the public domain. This is draft material not for distribution beyond the study group and contributors or for citation.

This work will conform to IEEE SA Standards Style Manual for guidelines on proper citations, distinguishing "normative" material from "Informative" material:

- **Normative -** Normative references are necessary for the implementation of the document. A normative reference is a source that users of the standard must have on hand and understand in order to correctly implement the material contained in the draft. Normative references must also be cited within normative text.
- **Informative** - Documents that serve as supplemental information, that are found useful when researching the material, and that are not needed for the implementation of the document are typically Informative and therefore belong in an informative annex entitled Bibliography.

Prior Work

The intent of CM4TLS is to survey relevant existing work and update 2003 IEEE 1484.1TM - Learning Technology Systems Architecture (LTSA) and to extend common education data standards to serialization and transport/security protocol layers.



Survey of Relevant Existing Work

1. A4L Unity Specification
2. A4L SIF Data Model
3. A4L SIF Infrastructure
4. A4L SDPC
5. Achieve NGSS
6. ADL SCORM
7. ADL / IEEE xAPI
8. ASN (University of Washington)
9. Blockcerts
10. CAST UDL
11. CCSSO/NGA CCSS
12. Credential Engine CTDL/CTDL-ASN
13. Dublin Core (DCMI)
14. ECMA JSON
15. EU EDCI
16. EU EBSI
17. EU ELMO
18. edX TSR
19. Ed-Fi Alliance Ed-Fi
20. Ed-Fi Alliance ODS
21. Ed-Fi Alliance Core Student
22. Ed-Fi Alliance Assessment API
23. Ed-Fi Alliance Enrollment API
24. HR Open Standards
25. IDPF EPUB
26. IEEE LTSC ICICLE
27. IEEE LTSC CM4LTS
28. IEEE LTSC LTSA
29. IEEE LTSC RAMLET
30. IEEE LTSC CDS
31. IEEE LTSC LOM
32. IEEE LTSC SCORM API
33. IEEE LTSC SCORM Data Model
34. IEEE LTSC eBooks/eReaders
35. IEEE LTSC CSDG
36. IEEE LTSC xAPI
37. IEEE LTSC AISS
38. IEEE LTSC FML
39. IEEE LTSC ARLEM
40. IEEE LTSC MLP
41. IETF HTTP
42. IMS Global OneRoster
43. IMS Global EduAPI
44. IMS Global CASE
45. IMS Global LTI
46. IMS Global IMS CC/TCC
47. IMS Global IMS CP
48. IMS Global IMS CLR
49. IMS Global QTI
50. IMS Global APIP
51. IMS Global OBI
52. IMS Global Caliper
53. ISTE ISTE Standards
54. ISO/IEC JTC1 SC 36 - Education
55. ISO/IEC JTC1 SC 34 - Doc /ePub Description and Processing Languages
56. ISO TC46/SC9 - Description and Identification
57. MedBiquitous
58. NIST
59. Singapore OpenCerts
60. PESC Core Main
61. PESC Academic Record
62. PESC Admissions Record
63. PESC ePortfolio
64. PESC Credential
65. PESC SPEEDE
66. Schema.org EOC

67. Schema.org LRMI
68. US Ed CEDS
69. US Ed CEDS NDS
70. US Government - FERPA
71. US Government - Section 508
72. W3C DIF
73. W3C DID
74. W3C EEA
75. W3C EOC
76. W3C HTML
77. W3C TMS
78. W3C VC
79. W3C WCAG
80. W3C XML

Conceptual Model for Learning Technology Systems

Section 1. Learning Contexts and Models

Summary. This guide addresses concepts applicable to learning that is facilitated, supported, or managed using learning technology systems. These concepts are intended to be broadly applicable to all learning contexts including formal and informal education such as early learning, primary and secondary education, postsecondary education, workforce and military training, and avocational contexts.

This guide is intended to be broad enough to support both current and future learning contexts. Its focus is on individual human learning while considering developing models of team learning and artificial intelligence augmentation of human performance. Since the previous version of this guide was published, the learning sciences have made significant new discoveries about how people learn and there have been significant advances in technology to support and optimize human learning.

1.1. Transition fromyTraditional Education and Training Models

Historically, education was delivered through a mechanism that started with the passing of tribal knowledge from elders to the next generation. In antiquity and through the middle ages, this meant an “apprenticeship” for the training of skills and the “academy” for education. First modeled by Plato, the academy arose as a formal “brick and mortar” institution for the learning of “philosophy”, which at the time encompassed all formal education and the mode of thinking that it engendered. From the writings of Plato, Socrates and Aristotle, the traditional “liberal arts” paradigm arose for teaching “physics” and “metaphysics”, including the “quadrivium” (i.e. four parts) of arithmetic, music, geometry, and astronomy, and language arts with the “trivium” (i.e. three parts) of grammar, rhetoric, and logic. Variations on these same approaches, typically available only to a small subset of the population, were dominant through the 19th century. The rest of the population, typically engaged in agricultural or cottage industrial work, learned almost entirely in an “on the job” master /apprentice experiential setting focused on work skill training rather than education.

In the mid-nineteenth century, the Prussian model that grouped students by age (i.e. “cohort”) and prepared them for Industrial age work, gained widespread acceptance. In the US, Horace Mann, a state legislator from Massachusetts, successfully advocated for a free, universal public education system based on the Prussian model, which would be compulsory for all young people [aged 5-16]. He led the creation of land use and tax policies that established the first US public school system in 1830’s era Massachusetts. In the early 20th century, American public educator John Dewey (of library “decimal system” fame) helped establish the educational theoretical underpinnings required to implement the Prussian model in the US. Their work birthed the US “factory model” of education. This model starts with a relatively static curriculum developed by experts and focuses on the throughput of the cohort through the educational factory exposed to that curriculum. Learning transfer was measured according to the communication theories of Claude Shannon and Warren Weaver, where the curriculum becomes the message “payload”, transmitted by the “instructor” to the student as “receiver” using test assessments to guarantee or “assess” successful transport.

In the 1990s, the internet and web technology had advanced to the point where “distance learning” or “distributed learning” became possible. Learning Management Systems (LMS) or Learning Content Management Systems (LCMS) allowed for the hosting or compilation (respectively) of multimedia content to provide the same kind of instruction historically presented in the classroom. These “computer-based trainers” (CBT) could be fielded in an “electronic classroom”, or independently to anyone with a properly configured web browser client. It retained the factory/Shannon model for content delivery and transfer assessment, but it decoupled the learning experience from the need for brick and mortar classroom or physical instructors as educational resources. This facilitated a massive increase in student throughput.

In the 2000s, there was further development of technology-enabled learning models (MOOCs, intelligent tutoring systems, virtual and augmented reality, AI-enhanced human-computer interactions, social learning models, instrumented learning & analytics, etc.). However, the predominant classroom-based models of education and training in practice had not fundamentally changed. Technology was primarily used to reduce labor or provide small enhancements to the classroom “delivery” model rooted in the 19th and 20th centuries.

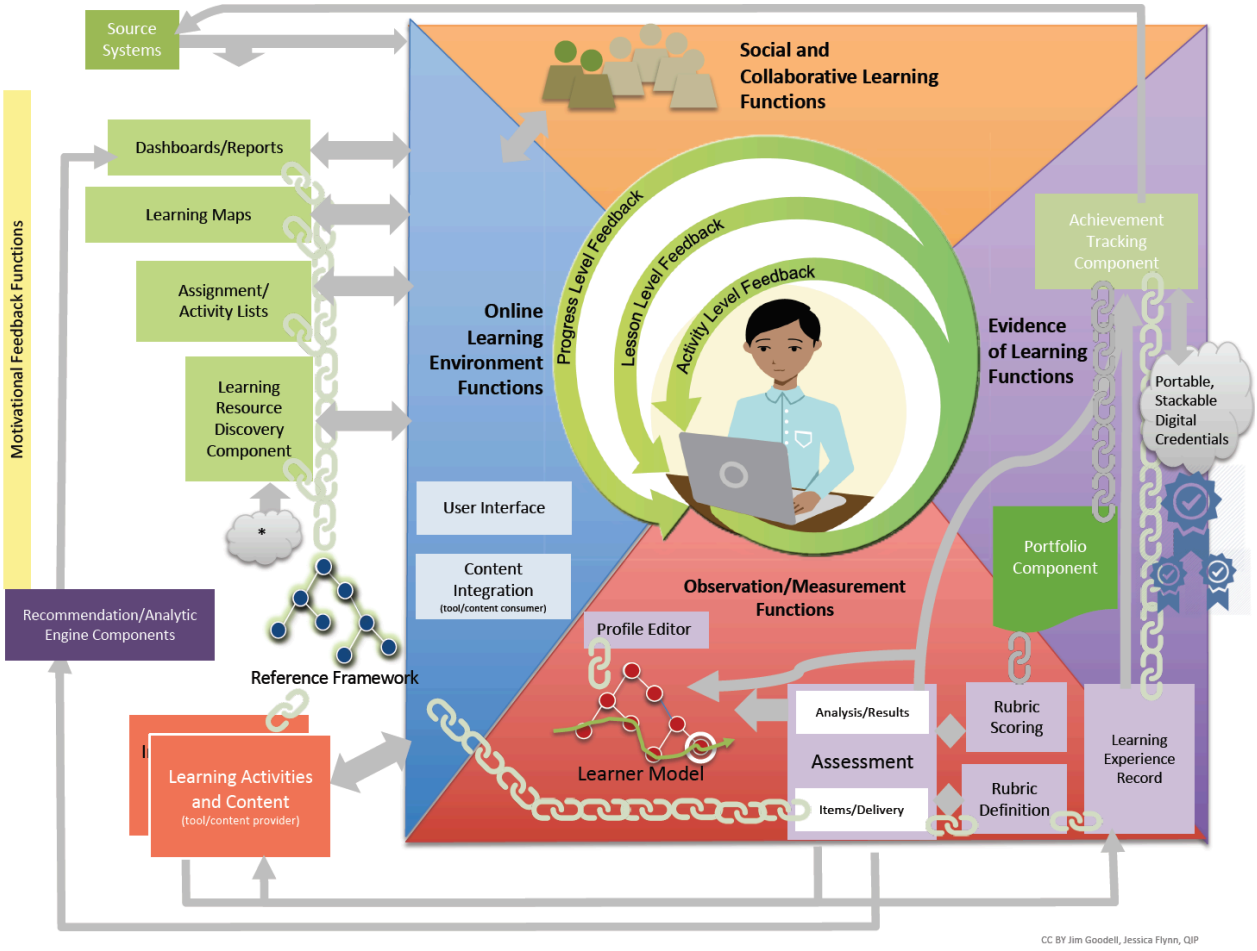
In the 2020s, promising developments in technology-enabled learning models have been or will be supported by other IEEE standards such as standards for virtual and augmented reality experiences, reusable competency definitions, adaptive instructional systems, instrumentation of learning, and interoperable learner records. Increasingly. Learning in both formal and informal contexts is relying on technology as a core enabler of new models.

At the time of this writing, these developments have not shifted well-established institutionalized models of education and training. They are, however, providing alternative pathways for learning and development that are increasingly being adopted by individuals and organizations.

1.2 Learner-Centered Model

Learner-Centered Education. The transition from industrial to the information age and global access to the Internet has led to a re-thinking of the education delivery model. In the 2016 paper on Learner-Centered Education, authors Liz Glowa and Jim Goodell describe a system that provides personalized, competency-based learning through a blend of modes. Figure 1 shows information and functional system components of a learner-centered system.

Education 3.0 Base Document



Adapted from Glowa, L. and Goodell, J. (2016) Student-Centered Learning: Functional Requirements for Integrated Systems to Optimize Learning Vienna, VA.: International Association for K-12 Online Learning (iNACOL). Used with permission.

The learner-centered model considers the learner as a part of a system in which the human learner engages in learning experiences, reacts to those experiences, and receives feedback from other humans (teachers, tutors) from the learning environment and from learning user interfaces of learning technologies. The feedback from other humans or from adaptive instructional systems informs learning at multiple levels. A micro-adaptive system gives feedback during the learning experience, a macro-adaptive system gives feedback between learning experiences. (See IEEE 2247.1)

The learner-centered model may support social, collaborative, and team-based learning.

ADL's Total Learning Architecture (TLA). Additional insights into this new learning model are described by Walcott and Schatz in Modernizing Learning (2019). The DOD digital modernization efforts such as the Total Learning Architecture (TLA) research effort at the Advanced Distributed Learning (ADL) Initiative, seek the development of a "future learning ecosystem". This ecosystem recognizes that learning is a continuous activity that joins formal education and training experiences with on the job training (OJT), work experience, and other autodidactic forms of learning. It expands from traditional pedagogy and adult learning models to include "heutagogy"; self-directed and self-regulated learning experiences where the learner establishes their own learning goals and approaches, and even self-evaluates the effectiveness of their learning and makes corrections.

Learning Science and Constructivism. These modern approaches mirror the shift in the psychology of learning from the older behavioralist models (focused on operant conditioning and repetition), through cognitivism (which models and leverages processes of the mind) and now constructivism. Constructivist paradigms recognize that each individual takes an individualized path through learning and that learning is not "transferred" from expert to learner vis a vis the Shannon/Weaver model, but instead individually discovered or "constructed". Because of the holographic nature of human memory, this constructed knowledge is highly connection-oriented, and new knowledge is dependent on its association with existing knowledge. Human Resources models are likewise shifting from using credentials from accredited institutions as risk mitigators to hiring, but instead modeling fitness by validating assertions of competency to perform work, demonstrated by job experiences and achievements, as evaluating the potential for growth. The latter is based not only on current knowledge and skill but measuring motivational and metacognitive "soft skills" as their own competencies that predict success in acquiring new knowledge and skills.

Personalized, Competency-Based Blended Learning. This future learning ecosystem thus presents learning that can leverage distributed and connected learning through modern computing systems and the ubiquitous presence of affordable handheld devices in our lives (e.g., how many people have "conducted just in time training" by watching a YouTube(™) video on their smartphone?). These devices present an "Anytime, anywhere" opportunity to access learning. They shift the focus from cohort, curriculum, and throughput, to individualized, lifelong learning. This learning adjusts for the individuals' learning preferences formed from past knowledge and "soft skills". It presents learning that is personalized based on specific competency gaps, rather than conformant to a single curriculum. And it changes the role of formal teacher, to a facilitator of learning, existing on a continuum from instructor, mentor, peer, advisor, or observer.

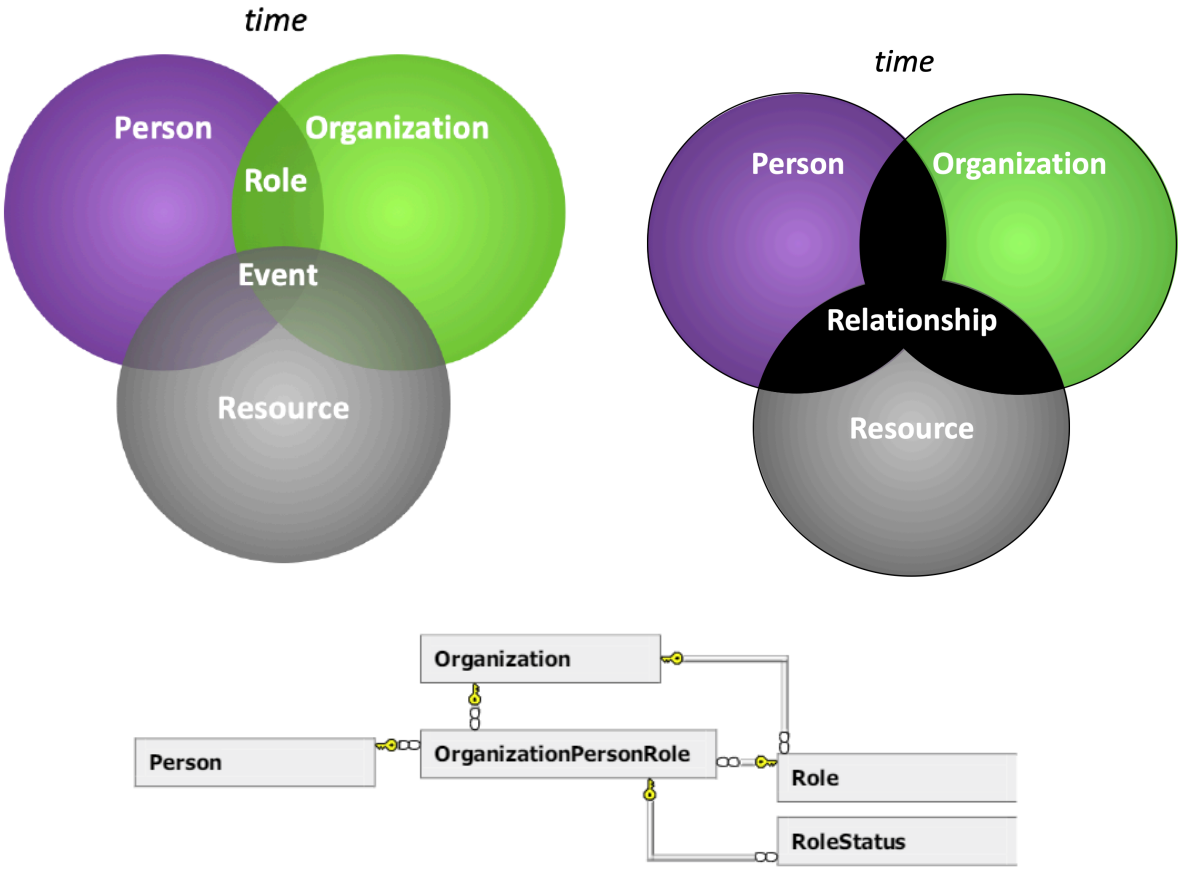
Possibly additional topics for this section to explore:

1. Semantic Web and Distributed Ledger Technology. [Jerry and Greg write]
2. Adaptive Instructional Systems (AIS) …
3. Micro-Credentials…
4. Electronic Performance Support Systems
5. Just in Time Training

Section 2. Information Model

2.1 Conceptual Model

The core information model for education can be reduced to 4 core concepts defined in V8 of the US Education Department's Common Education Data Standards (CEDS) Conceptual Model:



Key Concepts (super classes)

a. **Person.** A human being, alive or deceased, as recognized by each jurisdiction's legal definitions. (CEDS)
b. **Organization.** An organized group of one or more people with a particular purpose. (CEDS)
c. **Resource.** Anything could be a resource, depending on its context defined in metadata. Broadly applicable to creative works and information resources. Resources include anything necessary for "persons" to navigate the learning space. In the relationships between people and organizations, this may be in the form of possessed or required knowledge, skills, abilities, or other behaviors. It can also include the evidence of navigation through the learning space (i.e. "events"), or the activities performed, or elements required for performance, in the learning space.
d. **Relationship.** People, Organizations, and Resources all can have standard association types within and across concepts.
e. **Metadata**. Each object associated with a person, organization or resource (i..e "data") has a set of prescribed attributes (i.e."metadata"- data about data) used to determine the purpose of the object, or the potential relationships between objects.

Key Relationship Concepts

f. **Role.** People have roles in Organizations for specific periods of time.
g. **Event.** People and Organizations have events with each other and with Resources on or over specific periods of *time.*

In addition, relationships between a Person and a Resource could signify, for example, that the person has been awarded a credential, mastered a competency, authored a resource, or owns a resource. Relationships between an Organization and a Resource could represent ownership, authorship, stewardship, etc.

Resource Subconcepts (subclasses)

Resource is a broad category for entities that includes information assets or metadata objects other than people and organizations. Resource entities include but are not limited to:

a. **Competency Definition**: A resource that includes a statement that describes a capability or behavior that a person may learn or be able to do within a given situation and environment, and may include definitions of the potential levels of mastery and metadata related to that statement.
b. **Competency Framework:** A collection of Competency Definitions typically arranged in a hierarchical structure or classification scheme, reflecting expectations of learner competence.
c. **Credential Definition**: A resource that defines a competency or qualification, achievement, personal or organizational quality, experience, attribute, or aspect of an identity typically used to indicate suitability (See: Credential Engine's ceterms:Credential).

d. **System:** A collection of components organized to accomplish a specific function or set of functions. (In this context an information system that functions as an Actor in a use case.)

Event Subconcepts (subclasses)

Event is a broad category for CEDS Entities that includes information that captures changes in Relationships or properties of other entities over time.

a. **Competency Assertion**: Competencies are asserted based on evaluated evidence at some level of confidence. Competencies can be asserted by people, systems, self asserted or asserted through less trusted systems and then verified later. Competencies may or may not roll up into a credential.
b. **Credential Award**: Event data that include an award or conferral by an agent/issuer that documents a person or organization's qualification, certification, license, achievement, personal or organizational quality, experience, attribute, or aspect of an identity as of a certain date or date range. Credentials are based on trust, and can be used as proxies for competence across a range of topics. Constituent competencies provide auditability of credentials to conduct process improvement and to maintain their integrity.

Supporting Definitions

The following concepts are not data entities. They are provided here as normative references for the following sections of this document.

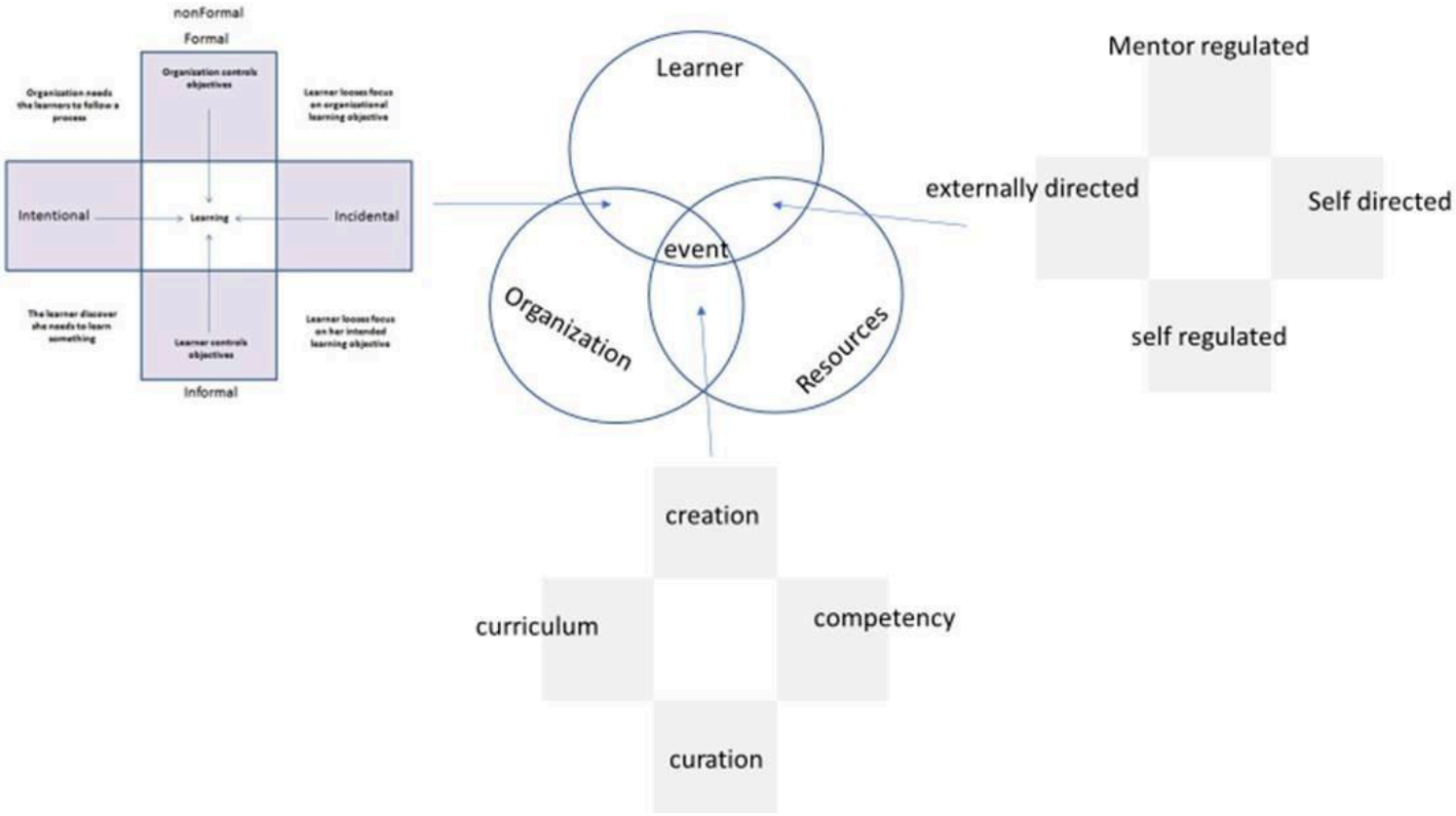
a. **Identity -** The unique fact of being who or what a person or thing is (NIST SP 800-63).
An attribute or set of attributes that uniquely describe a subject within a given context. (NIST SP 800-63)

b. **Digital Identity** - a unique fact of being who or what a person is IN the digital world. It may be connected to a real-world Identity (thus being a digital twin) or may not (alias/persona) (NIST SP 800-63). digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts (NIST SP 800-63-3, NIST SP 800-63B)
c. **Digital Identifier -** Unique information used to identify people, organizations, or things within a context. For example SSN, e-mail, SASID, LASID. A digital identity can have more than one digital identifier. (NIST SP 800-63)
d. **PII** - Personally Identifiable Information is any item, collection, or grouping of information about an individual that is maintained by an organization, including identifying information, education, financial transactions, medical history, Social Security Numbers, and criminal or employment history. (NIST SP 800-163 under the Personally Identifiable Information document: NIST SP 800-122)
e. **Personal Information** - PII, demographics, and linked event information. Some information becomes personal in context (such as small group size aggregates).
f. **Learner Information -** Information about a learner. GDPR definition of "Personal Data: Any information relating to an identified or identifiable natural person.[1]
g. **Privacy Rights -** Rights of a person to control access to and use of their personal information. More formal definition: “the right of a person to be free from intrusion into or publicity concerning matters of a personal nature” - Merriam-Webster Dictionary
h. **Authentication -** Actions and mechanisms that can authenticate the identity of a person that includes information about an authentication provider, the login identifier used to authenticate a person's identity, and other information related to authentication of a person’s identity. (NIST SP 800-63) Digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. (NIST SP 800-63B)
i. **Authorization -** the authority to access data or services given to authorized entities. (NIST SP 800-37)
j. **Access Control -** the protocols in a system that limit access to data or services to authorized entities. Information about a data system or application that an authenticated person or system may access.
k. **Self-sovereign identity** - An identity system architecture based on the core principle that Identity Owners have the right to permanently control one or more Identifiers together with the usage of the associated Identity Data.
l. **Information Security -** systems of controls designed to enforce privacy access controls and operational continuity.
m. **Data Controller.** the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.[2]
n. **Data Steward/Processor** - a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of a Data Controller[3] and has responsibility to have proper security for privacy access controls.
o. **Trust** - a person or system’s ability to rely on something from another. Fiduciary trust can be delegated from one entity to another.
p. **Verifiable Credential** - A verifiable credential is a tamper-evident credential that has authorship that can be cryptographically verified.

[1] GDPR
[2] GDPR
[3] GDPR. Also https://www.dama.org/content/body-knowledge)

q. **Federation** - data structures or processes that are logically contiguous, but may exist across multiple physical locations or assets, which can also change over time. Federations require a registration and discovery service to reconstitute all of the parts into the logical whole.

2.2 Logical Model



Thanks Brandt. Based on yesterday's exchange, I have made some updates to the list. I think the "types of functionality" is a key part of a conceptual architecture. TLA groups them logically, but the actual physical component allocation may change from site to site

Education 3.0 Base Document

1. Student Management
    a. archived records/transcripts
    b. assignments
    c. attributes
    d. Identity Credentials and access management
    e. path planning
    f. credentials and portability

2. Content/Activity* Management
    a. registration
        i. creation
        ii. curation
        iii. organization
    b. advertisement
    c. verification
    d. modality
    e. Metadata/purpose

3. Learning Management
    a. adjudication
    b. adaptation
    c. session control
    d. technical control

4. Training Management
    a. curriculum control
    b. certification/archival
    c. utilization

5. Configuration management
    a. user data
    b. curriculum
    c. content/activities and metadata governance
    d. job requirements/ competency

6. Resource Management
    a. requirements
    b. request/reserve/sched
    c. verification
    d. ordering/ERP

7. Competency Management
    a. job/work requirements
    b. dependencies and networks
    c. competency state calculation
    d. credentialing and verification
    e. credential alignment
    f. skill decay/proficiency

8. Decision Support
    a. learner performance
    b. curricular performance
    c. resource utilization
    d. cohort performance
    e. Competency Feedback/Credential Integrity

Key: Author Time Data Run Time Data Run-Author Time Data

In TLA we call the content/activity/alignment tuple an "experience"

Learning Management Systems (LMS) are e-learning platforms for the launch of online or digital courseware and the recording of course completions by learners. As these still encompass the older factory model, they often represent "walled gardens" of vendor-specific technology that provide all of the software functionality within a given learning solution. They can be extended with other related systems, such as Human Resources management, or cost management systems, but these typically rely on proprietary interfaces, and require solutions provided from a limited set of vendors. At some level, the functions performed by an LMS are required in any learning solution, but it is possible to move away from the closed product-based approach to an ecosystem of related data and devices that can grow, change and expand over time in response to the needs of learners and the technologies available.

The promise of a "future learning ecosystem" should release learners and institutions from the single-vendor and technology obsolescence constraints of legacy LMS based solutions. A true ecosystem enables an "any device, anywhere, any time" approach that allows the composition of hardware and software elements to change in response to need, innovation, or other circumstances, including the locations of the learners as they move through their careers. Enabling this ecosystem requires three things:

1. A way to enable the constantly changing collection of humans, hardware and software to manage the “state” of the learning experience in a way that doesn't require a specific component to be “in charge.”
2. A way to normalize the learner data generated and consumed by devices so that the person performing the learning, the digital experience providing the learning, and the impact of the learning on performance can be understood in a globally unambiguous way.
3. A way to visualize the relationship between features, components and interfaces to understand how to convert existing learning stacks to the ecosystem, and migrate them to newer technology over time.

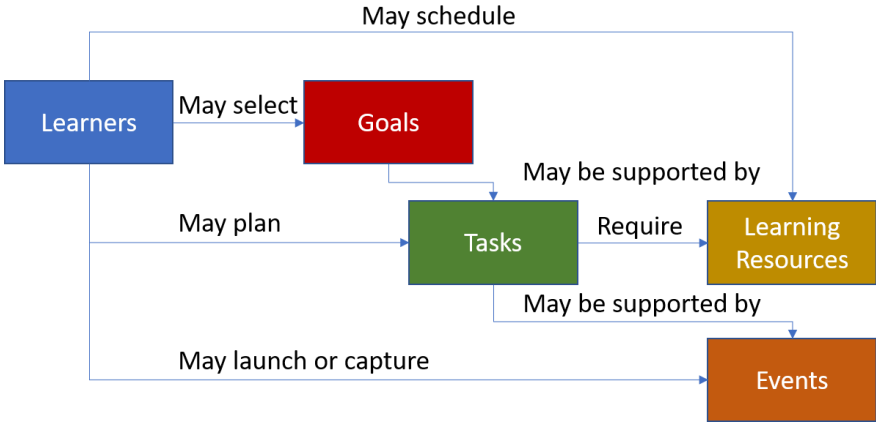
In talking about managing the execution of a process over time, we typically think in terms of “state.” State describes a system’s response to external stimuli that will need to change over time. “Stateful” systems must preserve the history of changes, because the correct next action is dependent on the actions prior to that point. In “stateless” systems the only thing governing behavior is current state (like a light switch can either be on or off, regardless of how many times it has been flipped).

In proposing a “learner centric” model for education, it seems logical to propose a *learner state model*, as opposed to a *factory state model*, as the central organizing principle for the technical concept of execution (CoE). The value of this approach is that *learner state* can be captured as the learner interacts with technology, and it doesn't matter which specific technology they interact with, only the purpose of that interaction. From the perspective of the hardware and software, the system is stateless, and thus simpler; no one component needs to be in charge of state management.

The value of tracking learner state, moreover, is that in the constructivist learning model, the path taken to gain knowledge is important, because knowledge is constructed in relation to other knowledge; thus history, and the statefulness it implies, is important. The exact configuration of hardware and software present needs not be fixed. Different organizations with their own solutions, and solutions that change over time, can accommodate the same overall CoE, because they are responding to the overall learner state, not their own technical states. Thus, a true ecosystem is possible - governed only by contracts specifying modes, and presentation of data interfaces. The only system component that must be present is the learner. All other potential components and data stores are loosely coupled and stateless, only reacting to external stimuli as received.

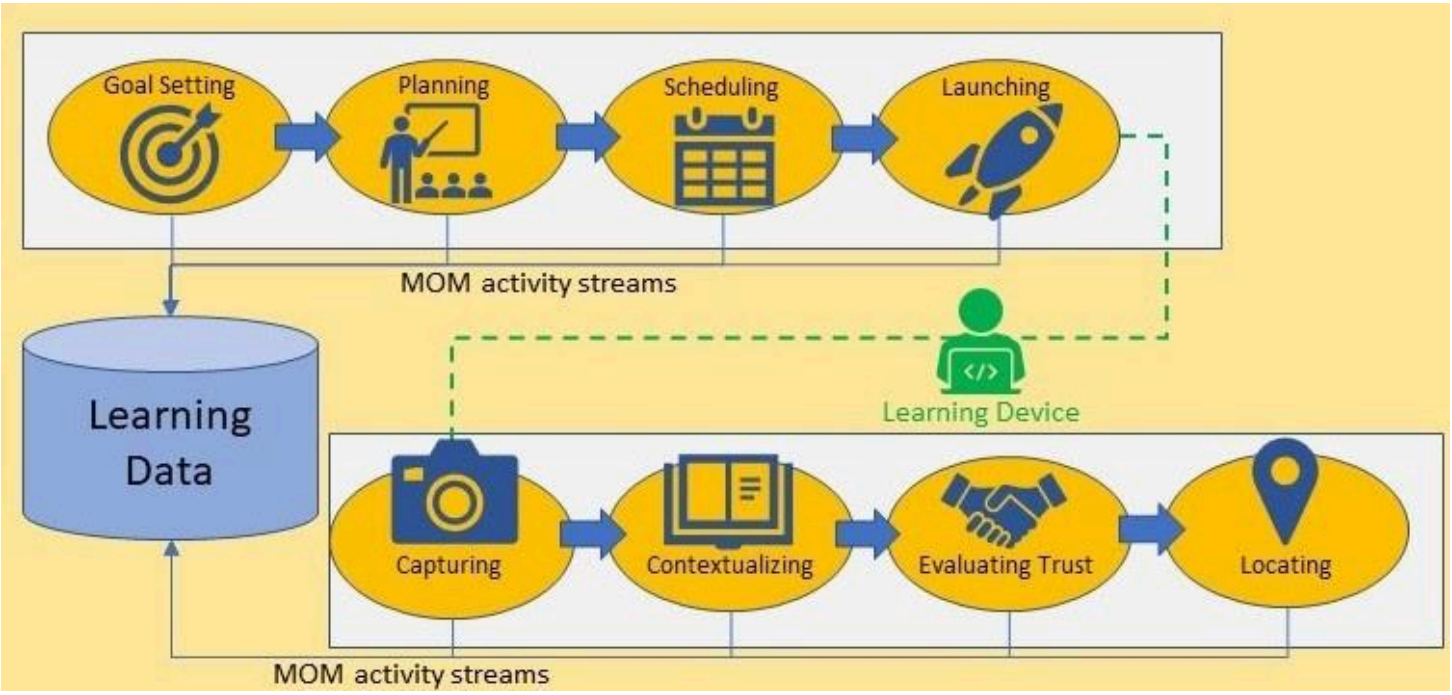
“learning thread” is another useful concept for understanding a continuous linkage of related learning activities for an individual learner. Learning is a continuous activity that rarely in practice is partitioned into linear seamless chunks. A given learner may experience multiple threads simultaneously, at different levels of complexity and completeness, such as when participation in a formal learning course includes a group project and independent study of a related concept. The following figure depicts the arrangement of concepts and relationships defining learner state.

The following figure depicts the arrangement of concepts and relationships defining learner state.



- **Goals** define the purpose of the learning event in terms of a network of one or more competencies, credentials (which may include subordinate competencies), or jobs (which may require subordinate credentials and/or competencies). Goals are an arbitrarily deep hierarchy that comprise a “milestone” along a lifelong learning path. For example, obtaining the credential of *Bachelor of Science* may be comprised of several competencies.
- **Tasks** define the instructional setting that can help achieve one or more goals. Tasks are organized to support goal hierarchies in a mutually supporting way. Task definition is analogous to course design in the factory model, where instructional design principles are applied. In the learner centric model, metadata provides clues to learners or instructors to structure the learning experiences to achieve goals.
- **Learning Resources** include classrooms, simulator time, consumables, observers or instructors, or anything representing an element required for the instruction that is subject to scarcity, and thus requires scheduling.
- **Events** capture the actual performance of the experience. Events consume or reserve the indicated resources for the period required to complete the event.

The TLA learner state model accommodates both legacy and modern models of learning. At the high level, the learner state model distinguishes between formal or deliberate learning, and informal learning. Modern learning theory recognizes that a great deal of learning has become "incidental”, conducted on the job, based on pop-up requirements or opportunities, or in response to a personal motivation, rather than a deliberate plan. "Intentional” learning is similar to the legacy factory model, however, in heutagogy, the learner is actively participating in the analysis and design activities that used to be the purview of the professional curriculum designer, so instead of “formal” curriculum, the learner may pursue an “informal” collection of self-identified goals, or pursue organizational goals loosely defined but in a user planned or “nonformal” way. In general, this intentional cycle includes the setting of performance goals the planning of learning experiences to achieve the goal(s), scheduling of resources required for the experience, and then conducting or “launching” the experience. Common to both intentional and incidental learning is capturing the results of the event, contextualizing the evidence provided by the event within the learner’s current progress and goal set, evaluating the trust level of the reporting systems, and updating the competency and state, or “locating” the learner based on this new evidence. This flow of learning activities is shown below in the learner object life cycle. Each sequence of Goal-Task-Event represents a fine grained “Learner Object” that defines a single thread of learning as it proceeds through the life cycle.



The learner object lifecycle represents the learning path for learners anywhere along the continuum from classical pedagogy to modern theories of self-regulated learning. The lifecycle is captured in an experience Application Program Interface (xAPI) profile and a pending IEEE standard. This profile is called the **Master Object Model (MOM).** The MOM specifies JSON statements for encoding the potential sequence of actions through the learner object lifecycle. This proforma sequence helps to normalize performance data and evidence of competency and credential so that disparate data can be evaluated using enterprise analytics.

The learner state model includes the following phases, as shown in the figure above:

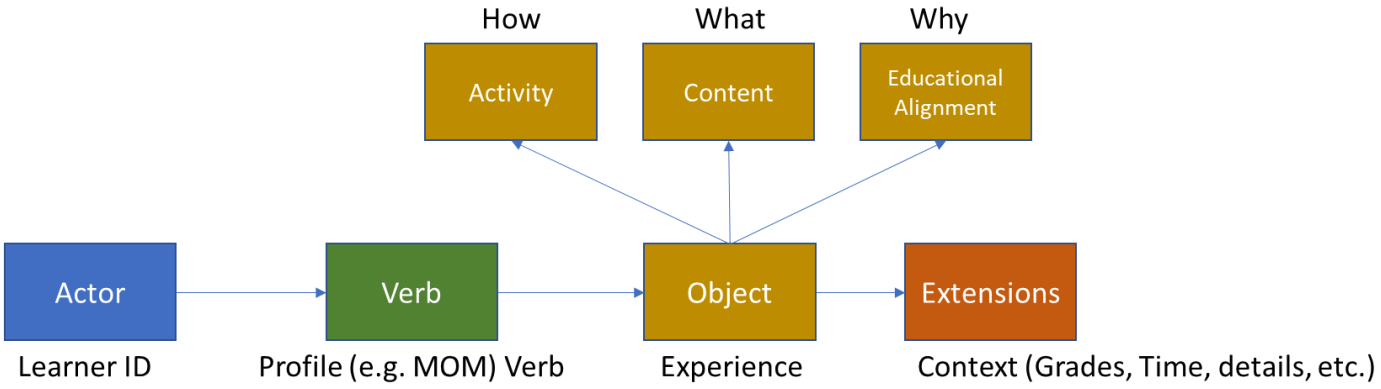
1. **Goal Setting** - **Goals** are the assignment of individual or sets of tasks, knowledge, skills, abilities, and other behaviors (i.e. competencies) required for a learner to obtain a credential or perform a job. Goals may be requested or selected by the learner (self-regulated learning), assigned by an instructor (or supervisor, observer, or other mentoring figure), or implicit in a traditional curriculum (i.e. “learning objectives”).
2. **Planning** - Planning assigns **tasks** to achieve goals, tasks are the assignment of a collection of learning resources to satisfy the goal. This may be an ordered or unordered set. Legacy courses are a special case of ordered set, according to their packaging and labeling specifications. Planning may be performed by instructional designer as they create a course, dynamically by instructors crafting learning experiences, reviewed by the learner to achieve or support their goals (e.g. self-directed learning) or shared socially by learners exchanging lists of learning aids.
3. **Scheduling** - Scheduling includes verification and reservation of the *resources* required to execute the planned task. A scheduled task is an event. These resources might be a web service address, a classroom and instructors, or a laboratory and observers.
4. **Launching** - Launching is the process associated with activating, performing, or reserving and executing resources required to conduct learning. It includes generations of the artifact of the *event*. (e.g. launching the content or starting the activity)
5. **Capturing** - Capturing includes the generation of the archived artifacts (e.g. xAPI statements) of the event, its time, components, purpose, participants, state, and results. Capturing may include events which were not deliberately

planned (e.g. a learner just looks up something interesting on an instrumented YouTube™ player). Events stay current until they are completed, terminated or abandoned to end the current learning session.

6. **Contextualizing** - Contextualization includes the path that was used to conduct the learning: Was it directed by an instructor? Suggested by a colleague? Investigated by the learner themselves as part of self-directed or self-regulated learning? Was it performed in a classroom or in situ? Contextualization helps build models of learner preference as well as evaluate effectiveness of instructional settings.
7. **Evaluating Trust** - Trust is captured based on the nature of the learning: Was it written exposure to the concepts? Was it performance in a simulator? Was it on the job? Was it an assessment? Who verified the answers? Was it self-asserted? The trust model builds confidence in the associated competencies. Trust ensures credentials are issued by properly authorized individuals, and that the credential can be safely used as a proxy for competence where applicable.
8. **Locating** - Location is the update of the learner's path, competency and credential state. The location may show completion of goals or tasks within the planned learning path, and it may be an update to conferred credentials or asserted competencies that will define the set of requirements and options for the next segment of the learning path. Location also includes resolving the state of assigned goals and tasks.

Each thread of learning can independently follow this learner object lifecycle. The complexity of the relationship between goals and tasks, since goal networks can be arbitrarily deep, represents a continuum of learning strategies or "microcurricula" that may exist nested within each other or an overarching curriculum. A classic example is a study group sharing ancillary content to help each pass a difficult set of concepts within a class. The class represents a formal, intentional setting, but the study group is informal. If one of the study members brings learning from an outside but related experience, it could also include incidental learning. Thus, each thread of learning represents a distinct intersection of the learner with elements of their learning environment, and provides keys to not only the depth of capability in knowledge and skills (showing the full learning path, not just a final grade or credential) but also the learner's preferences for media types and social settings for regulating or improving their learning. Each learner will potentially generate a large amount of normalized data for their lifelong learning journey, and enterprises will have access to large longitudinal data sets for evaluating the efficacy of education and training provided.

The accumulation of large, clean data sets is central to machine learning. These data are required for "training" of artificial intelligence algorithms, or for providing sufficient representative use-cases for the applied statistical models used in machine learning. Modern database and parallel computing technologies facilitate the collection, storage and retrieval of large data sets. Using the learner object lifecycle and its related learner state helps normalize the flow of learning events, but these learning events are composed of the grammatical triple of "someone" "doing" "something" or actor-verb-object. In the TLA, this triple is captured using the Experience Application Program Interface (xAPI). At its core, the xAPI is a Javascript Object Notation (JSON) format for capturing logical triples of noun-verb-object as set of resolvable references to lists of possible "who", "what", "why", "where", "when", "how" and "how much/well" descriptions of any event, including experiences associated with learning.



The basic syntax of capturing performance is represented in slightly different ways in the multiple existing standards for capturing performance data, such as the IEEE (P)9274 xAPI.The xAPI introduces the concept of profiles to standardize the use of verbs and the syntactic structure of actors, objects and extensions. As discussed previously, the MOM provides a profile to normalize the sequence of activities that comprise a given learning thread. This use of MOM verbs establishes a normalized *chain of evidence* for performance that can be used to make *assertions* of competency. As the learner proceeds through the object lifecycle, they will have identified candidate *experiences* that generate *events* when they are actually experienced. These experiences are comprised of an educational alignment (i.e. the goals addressed) answering *why* the experience is necessary, an activity type (e.g. a lecture or simulator) answering *how* the learning is experienced, and a content element (e.g. lesson plan, scenario) defining the specific learning provided and answering the *what* question.

FICAM…

Device Registry and Zero Trust ...

Together, this suggests four data structures that archive the elements and results of learner lifecycle messages that are created, associated, or captured in the process of following the learner state model.

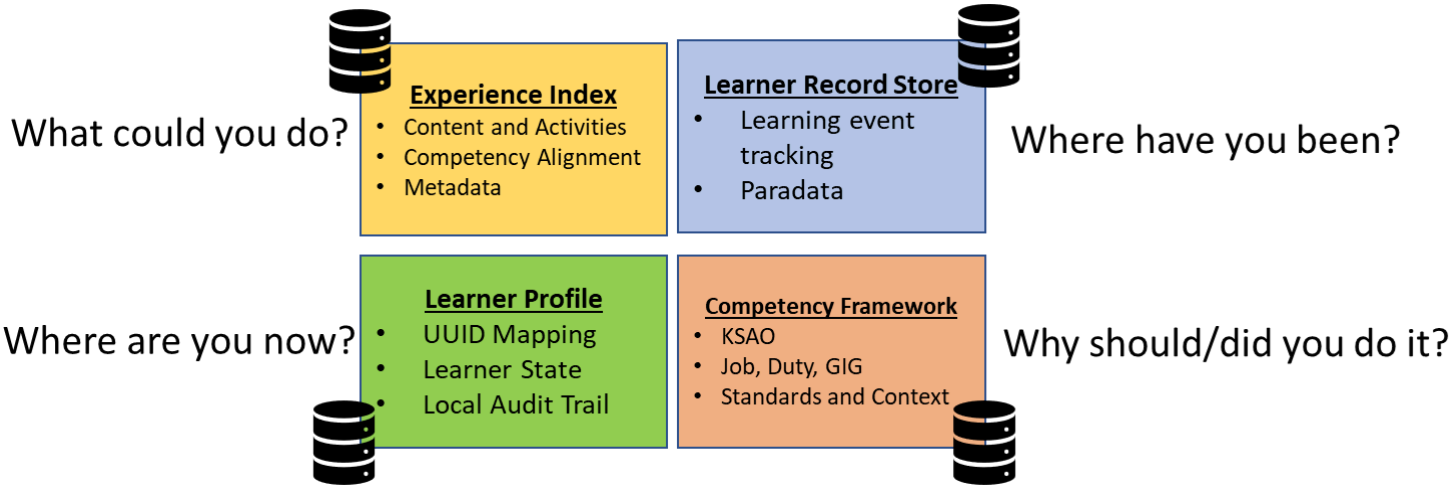
1. **The Learner Profile:** captures current learner identity (i.e. actor labels) with references back to authoritative sources of identity, and locally relevant learner data. Learner profiles are the repository of final assertions of competency and conferral of credentials, which is the summative portrait of learner state. The learner profile may be federated across multiple physical locations when tracking a lifelong learning journey. Local repositories also store formative learner states as a function of completed and in-work activities (goals, tasks, and events). The metamodel for learner profiles is IEEE 1484.2.

2. **Competency Framework:** captures the human performance elements and levels (e.g. standards) required to demonstrate performance on the job, in a role, at a particular level of mastery. The elements are arranged to show how progress may be made toward goals. Competencies are arbitrarily deep sets of knowledge, skills, attributes, and other characteristics (KSAOs), the relationships between them (at a given level of mastery) to a set of standards and under prescribed contexts. Competency Frameworks capture the elements used to define an *educational alignment.* The metamodel for competencies is the IEEE 1484.20.1.

3. **The Experience Index:** extends legacy content models for describing learning and allows for alignment to instructional purpose. Experiences recognize that *learning content* addresses subject matter, and *learning activities* address modality of experiencing the subject matter, which will have an impact on the type and efficacy of KSAO retained (i.e. confidence

in demonstration of competency). This can include traditional classrooms as well as on the job work, simulators, and live exercises. Some experiences may combine the same content in different contexts (such as the difference between reading the engine manual and reading the manual while taking apart the engine), each of which provides unique characteristics and thus different trust levels in demonstrated competency. The metamodel for experience indices is IEEE 1484.12.1.

4. **The Learner Record Store**: the server-side component of the xAPI specification. The LRS captures and validates the xAPI statements that define the learner state and provide evidence of competency and credential. If the LRS is part of the "core" architecture (defined below) it should comply with the learner object lifecycle state model. "Core" LRS may be federated with edge system LRS (see below) that rely on any user-specified profile. Edge systems may use LRS, or may rely on a different technology.



The TLA proposes a "core/edge" architectural paradigm for *visualizing* the relationship between hardware and software components within a learning system or ecosystem. The data structures listed above represent "core data." Core functions are those control elements, services, functions, modules, etc. that maintain those data structures and provide "ledgering" services between data so that the ecosystem can allow for heterogeneous learning experiences to be shared and analyzed. Back-end services provide the integration to network services to ensure that the loosely coupled devices of the learning ecosystem, the normalized core data, and housekeeping core functions, can "find" each other and maintain semantic consistency in referencing the actors, verbs, and objects encoded in the xAPI statements. Learning, performance adjudication, and analytics occur in the edge devices. Input devices include all the possible learning settings or opportunities to capture observation or assessment data. A normalized xAPI profile (the MOM) allows any mix of devices or core services to push the learner state forward, and the number of simultaneous learning actions is only limited by overall performance, because the federation of devices and data as a whole is stateless.

Within the core are several "functional groups" as described below. Depending on the actual composition of any particular system, edge and core functions may be combined in the same component. But the core/edge philosophy governs future microservice migration efforts, and helps evaluate the scope of changes, whether they must be managed at the local, regional or global level.

- ***Competency Management*** is associated with defining what the learner must be able to do, within a *competency framework,* to be considered proficient to perform work in the worksite context. It is composed of KSAOs, performed at a set of standards, under a set of contexts, for each level of mastery. While adjudication of performance is considered an

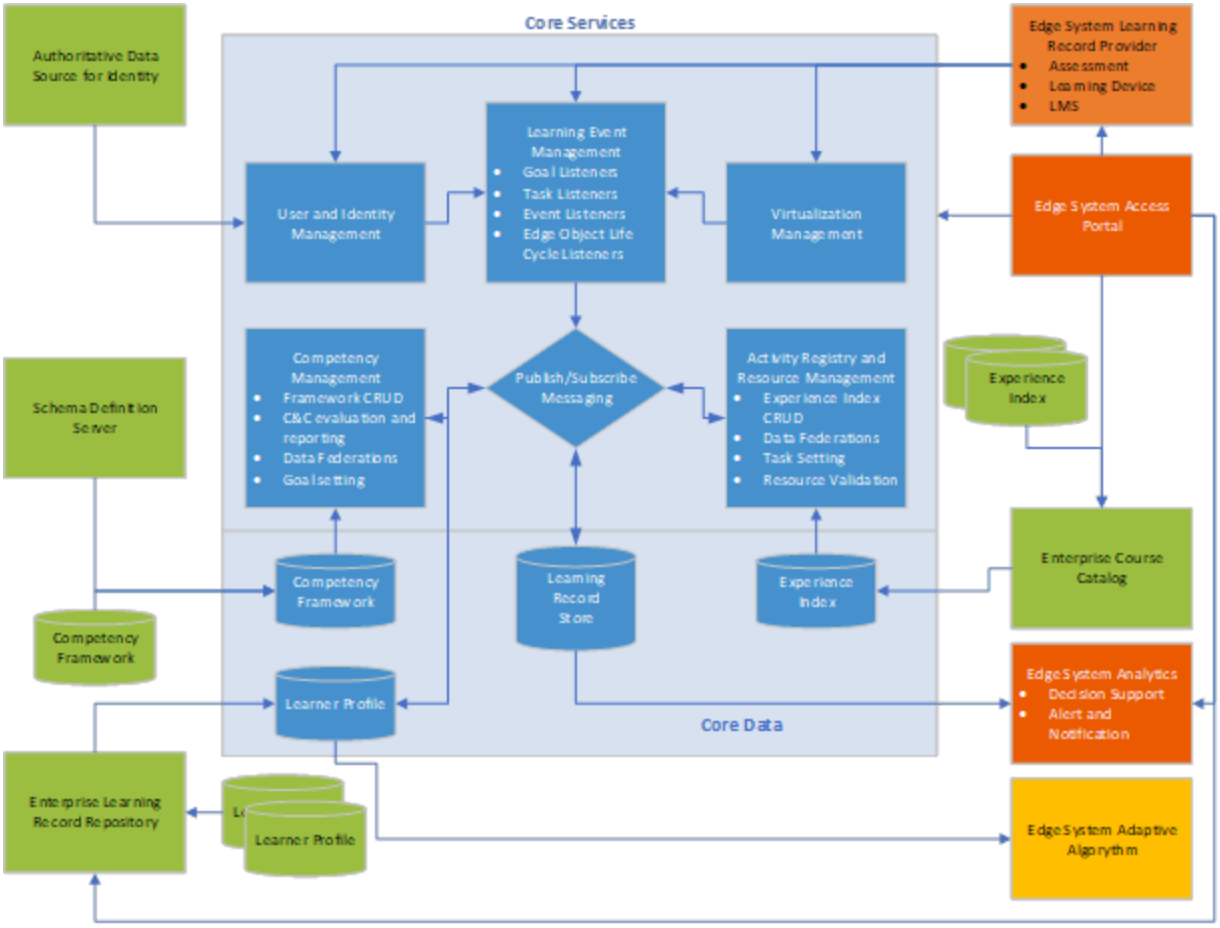
edge function, calculation of the relationship between granular levels of performance and the overarching proficiency at performing in a job, duty or gig is a constituent function of this group. Other constituent functions include affirming the completion of credentials based on this evidence, and creating the digitally signed conferral of the credential. Competency objects and relationships are stored in the competency framework, and summative results of competency and credentials are stored in the learner profile.

- ***Activity Registry and Resource Management*** is concerned with cataloging the available opportunities to enhance or demonstrate competence, including experience of digital learning resources, assessments, simulation events, observations from on-the-job training and job aids/work experiences. Resource management addresses scheduling of scarce consumables, simulator time, classroom space, instructors and observers required to conduct events that convey the experiences, as aligned with an educational purpose. The activities, content, resources, and educational alignments comprising the experiences are stored within the *experience index*.

- ***Learning Event Management*** includes those functions concerned with executing or tracking the *learner lifecycle* and creating the necessary records to define a *persistent learner state*. Learning events may assign educational goals, or select from existing goals, assign tasks to instruct, assess or verify demonstration of the educational objectives represented by those goals, schedule or prioritize exercises to accomplish the tasks, and capture and evaluate the impact of events archived in xAPI on the learner competency and credential state. Learner state and events are captured in the Learner Record Store (LRS). Learning event management can be visualized as a set of “listeners” that connect to specific learning technology to contextualize how learners and instructors interface with any given organization’s learning stack, within the normalized model of the learner state object lifecycle.

- ***Back-End Services – User and Identity Management*** are those functions associated with federated identity credential and access management (FICAM). Identity management ensures that users are labeled unambiguously within archived performance data. Credential management ensures that the actual person accessing resources is the same person as represented digitally. Access management is associated with privacy and security, and includes the use of “identity groups” and “collective identifiers” (e.g. classroom 23) to manage multiple interests.

- ***Back-End Services – Network and Virtualization Management*** are those functions associated with operation in a networked environment, especially a cloud environment. It includes services associated with dynamic IP endpoint and file management, registration and maintenance of network resources, and other services. Many of these are available in Platform-as-a-Service (PaaS) models available today.


Core Services
Authoritative Data Source for Identity
Edge System Learning Record Provider
Assessment
Learning Device
LMS
User and Identity Management
Learning Event Management
Goal Listeners
Task Listeners
Event Listeners
Edge Object Life Cycle Listeners
Virtualization Management
Edge System Access Portal
Competency Management
Framework CRUD
C&C evaluation and reporting
Data Federations
Goal setting
Publish/Subscribe Messaging
Activity Registry and Resource Management
Experience Index CRUD
Data Federations
Task Setting
Resource Validation
Experience Index
Schema Definition Server
Competency Framework
Learning Record Store
Experience Index
Enterprise Course Catalog
Competency Framework
Learner Profile
Edge System Analytics
Decision Support
Alert and Notification
Core Data
Enterprise Learning Record Repository
Learner Profile
Edge System Adaptive Algorythm

Section 3. Guiding Principles

As an active participant in the new Internet of Education, we ask that you review and pledge your commitment to the following core principles:

3.1 Contract for the Web

1. **There is only one global Internet -** The Internet is a network of networks. We all need to work together to protect the web from abuse and ensure it benefits humanity by adopting the Contract for the Web[4]
   - 1.1. **Access.** Ensure everyone can connect to the internet
   - 1.2. **Availability.** Keep all of the internet available, all of the time
   - 1.3. **Privacy.** Respect and protect people's fundamental online privacy and data rights
   - 1.4. **Affordability**. Make the internet affordable and accessible to everyone
   - 1.5. **Trust.** Respect and protect people's privacy and personal data to build online trust
   - 1.6. **Public Good.** Develop technologies that support the best in humanity and challenge the worst
   - 1.7. **Collaboration**. Be creators and collaborators on the Web
   - 1.8. **Civility.** Build strong communities that respect civil discourse and human dignity
   - 1.9. **Open.** Fight for the Web. Fight for the Internet of Education to be an open, global public resource for people everywhere, now and in the future.

3.2 SSI and Access Control

2. **Self-Sovereign Identity & Access Control[5].** Each personal learner record is dual controlled by the issuer and the learner.
   - 2.1. **Issuer Access Control.** The issuer has legal responsibility to control access to data within the issuing organization and get explicit consent from the learner or their legal guardian to share the personal record outside the organization except where specifically authorized by regulation or law.
   - 2.2. **Learner Access Control.** Within the bounds of the law, a person with learner records (or their legal guardian) has authority to control access to their personal learner records and must be able to curate records in sets and share with particular entities for a particular purpose and period of time.
   - 2.3. **Chain of Custody.** Once a record is shared with a third-party, there is a chain of custody where that information becomes part of the business record of the third-party. While new access after a particular period of time might be revoked, storage that occurred during permitted access period cannot.
   - 2.4. **Aggregated Dissociated-Identity data**. Where required by local or global policy or regulations, elements of learner data or metadata may be aggregated and dissociated from specific identity and published by issuing authorities with implied consent
   - 2.5. **Operational Security -** the ability to simultaneously reconstruct a complete portrait of learner capability, while minimizing the damage resulting from a single data hack. Military operational security, or corporate competitive advantage can be eroded due to improper disclosure of aggregated performance data, or even metadata with otherwise anonymized identity.

[4] Adapted from Berners-Lee, Tim, Contract for the Web, 2019

[5] Adapted from Hamilton, Kim, T3 Innovation Network Self-Sovereign Identity Principles, 2020, Ten Principles of SSI, ASU Trusted Learner Network Principles

3.3 Distributed Network Control

3. **Distributed network control -** Like the Internet, it is essential to trust that no one organization assert more control than is needed to enable interoperability between nodes; the power of the weak center.

3.4 Open Stand

4. **Collaboration on Open standards -** Technical and academic standards should be published without restrictions on use by organizations that align practices to OpenStand[6]. Shared technical documentation should follow five principles:
   - 4.1. **Cooperation.** Respectful cooperation between standards organizations, whereby each respects the autonomy, integrity, processes, and intellectual property rules of the others.
   - 4.2. **Adherence to Principles.** Adherence to the five fundamental principles of standards development:
     - **Due process.** Decisions are made with equity and fairness among participants. No one party dominates or guides standards development. Standards processes are transparent and opportunities exist to appeal decisions. Processes for periodic standards review and updating are well defined.
     - **Broad consensus.** Processes allow for all views to be considered and addressed, such that agreement can be found across a range of interests.
     - **Transparency.** Standards organizations provide advance public notice of proposed standards development activities, the scope of work to be undertaken, and conditions for participation. Easily accessible records of decisions and the materials used in reaching those decisions are provided. Public comment periods are provided before final standards approval and adoption.
     - **Balance**. Standards activities are not exclusively dominated by any particular person, company or interest group.
     - **Openness**. Standards processes are open to all interested and informed parties.
   - 4.3. **Collective Empowerment.** Commitment by affirming standards organizations and their participants to collective empowerment by striving for standards that:
     - are chosen and defined based on technical merit, as judged by the contributed expertise of each participant;
     - provide global interoperability, scalability, stability, and resiliency;
     - enable global competition;
     - serve as building blocks for further innovation; and
     - contribute to the creation of global communities, benefiting humanity.
   - 4.4. **Availability**. Standards specifications are made accessible to all for implementation and deployment. Affirming standards organizations have defined procedures to develop specifications that can be implemented under fair terms. Given market diversity, fair terms may vary from royalty-free to fair, reasonable, and non-discriminatory terms (FRAND).
   - 4.5. **Voluntary Adoption.** Standards are voluntarily adopted and success is determined by the market.

[6] Adapted from OpenStand

3.5 Learner-Centered Equity

5. **Learner-centered equity** - Any time, any place, any pace learning pK-12w should be valued. We need a way to capture academic and applied competency-based achievements from many issuers to enable personalization of learning pathways.[7]
   - 5.1. Education is a basic human right and Open EdTech can best enable equitable access to quality education for everyone on Earth
   - 5.2. We strongly support open standards and interoperability.
   - 5.3. Control of education technology should be collectively shared.
   - 5.4. We want to empower educators and learners to improve our world.
   - 5.5. Education should drive technology, not the reverse.
   - 5.6. We encourage strategic alliances and networks for those around Open EdTech.
   - 5.7. Open EdTech should be the most well-designed, competitive and sustainable technology available.
   - 5.8. We embrace the best of open source practices.
   - 5.9. We want to build on what already exists, including standards and tools.
   - 5.10. Openness in EdTech must include transparency about sustainability models.
   - 5.11. We work closely with our diverse communities to define our goals and roadmaps.
   - 5.12. We understand and respect diversity when creating and recommending Open EdTech tools and resources.

3.6 Ontologies and Assertions

6. **Ontologies and Assertions.** A learner record contains general descriptions of achievements (ontologies) and specific assertions by issuers about learners (assertions). Ontologies (competencies/skills, credentials, pathways) and assertions need not be published by the same issuer.
   - 6.1. **Ontologies.** Achievement descriptions (competencies and credentials) and other experiences and behaviors should generally first be defined as linked data and crosswalked to other descriptions to enable comparability.
   - 6.2. **Competencies Descriptions.** Competencies (aka, skill, knowledge, ability, outcomes, learning targets, academic standards) describe capabilities or behaviors that a person may learn or be able to do within a given situation and environment along with definitions of the potential levels of mastery and metadata related to that statement.
   - 6.3. **Credentials Descriptions.** Credentials describe qualification, achievement (competencies), personal or organizational quality, experience, attribute, or aspect of an identity typically used to indicate suitability.
   - 6.4. **Assertions**. Assertions (aka claims or awards) can be made to about either competency descriptions (competency assertion) or credentials descriptions (credential award or credential). Assertions should be considered personal data.
   - 6.5. **Verifiability.** Assertions should be verifiable as being from the issuer either through reflected site (hosted) or distributed ledger (signed). Assertions that are digitally signed by the issuer using the private key for the issuer's DID that. If this DID is published on a public ledger that is sufficiently trusted, it can be verified by any verifier. The role of the distributed ledger is DID registration and verification.
   - 6.6. **Transcript**. A transcript is an immutable array of assertions which cannot have records removed without altering the validity of the whole.

[7] Adapted from Open Edtech Principles

6.7. **Directed Acyclic Graph (DAG)** - a mathematical concept that specifies a network of concepts with multiple inheritance between concepts, or the ability to "track back" to earlier concepts. DAG are used to describe competency relationships or resource relationships to competencies.

6.8. **Immutable**. The data in the Network are immutable. Once an accomplishment is asserted by a TLN member entity, it cannot be manipulated or changed.

6.9. **Always Up-to-Date.** An issuer's assertion about an accomplishment can be supplanted by either an expiration or revocation if the record type supports such an update.

6.10. **Present Current Info First.** Always presents the most current view of a learner's record. The history ledger transactions are retained and can be viewed by the owner of those records.

3.7 Legitimacy Principles

7. **Legitimacy Principles** - GovLab
   - 7.1. Transparency
   - 7.2. Accountability - dispute resolution
   - 7.3. Participation - inclusivity, equity, underserved
   - 7.4. Representation - proportional weight
   - 7.5. Effectiveness -

Section 4. Technical Meta Model.

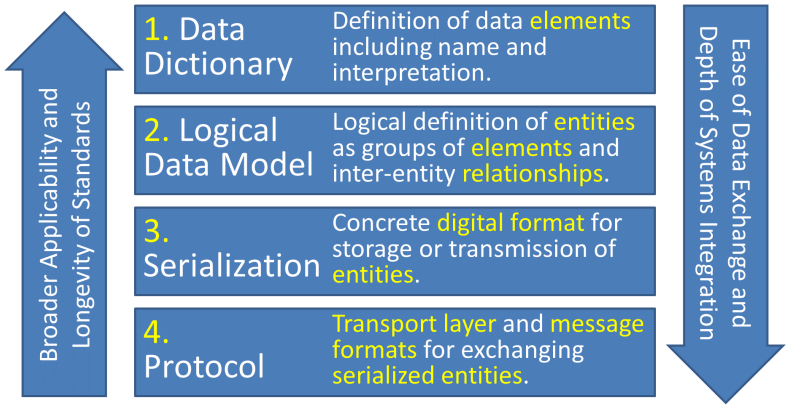
Interoperable systems are built on a foundation of data standards. The models presented here are helpful when interpreting standards to understand how they fit together. When developing standards and specifications these models can guide standards-makers to be deliberate about which parts are addressed by the new initiative.

4.1 Standards and Specifications

A specification is a technical document that describes how a system should work, how data are encoded and transmitted, or how systems operate. A standard is a specification that is managed and governed by an organization.

4.2 The Four-Layer Framework for Data Standards

There are four layers of work that fit together in a data design effort. Not all layers need to be present in a particular standard, but each layer must be addressed in a functional system.



1. **Data Dictionary:** This is a list of data elements; each with a title, definition, and sometimes a format. For example, Title: “Birth Date”; Definition: “Day an individual was born.”; Format: “year-month-day”.
2. **Logical Data Model:** Defines entities as collections of properties. Each property is an element in the data dictionary. In other words, an element becomes a property when it’s associated with an entity. The Logical Data Model also defines relationships between entities. For example, a Student entity might include the properties “name”, “birthdate”, “gender”, “address”, etc. The Student entity type would have a many to many relationship with the “Class” entity type.
3. **Serialization:** This is a concrete format in which entities may be stored or exchanged. Two popular frameworks for serialization are XML and JSON but custom serializations are also common. There may be (and often are) multiple serializations of the same data model. Synonymous terms include “physical data model”, “binary format”, “marshaled format”, “binding”, “storage format”, or “encoding”.
4. **Protocol:** The infrastructure over which the Serialized representations of Data Model Entities are accessed and exchanged. A typical protocol contains several sub-layers, hence the term “protocol stack.” Typical sub-layers include Messaging Framework (e.g. Publish/Subscribe, Request/Response, Create/Read/Update/Delete, REST, SOAP, Enterprise Service Bus), Transport (e.g. HTTP or FTP) and Network (e.g. TCP/IP).

The task of systems integration becomes easier and less expensive as more layers are standardized. When all four layers are addressed, systems integration should be a matter of proper configuration settings with no custom programming required. On the other hand, standards (or portions thereof) that focus on the higher levels of the stack have broader applicability. For

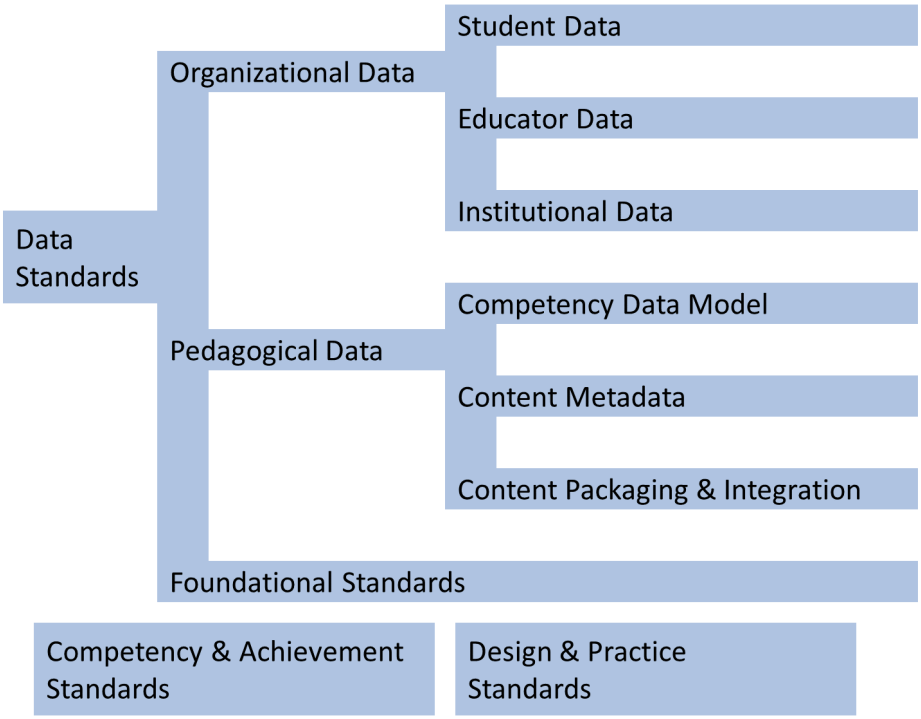
example, a principal benefit of a standardized Data Dictionary is reducing the risk that data may be interpreted differently by different systems. So, just standardizing the data dictionary achieves far-reaching benefits. Because of this, it's important to clearly delineate between the layers even when a single standard or specification addresses more than one.

4.3 Taxonomy of Learning Standards

EdMatrix uses a taxonomy with the following categories for learning standards:

- Data Standards
- Competency & Achievement Standards
- Design & Practice Standards

Data standards are further broken down according to the following diagram.



We must pay special attention when assigning categories. For example, the Next-Generation Science Standards (NGSS) is a competency framework containing a set of Competency & Achievement standards. NGSS may be stored according to Competency & Academic Standards Exchange (CASE) which is a Data Standard for the storage and exchange of Competency & Achievement Standards.

Competency & Achievement Standards include state and national standards for primary and secondary education. In the U.S. each state sets its own standards though many of the states have adopted the Common Core State Standards for English Language Arts/Literacy and for Mathematics. Most other countries have nationwide standards the Australian Curriculum or Scotland's Curriculum for Excellence.

In higher education, most college and university systems define their own outcomes though there is a growing movement to adopt competency frameworks defined by professional societies. Examples include Medbiquitous, which publishes standards for health professions, and the Project Management Body of Knowledge, published by the Project Management Institute.

Design & Practice Standards are guidelines and requirements for the development of learning experiences. They include broadly-applicable standards like the W3C Web Content Accessibility Guidelines (WGAG), legal requirements like the Family Educational Rights and Privacy Act (FERPA), and best practices like Universal Design for Learning (UDL).

Section 5. Taxonomy of Use Cases

Mutually Exclusive Collectively Exhaustive (MECE)

Use this structure to organize Implementation Guidance:

	Identity	Planning	Assessment	Learning	Learning Economy
Education provider	**1.1 Directory** - relate programs and agencies, employ and assign staff, and enable parent/guardians to enroll their non-adult learner or adult learners to enroll themselves	**2.1 Achievement Descriptions** - establish the competencies, co-curricular activities, pathways, and crosswalks to other achievement description frameworks that will serve as linked data learning targets and credentials **2.2 Learning Resources/Instructional Materials** - align curriculum and digital instructional materials, learning resources, and assessment items to linked data learning targets to create playlists for multiple pathways.	**3.1 Achievement Assertions** - assert a verifiable achievement level about a learner, referencing a linked-data description of the achievement, based on defined evaluation criteria and protocols	**4.1 Learning Management** - control access to learners' personal information to members and agents of that organization with legitimate educational purposes including learning analytics	
Educator	**1.2 Employment** - begin employment with an education agency and get access to communities of practice and rosters with class sections of learners	**2.3 Lesson Plans** - access district selected content and modify and plan for instructional delivery	**3.2 Evidence**- Evaluate student work and provide evidence for achievement assertions	**4.2 Instructing** - consuming CLR data to individidualize instruction	
Learner	**1.3 Enrollment** - complete my portion of enrollment and gain access to my personal learning records and services	**2.4 Pathways** - select goals and pathways	**3.3 Assessment** - participate in assessments and view results	**4.3 Learning** - access optimal learning experiences in the next 'zone of proximal learning' along the pathway to my educational goals	**5.1 CLR Wallet** - curate verifiable assertions of linked-data description of the achievements and other credentials in a secure 'wallet' and control access to designated education providers and prospective/current employers.
Parent/ guardian	**1.4 Parent/Guaridan Enrollment** - enroll my non-adult learner in a school district or supplemental education provider	**2.5 Individual Education Plan** - participate in evaluation meetings	**3.4 Support** - view assessment results and other achievement assertions and provide support	**4.4 Monitor and Motivate** - ensure basic needs are met and help manage time and motivation to try hard things and ask for help when challenged	**5.2 Consent** - control access to specific portions of my non-adult learner's personal record (by anyone outside of the education provider that issued the record) to specific individuals or organizations for specific periods of time
Employer					**6.1 Talent Signaling** - define jobs based on linked-data competencies and other desired characteristics and requirements **6.2 Job Data Exchange** - match shared verifiable assertions of linked-data description of the achievements and other credentials to identify qualified candidates for positions

- **1.1 Directory** - As an Ed Provider, I want to relate programs and agencies, employ and assign staff, and enable parent/guardians to enroll their non-adult learner or adult learners to enroll themselves
    - 1.1.1 Create Directory
        - W3C DID
        - 1.1.1.A LDAP & Single Sign On Solution
        - 1.1.1.B Active Directory
        - 1.1.1.C Google Federated Identity
        -
    - 1.1.2 Create HR Platform
    - 1.1.3 Create Student Parent/Guardian Enrollment

- **1.2 Employment** - As an Educator, I want to begin employment with an education agency and get access to communities of practice and rosters with class sections of learner

- **1.3 Enrollment** - As a Learner, I want to complete my portion of enrollment and gain access to my personal learning records and services

- **1.4 Parent/Guardian Enrollment** - As a Parent/Guardian, I want to enroll my non-adult learner in a school district or supplemental education provider

- **2.1 Achievement Descriptions** - As an Ed Provider, I want to establish the competencies, co-curricular activities, pathways, and crosswalks to other achievement description frameworks that will serve as linked data learning targets and credentials
    - 2.1.1. Create machine-readable, linked data learning targets and pathways
        - 2.1.1.A CASE
        - 2.1.1.B ASN?
        - 2.1.1.C CaSS?
        - 2.1.1.D Proprietary
            - Certica
            - Ed-Gate
            - ASN
            - Emsi

- **2.2 Learning Resources/Instructional Materials** - As an Ed Provider, I want to align curriculum and digital instructional materials, learning resources, and assessment items to linked data learning targets to create playlists for multiple pathways.

- **2.3 Lesson Plans** - As an Educator, I want to access district selected content and modify and plan for instructional delivery

- **2.4 Pathways** - As a Learner, I want to select goals and pathways

- **2.5 Individual Education Plan** - As a Parent/Guardian, I want to participate in evaluation meetings

- **3.1 Achievement Assertions** - As an Ed Provider, I want to assert a verifiable achievement level about a learner, referencing a linked-data description of the achievement, based on defined evaluation criteria and protocols
    - 3.1.1 Transform PESC transcript to IRL assertions
    - 3.1.2 Instrument ILS to produce IRL assertions
    - 3.1.3 Embed ILR assertion tool
        - 3.1.3.A LTI
        - 3.1.3.A LTI

- **3.2 Evidence**- As an Educator, I want to evaluate student work and provide evidence for achievement assertions
- **3.3 Assessment** - As a Learner, I want to participate in assessments and view results
- **3.4 Support** - As a Parent/Guardian, I want to view assessment results and other achievement assertions and provide support
- **4.1 Learning Management** - As an Ed Provider, I want to control access to learners' personal information to members and agents of that organization with legitimate educational purposes including learning analytics
- **4.2 Instructing** - As an Educator, I want to, consume CLR data to individualize instruction
- **4.3 Learning** - As a Learner, I want to access optimal learning experiences in the next 'zone of proximal learning' along the pathway to my educational goals

- **4.4 Monitor and Motivate** - As a Parent/Guardian, I want to ensure basic needs are met and help manage time and motivation to try hard things and ask for help when challenged
- **5.1 CLR Wallet** - As a Learner, I want to to curate verifiable assertions of linked-data description of the achievements and other credentials in a secure 'wallet' and control access to designated education providers and prospective/current employers.
- **5.2 Consent** - As a Parent/Guardian, I want to control access to specific portions of my non-adult learner's personal record (by anyone outside of the education provider that issued the record) to specific individuals or organizations for specific periods of time
- **6.1 Talent Signaling** - As an Employer, I want to define jobs based on linked-data competencies and other desired characteristics and requirements
- **6.2 Job Data Exchange** - As an Employer, I want to match shared verifiable assertions of linked-data description of the achievements and other credentials to identify qualified candidates for positions"
- **6.3 Forensic analysis of evidentiary chain** – as an employer I want to maintain a high level that credentials can be used as proxies for competence so I need a feed forward mechanism to suggest changes and a feedback mechanism to determine if there are systemic weaknesses in the contexts under which some credentials were awarded.

Section 6. Standards Alignment & Harmonization

6.1 Proposed Relationship of CM4LTS to other LTSC Groups

LTSC Group		Relationship to Conceptual Model
ICICLE	Industry Connections Industry Consortium on Learning Engineering (ICICLE) is an open forum and community-building platform for defining and supporting the profession of Learning Engineering -- the engineers who will design, build, deploy, operate, and maintain the increasingly complex products and systems used in education and training.	ICICLE participants will be asked to review and provide input to the Conceptual Model to ensure that the model reflects best thinking regarding learning.
LOM	Learning Object Metadata: A schema for metadata about learning objects or resources.	LOM will be reviewed to distinguish between event objects and resource objects.
SCORM	SCORM Renewal. Several IEEE standards are included in the broadly-adopted SCORM reference model for learning content portability. This working group is responsible for renewing these standards on their 10-year anniversary, as required by the IEEE Standards Association.	SCORM will be reviewed to distinguish between event objects and resource objects.
CDS	Competency Data Standards (CDS) (P1484.20.1) goal is to elevate existing standards, profile, and augment to establish a reference implementation model that addresses linking of competency definitions to people, pathways, and learning resources (including assessments and digital content). Charter.	CDS will be reviewed to distinguish between event objects and resource objects (see additional detail below regarding Competencies, Credentials, Badges and Assertions

xAPI	xAPI (P92741.1) purpose is to develop a standard to store and retrieve learning activity data streams as required by modern, data-intensive learning technologies. This standard also defines the behavior of a Learning Record Store database. Additional work will focus on a best practices report and standards for xAPI profiles.	xAPI models events. Events are at the heart of the Conceptual Model. xAPI will be reviewed to align with the Model.
AISS	Adaptive Instructional Systems Study Group (P2274) Standards to support adoption of a group of AI-enhanced product categories that includes adaptive/personalized instruction, Intelligent Tutoring Systems, content recommenders, and so on. Three working groups are now defining the conceptual model and terminology; component interoperability specs; and best practices for evaluating these products.	AISS extends LOM, CDS, and xAPI to provide an architecture for competency-based blended learning.
FML	Federated Machine Learning (P3652.1) defines a machine learning framework that allows a collective model to be constructed from data that is distributed across data owners who are not allowed to share the actual data, which is often the case in educational data mining.	
CSDG	Child and Student Data Governance (P7004) Goal is to produce guidance for educators and vendors about the range and nature of constraints on the collection, storage, distribution, and use of student data prescribed by laws and regulations around the world.	
ARLEM	Augmented Reality Learning Experience Model. (ARLEM) (P1589) A content portability standard that specifies a description of workplaces where people learn and/or work, and its “augmentation” with real-time delivery of (and interactions with) instructional content pertaining to the activities and tools in that workplace..	
MLP	Mobile Learning Platforms (P7919.1) Requirements for eReaders to support learning applications ranging from traditionally organized eBook to a fully adaptive learning and teaching system.	
	IEEE 2834	

6.2 Proposed Relationship of CM4LTS to open, published technical standards outside of LTSC

1. **A4L Unity Specification**
2. **A4L SIF Data Model**

3. **A4L SIF Infrastructure**
4. **A4L SDPC**
5. **AchieveNGSS**
6. **ADL SCORM**
7. **ADL / IEEE xAPI**
8. **Blockcert Blockcert**
9. **CAST UDL**
10. **CCSSO/NGA CCSS**
11. **Credential Engine CTDL**
12. **Dublin Core LRMI**
13. **ECMA JSON**
14. **edX TSR**
15. **Ed-Fi Alliance Ed-Fi**
16. **Ed-Fi Alliance ODS**
17. **Ed-Fi Alliance Core Student**
18. **Ed-Fi Alliance Assessment API**
19. **Ed-Fi Alliance Enrollment API**
20. **HR Open Standards**
21. **IDPF EPUB**
22. **IEEE LTSC ICICLE**
23. **IEEE LTSC CM4LTS**
24. **IEEE LTSC LTSA**
25. **IEEE LTSC RAMLET**
26. **IEEE LTSC CDS**
27. **IEEE LTSC LOM**
28. **IEEE LTSC SCORM API**
29. **IEEE LTSC SCORM Data Model**
30. **IEEE LTSC eBooks/eReaders**
31. **IEEE LTSC CSDG**
32. **IEEE LTSC xAPI**
33. **IEEE LTSC AISS**
34. **IEEE LTSC FML**
35. **IEEE LTSC ARLEM**
36. **IEEE LTSC MLP**
37. **IETF HTTP**
38. **IMS Global OneRoster**
39. **IMS Global EduAPI**
40. **IMS Global CASE**
41. **IMS Global LTI**
42. **IMS Global IMS CC**
43. **IMS Global IMS CP**
44. **IMS Global IMS TCC**
45. **IMS Global QTI**
46. **IMS Global APIP**

47. **IMS Global OBI**
48. **IMS Global Caliper**
49. **ISTE ISTE Standards**
50. **MedBiquitous Educational Achievement**
51. **NIST**
52. **PESC Core Main**
53. **PESC Academic Record**
54. **PESC Admissions Record**
55. **PESC ePortfolio**
56. **PESC Credential**
57. **PESC SPEEDE**
58. **Schema.org EOC**
59. **Schema.org LRMI**
60. **US Ed CEDS**
61. **US Ed CEDS NDS**
62. **US Government FERPA**
63. **US Government Section 508**
64. **W3C DIF**
65. **W3C DID**
66. **W3C EEA**
67. **W3C EOC**
68. **W3C HTML**
69. **W3C TMS**
70. **W3C VC**
71. **W3C WCAG**
72. **W3C XML**

ILR Recommended Practices

Section 1. Identity and Trust

Primary Author(s) - Drummond Reed, other?
Additional Contributors - ?

Scope. Recommended practices for public communities to use enterprise, federated, and decentralized identity and data sharing technology to implement trust over IP, manage self-sovereign identity and access control.

1.1 Key Concepts

1. **Key Concepts**
    a. **Distributed Leader Technology -** An immutable ledger of events in which trust is enforced by a consensus mechanism with no central authority.
    b. **Identity -** The unique fact of being who or what a person or thing is (NIST SP 800-63).
    An attribute or set of attributes that uniquely describe a subject within a given context. (NIST SP 800-63)
    c. **Digital Identity** - a unique fact of being who or what a person is IN the digital world. It may be connected to a real-world Identity (thus being a digital twin) or may not (alias/persona) (NIST SP 800-63). digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts (NIST SP 800-63-3, NIST SP 800-63B)
    d. **Digital Identifier -** Unique information used to identify people, organizations, or things within a context. For example SSN, e-mail, SASID, LASID. A digital identity can have more than one digital identifier. (NIST SP 800-63)
    e. **PII** - Personally Identifiable Information is any item, collection, or grouping of information about an individual that is maintained by an organization, including identifying information, education, financial transactions, medical history, Social Security Numbers, and criminal or employment history. (NIST SP 800-163 under the Personally Identifiable Information document: NIST SP 800-122)
    f. **Personal Information** - PII, demographics, and linked event information. Some information becomes personal in context (such as small group size aggregates).
    g. **Learner Information -** Information about a learner. GDPR definition of "Personal Data: Any information relating to an identified or identifiable natural person.[8]
    h. **Privacy Rights -** Rights of a person to control access to and use of their personal information. More formal definition: “the right of a person to be free from intrusion into or publicity concerning matters of a personal nature” - Merriam-Webster Dictionary
    i. **Authentication -** Actions and mechanisms that can authenticate the identity of a person that includes information about an authentication provider, the login identifier used to authenticate a person's identity, and other information related to authentication of a person’s identity. (NIST SP 800-63) Digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Authentication

[8] GDPR

establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. (NIST SP 800-63B)

j. **Access Control -** The protocols in a system that limit access to data or services to authorized entities. Information about a data system or application that an authenticated person or system may access.

k. **Self-sovereign identity** - An identity system architecture based on the core principle that Identity Owners have the right to permanently control one or more Identifiers together with the usage of the associated Identity Data.

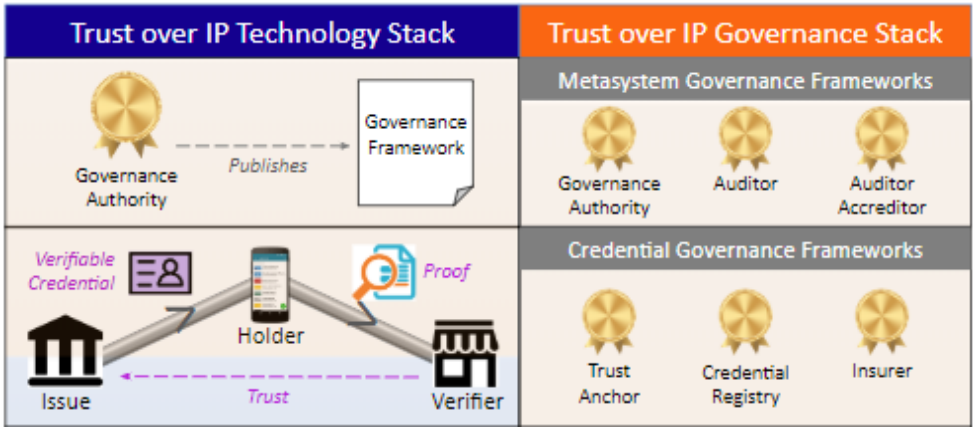
l. **Information Security -** Systems of controls designed to enforce privacy access controls and operational continuity.

m. **Data Controller -** The natural or legal person, public authority, agency, or other body which alone, or jointly with others, determines the purposes and means of the processing of Personal Data.[9]

n. **Data Steward/Processor** - A natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of a Data Controller[10] and has responsibility to have proper security for privacy access controls.

o. **Trust** - A person or systems ability to rely on something from another. Fiduciary trust can be delegated from one entity to another.

p. **Trust Over IP Stack** - the process in which a governance authority publishes a governance framework in both human and machine-readable formats to enable distributed verification of credentials.



q. **Metasystem Governance Framework** - a stated set of purpose, principles, and protocols agreed to by nodes of organizations and individuals to form the Network (IoE MGF).

r. **Smart Contract** -

s. **Digital Wallet** – a software module comprised of an Wallet Storage and one or more Wallet Agent. Digital Wallets allow users to log in to websites and other services with far higher security through Second-Factor Authentication (2FA) and Passwordless Login. The Digital Wallet must be able to organize information to allow its owner to find the information they need.

t. **Wallet Agent** – a piece of software that acts on the behalf of an Identity Owner that sends and receives messages, encrypts and decrypts information, signs digital information, manages information in Digital Wallet, and backs up and allows us to restore

u. **Wallet Storage** - a piece of software , and optionally an associated hardware module, for securely storing and accessing Private Keys, Link Secrets, other sensitive cryptographic key material, and other Private Data used by an Entity.

[9] GDPR

[10] GDPR. Also https://www.dama.org/content/body-knowledge)

v. **Personal Data Store (PDS)** - a service to let an individual store, manage and deploy their key personal data in a highly secure and structured way. It lets you keep your own data and also acquire and reuse proofs of claims or of relationships and qualifications (such as bank account, verified address, driving licence or passport).

w. **Verifiable Credential -** a Credential is a set of one or more claims made by an issuer. A Verifiable Credential is a tamper-evident Credential that has authorship that can be cryptographically verified.

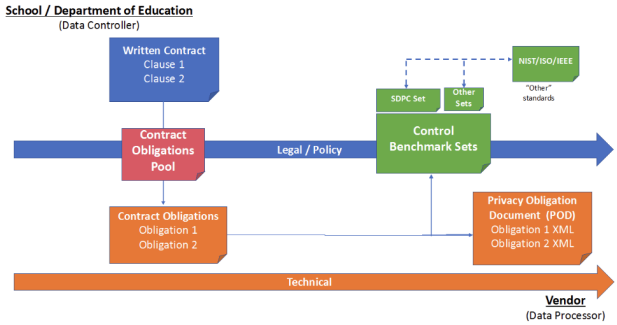
1.2 Pre-Conditions

x. **Privacy Considerations**

i. **The A4L Student Data Privacy Consortium (SDPC)** is designed to address the day-to-day, real-world multi-faceted issues that schools, states, territories and vendors face when protecting learner information. SDPC's vision is to develop common activities, artifacts, templates, tools and effective practices that can be leveraged through a unique collaborative of end users and marketplace providers working together.

1. **Common Contract -** a set of standard language that can be built for an agreement between two parties - MA
   a. Legal Content
   b. Technical Protocol

2. **Global Education Privacy Standard (GEPS)**



3. **SIF Infrastructure Specification 3.3: SIF Data Protection Enforcer Service** - Spec

The components that make up the privacy protections introduced in the SIF Infrastructure are:

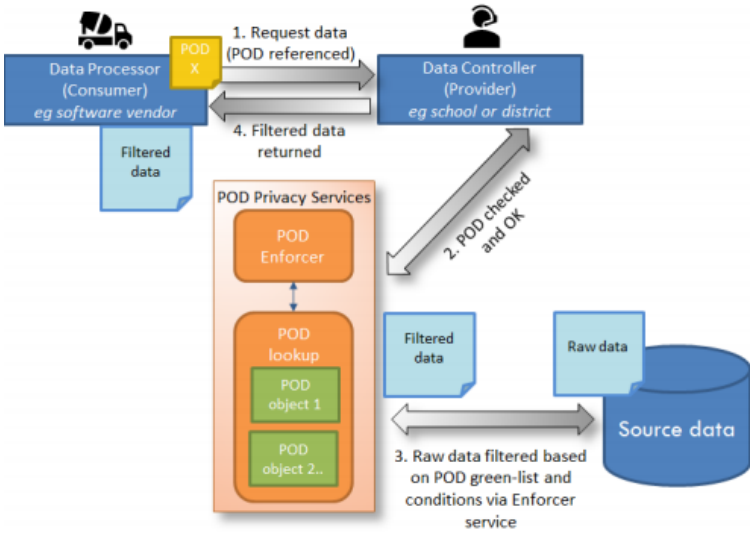
a. **Privacy Obligation Document (POD)** -- An artifact derived from a paper contract which contains details of the parties involved, the data which can be transferred from one party to another, details of the technical benchmarks which must be adhered to (e.g. encryption levels) and details of any additional parties which may handle the data.

b. **POD Lookup Service** – Officially the "Privacy Obligations Registry Utility Service" this provides a means by which external applications request and obtain the current POD that applies to them

c. **POD Enforcer** – Officially the "Data Protection Enforcer Service" this service:

i. Checks that any incoming requests from external applications are referencing their correct POD

ii. Uses the rules from the applicable POD to clean the raw data being returned in a request, ensuring that a 'cleansed' data set is returned to the requesting external application.



y. **Metasystem Governance Framework**

i. A metasystem governance model is a set of protocols to determine who amends the code within an ecosystem:

1. To fix bugs and vulnerabilities
2. To upgrade the underlying technology
3. To repair damages from attacks

ii. **Governance model components:**

1. The rules of the **protocol** (encoded as data) to establish trust and dictate access controls
    a. Interoperability
    b. Security
    c. Privacy
2. The incentives of actors in the network

iii. **Types of blockchain governance**:

1. **Off-chain Governance** — Wider consensus has to be reached in order to implement changes in the protocol, e.g. Ethereum, if consensus is not reached, hard forks occur.
2. **On-chain Governance** — Voting power is determined by the amount of tokens an actor holds.

z. **Credential Governance Framework**

i. **W3C Credential**

ii. **Community standards for wallets - Hyperledger ARIES**

aa. **Directory and Exchange Services**

i. **Example from finance sector - LEI** - Legal Entity Identifiers (GLEIF.org) - ISO Standard

ii. GeoCode - control vocabulary. Unique ID for every education provider in the world. Working with organization in China and EU. All Canada, US High Schools, many higher ed. Based on name of the school, physical address of the place and any national code. (Jim Kelly is running this in PESC). University of Southern CA is commiting Grad Students to do S&M. ECE has done the coding. S&M is being done

iii. **EdExchange** - organizational registry and broker, with service to publish and transport support peer-to-peer to identify uniquely trading partner.
    1. Exchange Server
    2. Directory Server (will use GeoCode)

iv. KnowIdentity - Trust over IP Stack

v. IEEE Magazine - specialized edition on decentralized identity

1.3 Protocols

1. Decentralized Identifiers (DIDs)
2. DID Documents
3. DID Document Syntax
4. DID Methods Adapted for Education/CO
5. DID Resolvers

1.4 References and External Links

1. W3C DIDs Data Model
2. W3C DID Working Group
3. W3C VC Data Model
4. W3C VC Implementation Guide
5. NIST's Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems.
6. Standards for Agency and Decentralized Information Governance
7. Hyperledger Aires - DIDComm Protocol
8. The Sovrin Governance Framework
9. T3 Paper on SSI in Education and Workforce
10. IoEd Metasystem Governance Framework

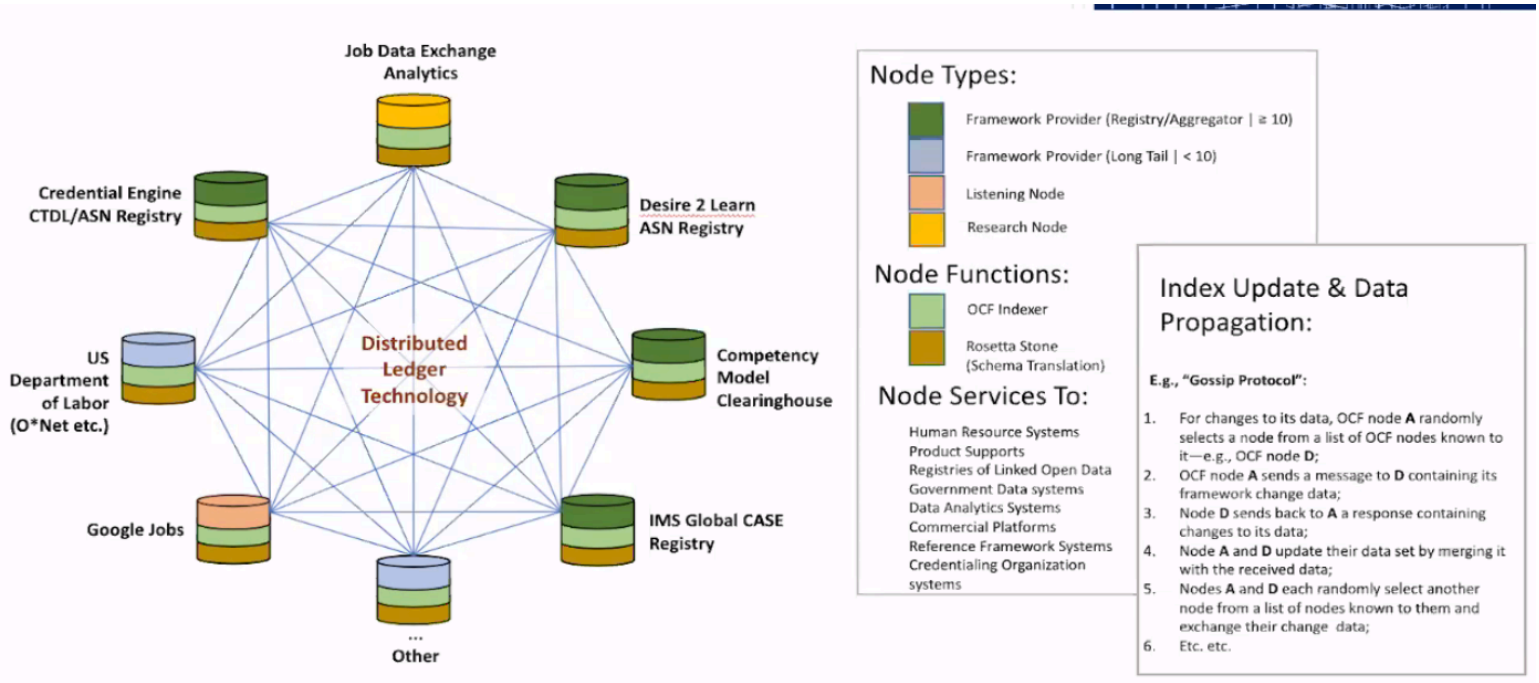
Education 3.0 Base Document

Section 2. Open Ontology References

2.1 Key Concepts

- A taxonomy is a simple hierarchical arrangement of entities where you have a parent-child kind of relationship.
- An ontology describes concepts through complex relations between concepts
- Crosswalks describe relationships between taxonomies to form ontologies
- Machine-readable data can be accessed through an application programming interface (API)
- Open, machine-readable ontologies are services that enable content and achievement assertions to be correlated and crosswalked without restriction

2.2 Meta Registry Services



2.3 Inventory of Machine-Readable Ontologies

Publisher	Description	Contact	Open Ontology Contribution
ACT Holistic Framework	The ACT Holistic Framework is a research backed learning taxonomy across the multiple domains necessary for academic and career success. ACT has also published the National Career Readiness certificate on Credential Engine.	Brandon Dorman brandon.dorman@act.org	Holistic Frameworks are in CASE format and are shared

Competency and Skills System (CASS)	CASS an open source project effort funded by the US DOD ADL that facilitates machine readability and interoperability with other systems by automatically exposing competencies as linked and open data. CASS can be configured as a lightweight open system or as a highly secure system with strong cryptography. Multiple instances of CASS can communicate and work together through a federated architecture. CASS can be deployed as a public or private cloud-based solution. CASS can be deployed as a public or private cloud-based solution. Competencies stored in CASS are automatically exposed as linked and open data to facilitate machine readability. CASS can be configured as a lightweight open system or as a highly secure system with strong cryptography. Blockchain technology can be used to create competency records that are secure, verifiable, and shareable only when authorized.	Robby Robson robby.robson@eduworks.com Fritz Ray fritz.ray@eduworks.com	
CPALMS	CPALMS is an online toolbox of information, vetted resources, and interactive tools that helps educators effectively implement teaching standards. It is the State of Florida's official source for standards information and course descriptions.	Rabieh Razzouk, rrazzouk@lsi.fsu.edu 850-694-1682	CPALMS has committed to publish in CASE format and mirror in CASE Network without usage restrictions.
Credential Engine Registry	The Credential Registry is a cloud-based library that collects, maintains, and connects information on all types of credentials, from diplomas to apprenticeships and from licenses to PhDs. The Registry holds detailed information on all types of credentials in an easily-accessible format. Here you can explore competencies, learning outcomes, up-to-date market values, and career pathways and reference data on modern credential attainment and quality assurance at schools, professional associations, certification organizations, military, and more.	Jeff Grann grann@credentialengine.org Deb Everhart deverhart@credentialengine.org	
D2L ASN	The Achievement Standards Network™ (ASN™) provides access to machine-readable representations of learning objectives and curriculum standards.	Paul Janzen Paul.Janzen@D2L.com	While the content is licensed under CC-BY, D2L terms of use prevent use without approval.
EdGate	EdGate manages a database of U.S. and international standards. Our primary focus is to offer publishers and content providers an accurate, cost-effective way to align books, software, media and other instructional materials directly to educational performance standards and other content. EdGate's team of subject matter relies on the EdGate taxonomy to align content to standards. EdGate also licenses the ExACT alignment tool, empowering publishers with the ability to correlate their own unique content to standards and to generate alignment statistics reports for sales, marketing, RFP, and adoption requirements. Additionally, EdGate creates metadata and keywords; offers complete crosswalking services and gap analysis;	Gina Faulk gfaulk@edgate.com Peter Sibley PSibley@journeysmap.com	EdGate offers a database of over five million U.S. and international standards. Subjects include Math, Science, ELA, Social Studies, SEL, Health, P.E., World Languages, Technology Education, Early Childhood, Library Media, Religion, CTE (and all clusters/pathways contained within CTE). Our proprietary taxonomy contains thousands of concepts that map to relevant educational standards.

	film segmenting and alignment; licenses out premium standards; and licenses access to an OER repository. EdGate is offering the CASE identifiers as a deliverable to our alignment clients. Additionally, EdGate will be integrating with the CASE network via API. We will provide IMS partners with premium standards via the CASE network.		Our OER database contains 140,000 unique standards-aligned items. EdGate offers the CASE identifiers as a deliverable for our alignment clients, upon request.
Emsi Skills DB	Labor market data available to professionals in higher education, economic development, workforce development, talent acquisition, and site selection. Our data, which covers more than 99% of the workforce, is compiled from a wide variety of government sources, job postings, and online profiles and résumés.	Kelly Bailey kelly.bailey@economicmodeling.com Bob Hieronymus bob.hieronymus@economicmodeling.com	
GeorgiaStandards.org	Georgia Department of Education publishes its academic standards and course codes in CASE format.	Keith Osburn kosburn@doe.k12.ga.us	GA standards are mirrored in CASE Network and available for use without restriction.
IMS Global CASE Network	CASE Network enables better support for aligned instruction across the digital learning ecosystem via a free public digital registry that includes standards for all 50 U.S. states and the Common Core. Currently, the registry includes full sets of English Language Arts and Mathematics standards in CASE format that can be downloaded or accessed by an authenticated API by registered users.	Bruce Umpstead bruce@scaleuped.com	IMS publishes 128K+ state academic standards covering K12 math and ELA from all states and a growing number of other subjects. Content can be used without restriction.
ISKME		Lisa Petrides lisa@iskme.org Michelle Brennan michelle@iskme.org Steve Schoettler steve.schoettler@gmail.com	
MatchMaker Education Labs		Michael Jay michael@matchmakeredlabs.net Brandt Redd brandt@redd.org	
OpenTaxonomy.org		Wayne Skipper wayne@concentricsky.com Nate Otto notto@concentricsky.com	

ESCO	ESCO is the multilingual classification of European Skills, Competences, Qualifications and Occupations. ESCO is part of the Europe 2020 strategy. The ESCO classification identifies and categorises skills, competences, qualifications and occupations relevant for the EU labour market and education and training. It systematically shows the relationships between the different concepts. https://ec.europa.eu/esco/portal/home	simone.ravaioli@digitary.net	It's published as Linked Open Data with a set of open API. ESCO - API

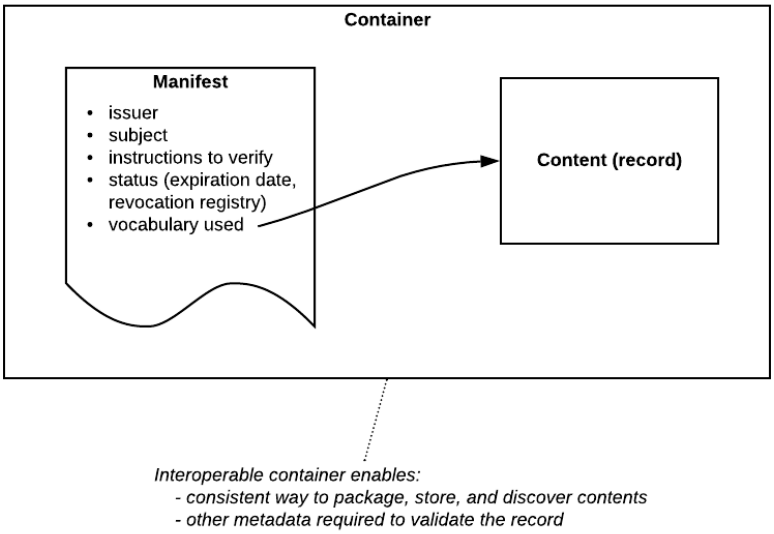
Section 3. Verifiable Assertions

Scope. The ILR ecosystem assumes a distributed network of networks and nodes enabling personalized, competency-based, lifelong, blended learning at the scale of the Internet

3.1 Key Concepts

1. **Pre-Conditions**
    a. Identity and Trust
    b. Open Ontologies

2. **High Level Design.** The consistent packaging with discoverable metadata (like VCs, and like the generic package that Jim describes) is relevant when you consider what happens when either a subject (as shown below) has to deal with a large number of records. The consistent packaging lets the wallet store and inspect/organize all of these credentials, despite the fact that the content may be very different.



3. **Core Data Model**

    a. **Credential.** A Credential presents an achievement, personal attribute, or experience, typically for the purpose of presenting eligibility or qualification to do something or fill a particular role. Credentials exist in the physical world in many forms, and they can be represented digitally. A Credential makes claims about a subject, potentially including claims that recognize that subject for achievements.
    b. **Assertions.** An assertion is a credential that makes a claim that a learner holds a defined achievement, that they have met the criteria of that achievement and have been granted it. Examples of this concept include Open Badges Assertion / CLR Achievement Record.
    c. **Defined Achievement.** A defined achievement is a classification of recognition within a community that is named and described in terms of criteria and other metadata, sometimes including a graphic image as

symbolic representation. Examples of this concept include Open Badges BadgeClass / CLR Achievement, CTDL-ASN Competency.

d. **Presentations - (W3C VC).** Assertions may be assembled into presentations, which are documents that contain multiple claims about a particular Credential Subject. Presentations themselves may be signed to enable assurance that the particular assemblage of assertions has not been modified from the content selected for inclusion by the presentation's issuer.

e. Concrete Lifecycle Example:

- Jen registers for and takes an online MOOC from a provider and obtains completion credential. She attends formal courses at a university where she obtains credentials that describe her course completions. She also obtains competency recognition credentials. She can combine all these credentials in a credentials storage service that represents her. She can hold them on her own device in a wallet.
- The course completion credentials are issued by the definer of the achievement. The competency recognition credentials are issued by the institution represented by the instructor that assessed them, but the competencies that are recognized may have been defined by the state or a coalition of educators and employers. These two types of verifiable assertions are both important parts of Jen's recognized learning, and it's important to be able to distinguish the two, because for the course completion credentials, only the definer of the achievement should be trusted to issue assertions (and their value would be dependent on the inspector's trust in that definer), where for the competencies, an inspector may trust a variety of issuers to recognize learners with assertions, based on whomever the inspector knows to be an authority on the competency at hand.

4. Additional Concepts (W3C VC)

a. **Contexts.** Contexts enable implementers to provide both convenient and memorable names for terms without losing the specificity that comes from using precise IRIs to define them. Contexts tie each term within their scope to a IRI where documentation may be available.

b. **Identifiers.** Entities that exist in the physical world are known to the humans and machines around them by various identifiers. These include names, email addresses, phone numbers, object identifiers, ISBNs, and more recently Decentralized Identifiers (DIDs). When it is necessary to describe an entity in the credentialing landscape, using primary and additional typed identifiers is helpful. When holding an identifier for an entity, it is useful to be able to "resolve" that identifier to look up more information about the entity. Various types of identifiers offer different affordances for lookup, authentication.

c. **Credential Subject.** The recipient of an assertion is the subject of a claim it makes that they hold a particular defined achievement.

d. **Issuer.** The issuer of an Assertion is the authority who claims that the Credential Subject has met the criteria. By issuing an assertion the Issuer grants the Credential Subject the award.

e. **Issuance Dates.** Assertions are each awarded at a particular time, which is recorded in the credential.

f. **Proofs (Signatures).** Proofs allow for the verification that a credential is issued on the authority of its listed issuer and has not been falsified or adulterated. These are typically cryptographic signatures produced by a private key known to be held by the issuer. Various proof formats exist, including signature suites that afford varying capabilities for what type of cryptographic keys may be used or how those keys may be rotated, for instance.

g. **Expiration.** Assertions may have limited duration of validity, according to their issuer. An expiration timestamp may be recorded.

h. **Status.** Assertions may be revoked, so it is often relevant to verify the status of a particular assertion.

i. **Presentations.** An assembly of multiple Credentials (Assertions)

3.2 Advanced Concepts

1. Advanced Concepts (W3C VC)
    a. Lifecycle Details
    b. Trust Model
    c. Extensibility
    d. Data Schemas
    e. Refreshing
    f. Terms of Use
    g. Evidence
    h. Zero-Knowledge Proofs
    i. Disputes
    j. Authorization

2. Syntaxes (W3C VC)
    a. JSON
    b. JSON-LD
    c. Proof Formats

3. Privacy Considerations (W3C VC)
    a. Spectrum of Privacy
    b. Personally Identifiable Information
    c. Identifier-Based Correlation
    d. Signature-Based Correlation
    e. Long-Lived Identifier-Based Correlation
    f. Device Fingerprinting
    g. Favor Abstract Claims
    h. The Principle of Data Minimization
    i. Bearer Credentials
    j. Validity Checks
    k. Storage Providers and Data Mining
    l. Aggregation of Credentials
    m. Usage Patterns
    n. Sharing Information with the Wrong Party
    o. Frequency of Claim Issuance
    p. Prefer Single-Use Credentials
    q. Private Browsing

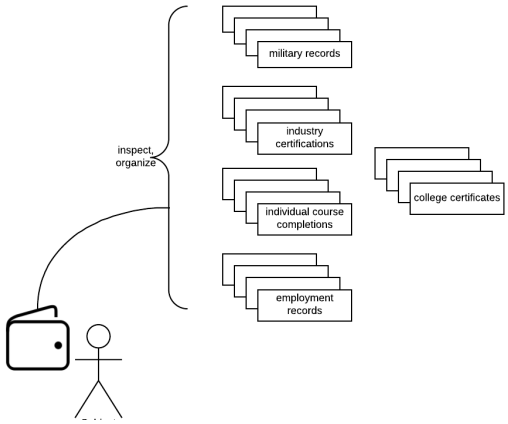
4. Security Considerations (W3C VC)
    a. Cryptography Suites and Libraries
    b. Content Integrity Protection
    c. Unsigned Claims
    d. Token Binding
    e. Bundling Dependent Claims
    f. Highly Dynamic Information
    g. Device Theft and Impersonation

5. Accessibility Considerations (W3C VC)

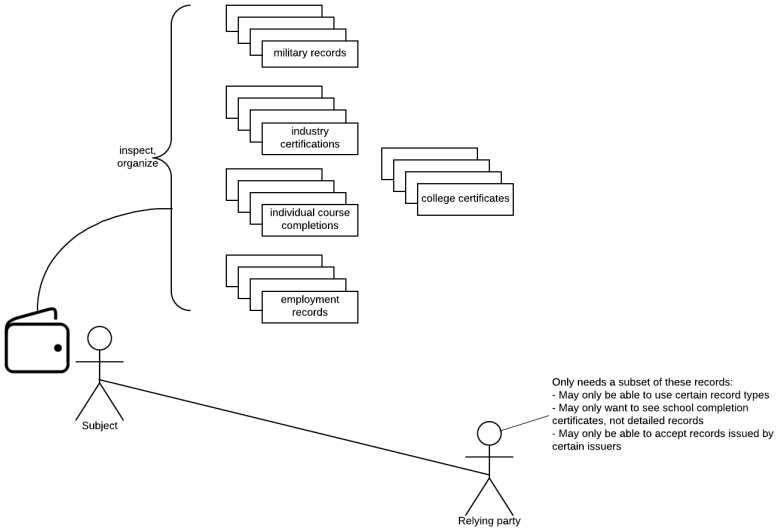
6. Internationalization Considerations (W3C VC)

3.3 Use Cases and Requirements

1. **As a learner/subject, I want to inspect, organize, and control access to my academic, military, industry, employment.**



2. **As a provider, I want to consume data on behalf of assertion issuers and package publishers, transform into CLR data, and provide to other authorized consumers.**



Education 3.0 Base Document

Archive of Materials Not Yet Incorporated

1. Links
    a. Principles
        i. Linked data, not replicated data
    b. Contract for Web
    c. Self-Sovereign Identity and Access Control
    d. Trust Over IP Stack
    e. Ontologies
    f. Assertions
    g. ADL Alignment to IEEE CM4LTS
        i. **Identity** - Federated Identity, Credential, and Access Management (FICAM)
            1. Recommended practices to implement NIST 800
                a. Back End - Centralized Authority
                b. Last Mile - Shelly - 9274.4.x?
                c. Integration the Two
        ii. Ontologies
            1. Ontologies
                a. Army Cool
                b. Navy Cool
        iii. Assertions
            1. Milgears - Assertions and Mappings
            2. Airman Learner Record
            3. Enterprise Learner Record
        iv. Activities
            1. xAPI
                a. Noisy LRS
                b. Normalize
            2. Caliper
        v. Resources
            1. LTI
            2. SCORM

1. Self-Sovereign Identity and Access Control Trust Networks
    a. Self-Sovereign Identity
    b. Access Control
    c. Trust Networks
        i. Best governance is most decentralized - weak center
        ii. Meta system governance framework for education and learning
        iii. Soverin Foundation
        iv. Actor/Network

v. Cloud capacity, distributed agents
vi. Connection between parties
vii. Set of actors inteacting in network under a governance framework
viii. Human
ix. SSI of
x. Governance Authorities
xi. Examples
    1. ICAN
    2. Federal Reserve

2. Open Ontology References

3. Verifiable Assertions

Trusted Learner Network[11]

Stores Learner Achievements. *A place to store assertions made about a learner's achievements by educational institutions, employers or other organizations who are partners in the TLN and use the TLR data model.*
Safe + Secure Info. *The data in TLR are immutable. Once an accomplishment is asserted by a TLN member entity, it cannot be manipulated or changed.*
Always Up-to-Date. *An issuer's assertion about an accomplishment can be supplanted by either an expiration or revocation if the record type supports such an update.*
Issued and Maintained by the Entity. *A learner accomplishment is owned by the entity making this assertion. Ownership means the ability to view, share, or update said record.*
Present Current Info First. *The business logic of the TLN always presents the most current view of a learner's record. The history ledger transactions are retained and can be viewed by the owner of those records.*
Records Learner Consent. *Sharing a learner record of accomplishment is dependent upon earner consent, which is recorded in the database. Learner consent can be revoked by the learner at any time.*
Shared Only Within the TLN. *Learner records can only be shared with other members of the TLN. Sharing to off-chain and to non-TLN entities will be implemented at a later date as the required technology emerges.*
Co-Owned by the Learner. *Learner accomplishments are co-owned by the learner. Coownership allows the learner to selectively share the metadata describing their achievements with others.*
Open-Source Tools + APIs. *The technology to participate in the TLN is not dependent on proprietary or commercial vendor products.*
IAM Tools Included. *Identity and Access Management is central to the confidence in and adoption of the TLN as a mechanism for the value of achievements associated with learning.*
Non-Commercial Use. *All TLR sharing will require explicit permission by the individual and/or organization as part of the logic of the database and supporting applications.*
Network of Networks. *The TLN is not designed to be a hierarchical network with a single anchor entity. The network effect of the distributed database should naturally evolve into multiple networks to support crosssections of different members.*

Guiding Principles of SSI[12]

Existence. *Users must have an independent existence. Any self-sovereign identity is ultimately based on the ineffable "I" that's at the heart of identity. It can never exist wholly in digital form. This must be the kernel of self that is upheld and supported. A self-sovereign identity simply makes public and accessible some limited aspects of the "I" that already exists.*
Control. *Users must control their identities. Subject to well-understood and secure algorithms that ensure the continued validity of an identity and its claims, the user is the ultimate authority on their identity. They should always be able to refer*

[11] Adapted from ASU Trusted Learner Network
[12] Adapted from Christopher Allen's Ten Principles of SSI

to it, update it, or even hide it. They must be able to choose celebrity or privacy as they prefer. This doesn't mean that a user controls all of the claims on their identity: other users may make claims about a user, but they should not be central to the identity itself.

Access. *Users must have access to their own data. A user must always be able to easily retrieve all the claims and other data within his identity. There must be no hidden data and no gatekeepers. This does not mean that a user can necessarily modify all the claims associated with his identity, but it does mean they should be aware of them. It also does not mean that users have equal access to others' data, only to their own.*

Transparency. *Systems and algorithms must be transparent. The systems used to administer and operate a network of identities must be open, both in how they function and in how they are managed and updated. The algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture; anyone should be able to examine how they work.*

Persistence. *Identities must be long-lived. Preferably, identities should last forever, or at least for as long as the user wishes. Though private keys might need to be rotated and data might need to be changed, the identity remains. In the fast-moving world of the Internet, this goal may not be entirely reasonable, so at the least identities should last until they've been outdated by newer identity systems. This must not contradict a "right to be forgotten"; a user should be able to dispose of an identity if he wishes and claims should be modified or removed as appropriate over time. To do this requires a firm separation between an identity and its claims: they can't be tied forever.*

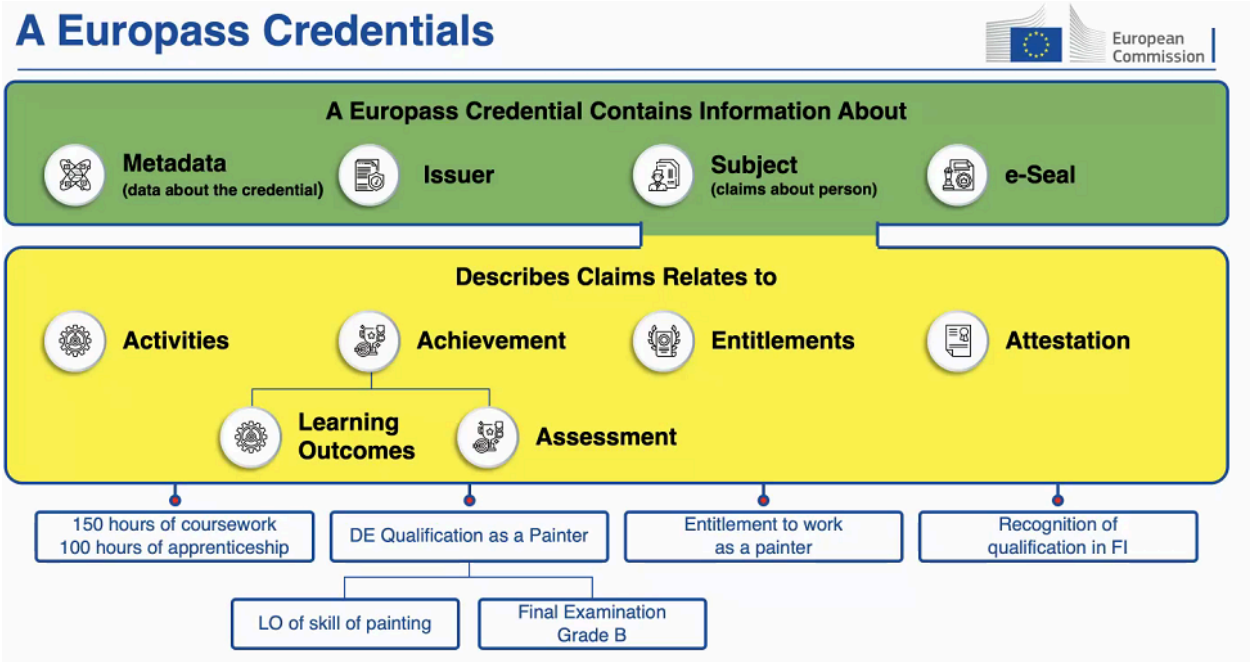
Portability. *Information and services about identity must be transportable. Identities must not be held by a singular third-party entity, even if it's a trusted entity that is expected to work in the best interest of the user. The problem is that entities can disappear — and on the Internet, most eventually do. Regimes may change, users may move to different jurisdictions. Transportable identities ensure that the user remains in control of his identity no matter what, and can also improve an identity's persistence over time.*

Interoperability. *Identities should be as widely usable as possible. Identities are of little value if they only work in limited niches. The goal of a 21st-century digital identity system is to make identity information widely available, crossing international boundaries to create global identities, without losing user control. Thanks to persistence and autonomy these widely available identities can then become continually available.*

Consent. *Users must agree to the use of their identity. Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs. However, sharing of data must only occur with the consent of the user. Though other users such as an employer, a credit bureau, or a friend might present claims, the user must still offer consent for them to become valid. Note that this consent might not be interactive, but it must still be deliberate and well-understood.*

Minimalization. *Disclosure of claims must be minimized. When data is disclosed, that disclosure should involve the minimum amount of data necessary to accomplish the task at hand. For example, if only a minimum age is called for, then the exact age should not be disclosed, and if only an age is requested, then the more precise date of birth should not be disclosed. This principle can be supported with selective disclosure, range proofs, and other zero-knowledge techniques, but non-correlatibility is still a very hard (perhaps impossible) task; the best we can do is to use minimalization to support privacy as best as possible.*

Protection. *The rights of users must be protected. When there is a conflict between the needs of the identity network and the rights of individual users, then the network should err on the side of preserving the freedoms and rights of the individuals over the needs of the network. To ensure this, identity authentication must occur through independent algorithms that are censorship-resistant and force-resilient and that are run in a decentralized manner.*


A Europass Credentials
European Commission
A Europass Credential Contains Information About
Metadata
(data about the credential)
Issuer
Subject
(claims about person)
e-Seal
Describes Claims Relates to
Activities
Achievement
Entitlements
Attestation
Learning Outcomes
Assessment
150 hours of coursework
100 hours of apprenticeship
DE Qualification as a Painter
Entitlement to work as a painter
Recognition of qualification in FI
LO of skill of painting
Final Examination Grade B