T3 INNOVATION NETWORK

PUBLIC SPECIFICATION FOR

LEARNING AND EMPLOYMENT RECORD (LER) WRAPPER AND WALLET

A Universal Cross-Standard Digital Container for Self-Sovereign Management of Learning and Employment Records with Cross-Standard LER Wrappers

JULY 2020

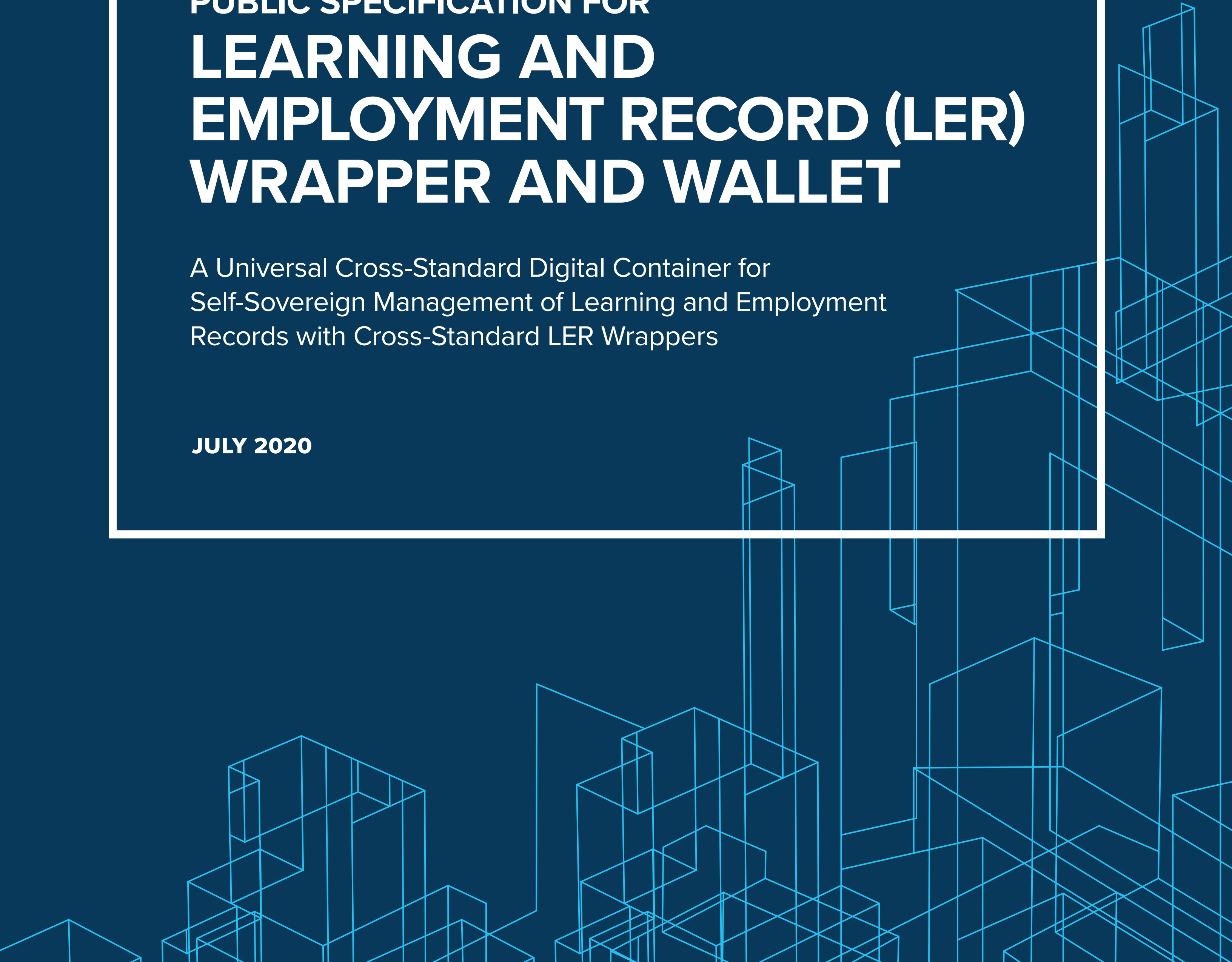


TABLE OF CONTENTS

INTRODUCTION

This draft specification was developed in the public domain and will be offered for recognition as a standard by relevant standards organizations concerned with Learning and Employment Records (LERs). An LER is a digital record of learning and work that can be linked to an individual and combined with other digital records for use in pursuing educational and employment opportunities. An LER can document learning wherever it occurs, including at the workplace or through an education experience, credentialing, or military training. It can also include information about employment history and earnings. LERs are similar to electronic health records (EHRs) and have the potential to improve education and hiring outcomes in the same way that EHRs have improved healthcare delivery. What makes LERs unique is their ability to be fully transferable and recognized across student information, learning management, employer HR, and military systems. LERs go by many names and are also referred to as an interoperable learning record (ILR). This draft specification was developed within the T3 Innovation Network (T3 Network) with assistance from project teams to leverage existing LER standards, not replace them. It will be offered for adoption by various standards organizations. This work has been done in cooperation with a large group of standards and stakeholders including Access 4 Learning (A4L), Common Education Data Standards (CEDS), IMS Global Learning Consortium, Postsecondary Electronics Standards Council (PESC), HR Open Standards Consortium, and World Wide Web Consortium (W3C), among others[1]. In addition, the Institute of Electrical and Electronics Engineers (IEEE)[2] approved a workgroup for a new guide to interoperable learner records that will be informed by this document. This draft specification will be reviewed and pilot-tested by LER pilot teams to improve and update the specification over time.

This document specifies a universal cross-standards container for LERs to provide guidance to implement an LER using a W3C Verifiable Credential structure created in an open architecture for any given domain to use and extend depending on their use case. The specification is intended to provide a future-proof and flexible approach to a collection of LERs, allowing for any kind of learner record from early learning through employment learning experiences. This also includes records related to a learner's competencies. The specification recognizes that different standards organizations may specify the standards needed to support many types of records, and across geographical boundaries. In some cases, the standard or set of standards from one organization will be sufficient to meet the needs of a particular use case.

However, the authors anticipate the need for a universal cross-standards learning and employment wallet able to support specialized standards. We define a "wallet" as an application, device, or cloud base that can securely store and manage all of an individual's records from all issuers of such variable credentials, achievements, and assertions of learning and employment. A wallet enables an individual to manage, curate, grant access to, and re-distribute their full set of records. A few examples of the range of standards and uses that a universal cross-standards LER Wallet may need to support are listed below.

- Medbiquitous specializes in learner record standards for medical education
- PESC focuses on postsecondary record standards
- HR Open specializes in standards for workforce
- W3C Verifiable Credential specifies credential assertions
- IMS Global's Comprehensive Learner Record and IMS Open Badges support various types of achievement records
- A4L SIF specification includes U.S. special education (Individual Education Plans, or IEPs) and other K12 data types
- CEDS includes data definitions for early learning childhood development through workforce
- Schema.org and Credential Engine provide credential and object description languages that span these vertical and horizontal segments
- Europass specifies interoperable documents to make skills and qualifications clearly and easily understood in Europe
- China is implementing a dual credentialing system of qualification certificate and degree certificate

[1] Annex A: Participants and Contributors
[2] https://standards.ieee.org/

- Individual self-assertions with evidence (e.g., ran a marathon in a given time)
- xAPI achievement profiles

The specification also recognizes starkly different kinds of data are needed for different uses of LERs (e.g., some LERs verify achievements to employers or potential employers, other LERs directly support learning processes for formative feedback and tutoring). As a result, any scalable solution must include the possibility of using different types of payloads. A solution with multiple payload types also supports legacy and embedded practice at the vendor, local, state, and federal level.

Design Principles

This specification is being developed with input from multiple standards organizations and working groups listed in the Annex A - Participants and Contributors. All participants and contributors agreed to the design principles listed below. It is important to note that this approach also supports the U.S. Government's Office of Management and Budget (OMB) Circular A-119 which establishes policies on federal use and development of voluntary consensus standards and on conformity assessment activities.

General

- Keep it simple.
- Support all standards in payload.
- Use existing standards.
- Start with the JSON-LD wrapper design to be as simple and as close to the W3C Verifiable Credential design pattern as is possible and practical.

LER Wallet

- Limit to functional specifications (the "what").
- Do not prescribe specific technologies, architectures, or protocols (the "how").

LER Wrapper

- Informed by W3C Verifiable Credential.
- Support all standards payloads.

Design Goal Table

Goal	Description
Control	Give entities, both human and non-human, the power to directly control their LERs.
Privacy	Enable entities to control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data.
Security	Enable sufficient security for relying parties to depend on the LER’s verification and security model for their required level of assurance.
Proof-based	Enable LER subjects (individuals) to provide cryptographic proof when interacting with other entities.

Discoverability	Make it possible for entities to discover LERs for other entities to learn more about or interact with those entities.
Interoperability	Use interoperable standards so LER infrastructure can make use of existing tools and software libraries designed for interoperability.
Portability	Be system and network-independent and enable entities to use their LER metadata with any system that supports LERs and wallets.
Simplicity	Favor a reduced set of simple features to make the technology easier to understand, implement, and deploy.
Extensibility	Where possible, enable extensibility provided it does not greatly hinder interoperability, portability, or simplicity.

Design Principles and Connections to Initiatives:

Informed by W3C Verifiable Credentials Data Model 1.0

The specification is informed by the work of the W3C Verifiable Credentials Community Group and some key metadata concepts used in the W3C Verifiable Credentials Data Model 1.0[3]. However, the intent of this specification is a solution applicable to other kinds of LERs beyond credentials. Therefore, this specification delegates the LER payload to applicable standards and may add some elements not included in the W3C Verifiable Credential specification. The intent of this specification is to expand the verifiable credential (VC) specification in appropriate ways and to make no breaking changes, if possible. Any changes made to this foundational template will be documented so it can be understood by developers and implementers.

Applicable W3C Verifiable Credential Metadata Concepts

- Identifiers
- Issuer
- Credential Subject
- Issuance Date
- Expiration
- Status
- Types
- Contexts

T3 Innovation Network

This document was drafted in coordination with the cross-standards mapping project of the T3 Innovation Network. The T3 Network is a U.S. Chamber of Commerce Foundation led initiative exploring the emerging technologies and standards in the talent marketplace to create more equitable and effective learning and career pathways. It is informed particularly by the T3 Network’s phase two projects including: Map and Harmonize Data Standards, Comprehensive Learner/Worker/Military Records Standards, Management and Use of Individual-Level Data Records, and “Applying Self-Sovereign Identity Principles to Interoperable Learning Records: Principles, Challenges, and Community Guidance.” [4]

[3] https://www.w3.org/TR/vc-data-model/

[4] https://www.uschamberfoundation.org/sites/default/files/mediauploads/Applying%20SSI%20Principles%20to%20ILRs%20Report.pdf

LER Wrapper

This proposed specification leverages a thin wrapper with a minimal set of metadata to support different types of LER payloads defined by existing and future data standards.

Self-Sovereign LER Wallet

This proposed specification supports a learner wallet by which a person may be able to manage their own LERs as a set, regardless of source, purpose, and standard encoding format. This self-sovereign wallet supports portability, privacy rights, and agency of a person to curate some aspects of digital identity as it relates to his or her LERs.

This approach is based on the work of the T3 Innovation Network project—Management & Use of Individual-Level Data Records—which developed the paper, "Applying Self-Sovereign Identity Principles to Interoperable Learning Records: Principles, Challenges, and Community Guidance."[5] The paper outlined the following objectives:

- Provide an introduction to Self-Sovereign Identity (SSI)-based approaches and technology.
- Describe how self-sovereign technical standards could be applied to help achieve individually-controlled, portable, interoperable learner, worker, and military records.
- Describe how implementers (such as LER pilots supported by the T3 Network) can begin adopting technical standards to promote self-sovereign management of individual-level records, as well as opportunities to contribute to forward-looking SSI technologies through research and development projects.
- Describe how ecosystems such as the T3 Network can promote sustainable growth of networks committed to ethical, equitable outcomes for learners and workers.

NORMATIVE REFERENCES

The following standards, proposed standards, and specifications are essential for the implementation of this specification regardless of the LER payload:

- IANA Media Type [https://www.iana.org/assignments/media-types/media-types.xhtml]
- IRI - IETF RFC 3986 [https://www.ietf.org/rfc/rfc3986.txt]
- JSON [https://tools.ietf.org/html/rfc8259]
- JSON-LD [https://www.w3.org/2018/jsonld-cg-reports/json-ld/]
- JSON Web Tokens (JWTs) - IETF RFC 7519 [https://tools.ietf.org/html/rfc7519]
- JSON Web Signatures (JWSs) - IETF RFC 7515 [https://tools.ietf.org/html/rfc7515]
- Linked Data Signatures [https://web-payments.org/vocabs/security#LinkedDataSignature2015]
- Multibase [https://github.com/multiformats/multibase]
- W3C Verifiable Credentials [https://www.w3.org/TR/vc-data-model/]
- DCMI [http://purl.org/dc/terms/]
- Schema.org [http://schema.org/]
- W3C Security [https://w3id.org/security#],
- Decentralized Identifiers (DIDs) [https://w3c.github.io/did-core/]
- XML [http://www.w3.org/2001/XMLSchema#]

[5] https://www.uschamberfoundation.org/sites/default/files/mediauploads/Applying%20SSI%20Principles%20to%20ILRs%20Report.pdf

Payload-Specific Normative References

The following standards are essential for the implementation of this specification when used with specific LER payloads:

- A4L Unity IEP Object http://specification.sifassociation.org/Implementation/NA/4.0/XPressWorkingGroup.html#obj:XIndividualizedEducationPlan
- A4L Student Record Exchange (xSRE) http://specification.sifassociation.org/Implementation/NA/3.5/Collections/xSREs.xhtml
- A4L Unity Student Personal http://specification.sifassociation.org/Implementation/NA/4.0/StudentInformationSystemsWorkingGroup.html#obj:StudentPersonal
- A4L Unity Student http://specification.sifassociation.org/Implementation/NA/4.0/XPressWorkingGroup.html#obj:XStudent
- Credential Engine CTDL https://credreg.net/ctdl/terms
- Credential Engine CTDL-ASN https://credreg.net/ctdlasn/terms
- Europass Digital Credential Infrastructure (EDCI) EDCI Data Model on GitHub
- HR Open Assessments http://hropen.jschema.com/specifications then "Assessments"
- HR Open Candidate http://hropen.jschema.com/specifications then "Recruiting"
- HR Open Position Opening http://hropen.jschema.com/specifications then "Recruiting"
- HR Open Screening http://hropen.jschema.com/specifications then "Screening"
- HR Open Resume or CV Standard (Development is in progress.)
- HR Open Employment History (in Candidate) http://hropen.jschema.com/specifications then "Recruiting"
- IMS CLR 1.0 https://www.imsglobal.org/activity/comprehensive-ler
- IMS Open Badges V2 https://www.imsglobal.org/activity/digital-badges
- IMS CASE https://www.imsglobal.org/activity/case
- MedBiquitous Educational Achievement https://www.medbiq.org/educational_achievement
- PESC Approved Admissions Application Standard https://www.pesc.org/admissions-application
- PESC Approved College Transcript Standard https://www.pesc.org/college-transcript
- PESC Approved Course Inventory Standard https://www.pesc.org/course-inventory
- PESC Approved Credential and Experiential Learning Standard https://www.pesc.org/credential-and-experiential-learning
- PESC Approved ePortfolio Standard https://www.pesc.org/eportfolio
- PESC Approved High School Transcript Standard https://www.pesc.org/high-school-transcript
- PESC Approved Test Score Reporting Standard https://www.pesc.org/test-score
- U.S. Military Joint Services Transcript https://jst.doded.mil/jst

SPECIFICATION

This specification includes:

1. Data definitions
2. Data serialization
3. LER Wallet functional requirements

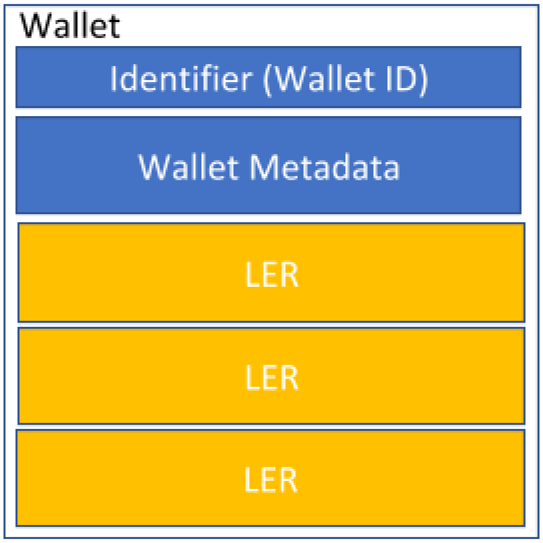
The specification includes three sections:

1. **LER Wallet** - a container capable of holding multiple learner and employment records, each encoded in one of various standards-defined record formats.
2. **LER Wrapper** - a serialization structure that includes metadata and a payload of a single learner and/or employment record encoded in a one or more standard formats.

3. **Verifiable Presentation** - a serialization structure that supports sending an LER from a holder to a third-party receiver.

1. LER Wallet

The LER Wallet is a container capable of holding multiple learning and employment records, each encoded in standards-defined record formats implemented as software with a set of minimum and optional functions.



1.1. Data Privacy and Security

Wallets must ensure both the privacy and security of the LERs under its management.

This means:

1. Encryption in transit
2. Encryption at rest
3. Protection of:
   a) Learning and employment records themselves
   b) Information derived from those records
   c) Use, distribution, and interaction meta-data about those records

Issuers may enhance the security and privacy of LERs by encrypting the record payload. This ensures that any collections of records that might become compromised are of limited use unless the attacker also manages to compromise the private keys of all identifiers used for all of those records. When LERs are encrypted in transit and in rest there are multiple layers of encryption protecting the data, using keys from multiple parties, stored in different systems.

It is anticipated that many wallets will provide enhanced search, analysis, and compositional capabilities based on the contents of recognized LERs. That is, some wallets will be able to ingest well-known payload formats and provide enhanced capabilities by indexing and presenting views of this collected information. The information so derived must be protected just as the original LERs.

It is critical to have data and policy governance to protect the privacy and security of learners. IEEE P7004[6] is working on a standardized approach to that subject. Whether explicitly or implicitly, wallet providers have a fiduciary responsibility to place the interest of its learners and workers before its own, with regard to the use and management of LERs.

The point of this design is to enable individuals to take control over the management and sharing of LERs while retaining appropriate guarantees of authenticity and authority for those issuing entities. The result is greater privacy through better control of the transfer of potentially damaging information and better security through the separation of concerns between issuers, wallets, recipients, and individuals.

1.2. Data Serialization

Data sent to and from the LER Wallet uses the LER Wrapper format specified in section two of this document. This specification does not constrain the method of local storage used by implementations of an LER Wallet.

Note: Each LER payload may be encrypted. The wallet data store should also be encrypted. Learning and employment records within the wallet may be shared or the entire wallet may be shared.

1.3. Individual Identifiers

There is a need in the entire education, training, and workforce ecosystem to identify learners and workers. Traditionally this has been done by using identifiers assigned by an authority in a particular context such as:

- A Social Security Number (assigned by the Federal Government)
- Military identifiers (e.g., CAC ID)
- State person IDs (e.g., Driver’s License)
- State assigned student IDs (e.g., SASIDs or SSIDs assigned by a state education agency)
- Local-assigned student IDs (e.g., LASIDs assigned by a district or college)
- Vendor-assigned identifiers (e.g., SIS or ERP assigned number)
- Employer-assigned IDs (e.g., ID assigned by the person’s employer)

The LER wallet and LER wrapper will not have an explicit call out to this kind of identifier for the learner and worker for the following reasons.

- There are no universally accepted standards for doing this either in the workforce (which still predominantly relies on Social Security numbers and tax IDs, even though that is discouraged) or in any of the education horizontals.
- There are privacy and security risks with using identifiers like Social Security numbers.
- There are use cases in which the physical identity of a person who is the subject of an LER must not be tied directly to the record.

Instead we will rely on a proof-of-control identifier that allows a specific individual to positively assert that the record is authentic and issued to that person. This proactive form of authentication follows modern design principles of privacy and security to disambiguate the identity of the learner and worker using the metadata outside of the payload, which can be verified without potentially leaking personal information within an LER.

This does have implications for the wallet, which will need to develop methods for identifying the individual’s information either from the payload itself or some other means. This design is intentionally constructed to allow static single-point authority-based identifiers (e.g., a school ID) to be deployed and true decentralized encrypted identifiers with proof of control built in. This can also cleanly be laid on top of, and integrated with, a block chain-oriented SSI framework. These are all legitimate mechanisms for identifying an individual and an issuer but have differing consequences and risks associated with them.

[6] https://site.ieee.org/sagroups-7004/

It is outside the scope of this specification to evaluate or judge any of these approaches. However, this specification allows LERs to be deployed based on what is appropriate for the ecosystem the record(s) exist in, the trading network in which they are being moved, and the use case being solved for.

1.4. LER Wallet Functional Requirements

The LER Wallet requirements include:

1. **Receive** LERs
   a) The wallet **must** be able to receive learning and employment records.
   b) The wallet **must** be able to persist those records and store the appropriate metadata (see Persist LERs).
   c) The wallet **may** be able to unpack the payload, but it is not required to do so.
   d) The holder **may** choose to receive one or more records, with identifier authentication[7].
   e) The wallet **may** be able to request, listen for, or subscribe to LERs.

2. **Persist** LERs (see footnote 6)
   a) LERs **must** be able to be held with native format encoding from multiple standards.
   b) Those stored LERs **must** be persisted with sufficient metadata to allow the wallet to execute the minimal functions described in these requirements.
   c) The LERs **may** be stored in both the native format and/or a processed format preferred by the wallet so long as the wallet can fully produce the original record intact (see Send LERs).

3. **Select** LERs by querying the wallet data store (filter persisted LERs)
   a) The wallet **must** be able to discover LERs at least by the name property and description property in the LER.
   b) The wallet **may** discover content by other parameters.
   c) The wallet also **may** expose an external API.

4. **Send** LERs
   a) The wallet **must** have a mechanism for receiving and processing requests for LERs and responding to them.
   b) The wallet **must** have a way of allowing the wallet owner to trigger the wallet sending an LER or LER set.
   c) The holder **may** choose to send one record or many, in whatever format, with identifier authentication (see footnote 6).

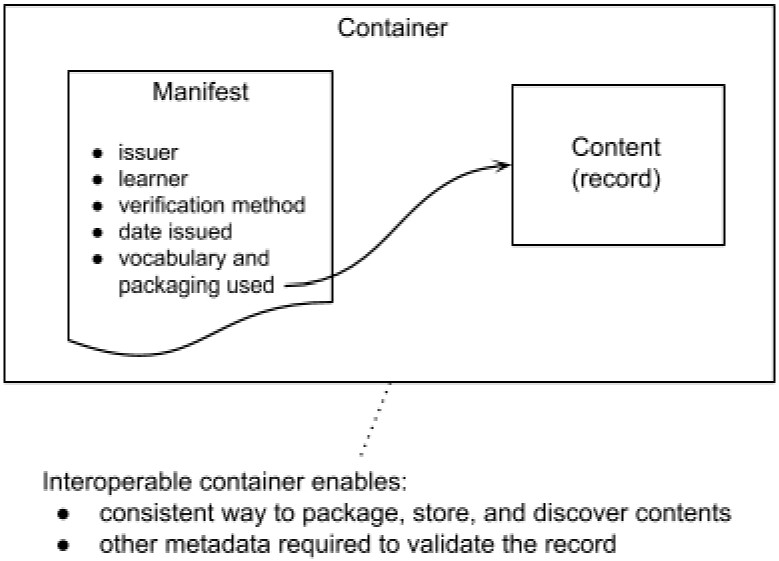
The LER Wallet may be able to:

5. **Log** activity (e.g., LERs sent and received for privacy auditing)
6. **Issue** Pair-wise Unique Decentralized Identifiers (DIDs) for the subject/individual when sending LERs
7. **Manage a set of identifiers** that the holder of the wallet has control over (in a typical use case those identifiers are assumed to represent the individual)

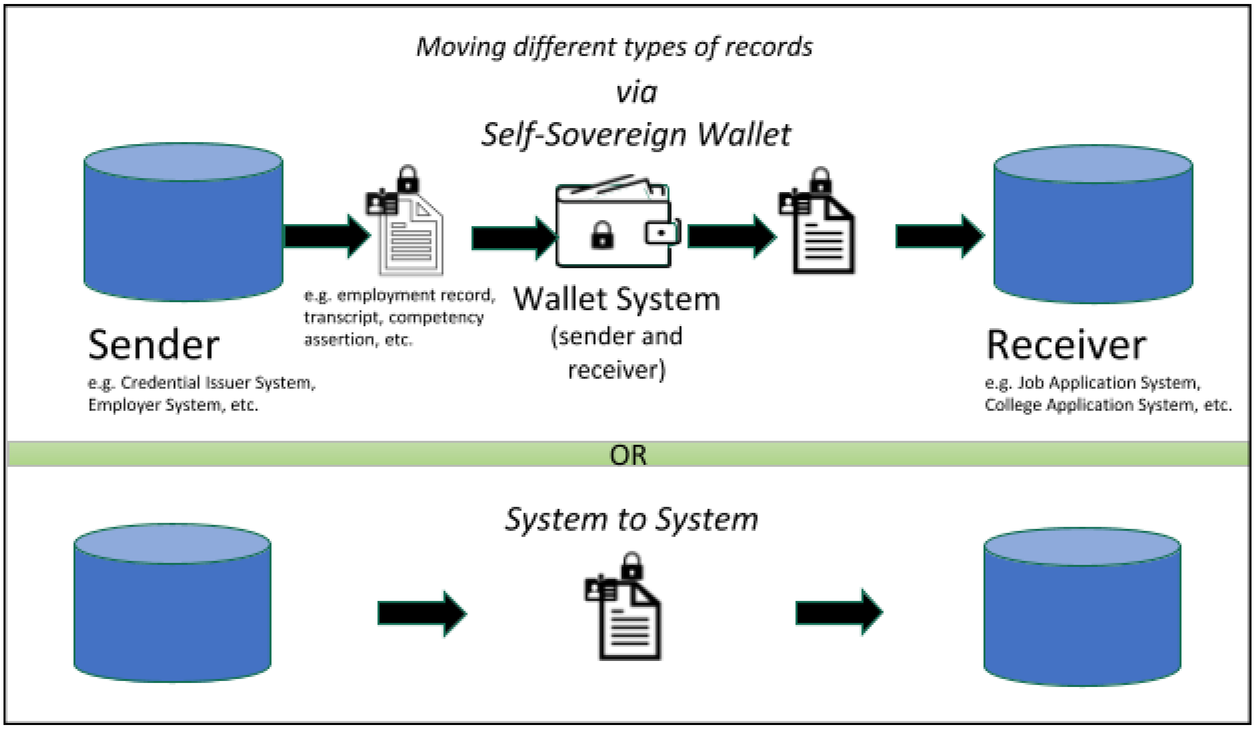
[7] Identifier Authentication - either the trading partners have an agreement on an identity framework being used or there is a resolution service that translates the identifier into one that is understood by the receiver (e.g., DID, URL, email). The ideal method is one in which the system can prove that the individual is capable of authenticating to the identifier. See Verified Presentation.

2. LER Wrapper

The LER Wrapper is the container for an individual record that provides a consistent way to package, transport, store, and discover any type of standardized record. The following diagram shows a conceptual model of the ILR adapted from “Applying Self-Sovereign Identity Principles to Interoperable Learning Records.”


Container
Manifest
issuer
learner
verification method
date issued
vocabulary and packaging used
Content (record)
Interoperable container enables:
consistent way to package, store, and discover contents
other metadata required to validate the record

This specification supports system to system transport of LERs, complex trust networks, and interoperability with implementations of an LER Wallet.


Moving different types of records
via
Self-Sovereign Wallet
Sender
e.g. Credential Issuer System, Employer System, etc.
e.g. employment record, transcript, competency assertion, etc.
Wallet System
(sender and receiver)
Receiver
e.g. Job Application System, College Application System, etc.
OR
System to System

The LER Wrapper includes:

- **Metadata** applicable to any type of Learning and employment record data
- A **payload** which may or may not be compressed and encrypted

- A **proof** for verification/validation of the record

Each payload of the LER Wrapper may include one of multiple payload formats including JSON-LD, JSON, XML, binary code, and plain text, each representing in different formats the same underlying record. It is highly recommended that standards-based machine-readable serializations should be used in order to allow for scalable interoperability. See Annex for examples.

In the following table, properties not labeled as optional are required for compatibility.

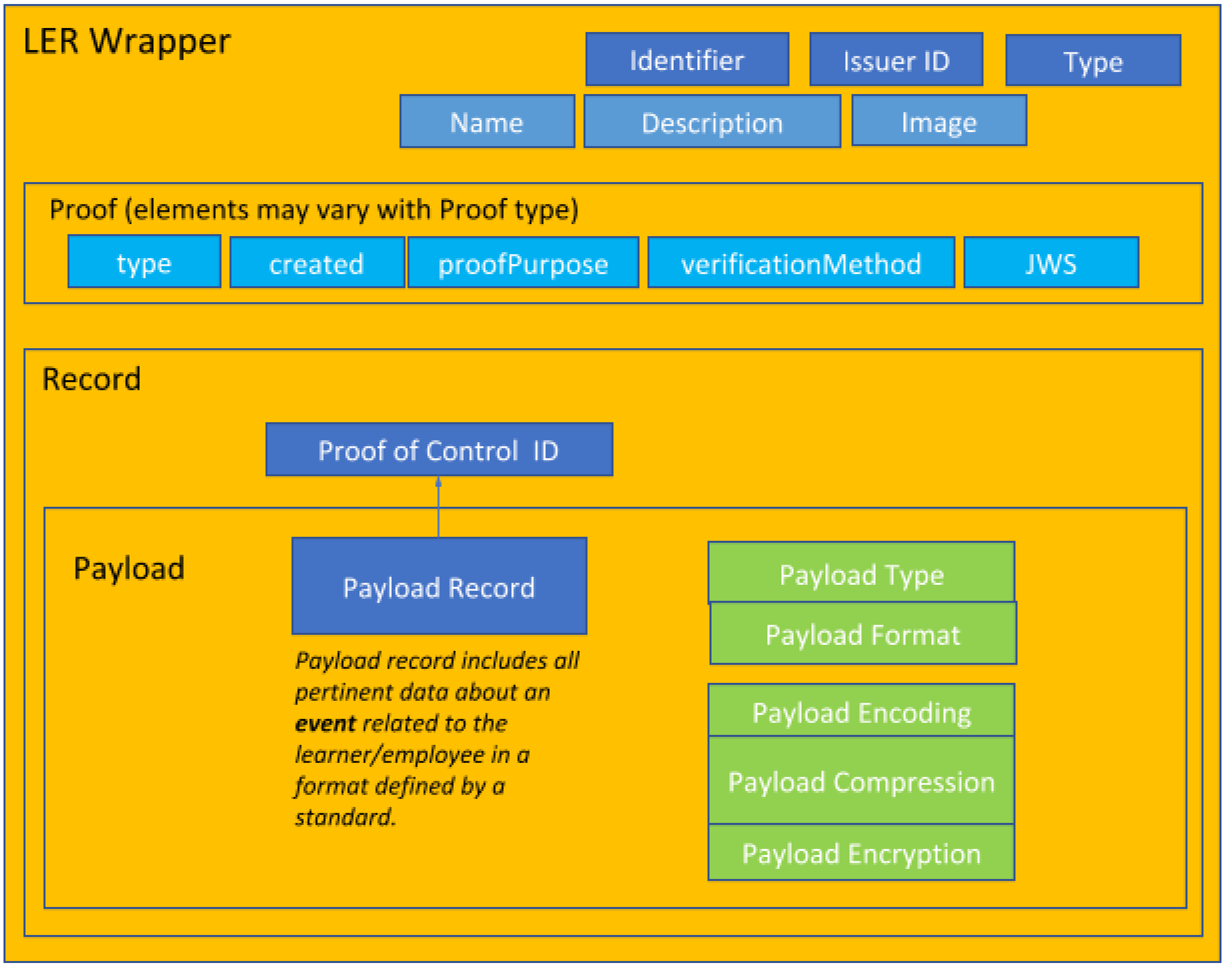
Property	**Definition**	**Format**	**Vocabulary**
Identifier (id)	A unique identifier for the LER Wrapper.	IRI or **DID***	
Issuer Identifier (issuerId)	A unique identifier for the entity that issued the LER.	IRI or **DID**	
Type (type)	The type of JSON object.		(URI to "LERWrapper","VerifiableCredential"in @context)
Date (date)	The date the LER Wrapper was created.	ISO-8601	
Name (name)	The issuer-defined name of the LER (wallet use case).	text	
Description (description) *[**optional**: supports wallet use case]*	The issuer-defined description of the LER.	text	
Image (image) *[**optional**: supports wallet use case]*	A URL for an issuer-specified image.	URL	
[Record]			
proof-of-control Identifier (pocId)	An identifier for the subject of the record used to prove that the record is associated with the holder/presenter. (This may or may not uniquely identify a physical person.)	IRI or **DID**	
[Payload]			
Payload Type (type)	JSON-LD type specifying the standard used to serialize the LER payload (standard schema with version).		(Defined using JSON-LD @Context)

Payload Format (format)	The format of the payload specified as an IANA Media Type (assumed to be JSON-LD if not specified).		(Using IANA Media Type, e.g. application/ld+json | application/json | application/xml | application/pdf**)
Payload Encoding (encoding)	The encoding of the payload.		native | multibase | string (see definitions below)
Payload Compression (compression)	The compression method used on the payload.		none | gzip (see definitions below)
Payload Encryption (encryption)	The encryption method being used on the payload.		(The encryption method is not strictly defined as different environments and trading networks will call for differing encryption protocols.)
Payload Record (payloadRecord)	The LER in the standards-defined record type, either JSON-LD or other formats.		(Anything that can be carried in JSON-LD, non-LD formats must be encoded.)
Proof			
type		JSON	
(elements may vary with Proof type) (See 3.3)			

*Decentralized Identifier (DID) recommended.

**Payloads with human-readable content could also include alternative machine-readable content if possible. JSON-LD is the preferred machine-readable format. Standards using PDF presentation should, if practical, include machine-readable or parsible embedded metadata and content to support discovery and curation.

The following diagram shows the structure of the LER:



See examples in Annexes.

2.1. Payload

The payload is LER data that is:

- Compatible with any standard or supported payloadType (specified by "payloadType").
- In a particular format, specified by "payloadFormat," which may correspond with an IANA -registered media type.
- Encoded for transport using the method specified in payloadEncoding.
- Compressed using the method specified in "payloadCompression".
- Displayable.
- Encrypted using the method specified in "payloadEncryption".

An LER Wrapper may contain multiple payloads. The payloads in a single wrapper should represent the same essential record, for example, a PDF and JSON-LD representation of the same achievement. See section 3 on Verifiable Presentation for recommendations on bundling multiple LERs for transport or presentation.

Payload Types

The payload is any JSON-LD compatible object or any content encoded for JSON-LD compatibility. The LER "Payload Type" metadata element uses a JSON-LD Type which allows LER issuers to specify how to interpret the payload semantically. It relies on JSON-LD context provided by payload specification providers, such as those listed in the section titled "Payload-Specific Normative References." This allows LERs to wrap any type of payload, including types not yet formalized at the time of writing this specification.

For example, PESC can host a PESC Master Context file that defines PESC LER types such as the PESC College Transcript Serialized in XML. Then anyone wishing to issue an LER based on that type simply includes the PESC context and uses the appropriate type value for the payload (see Annex B - @Context Files Hosted by standards organizations and Annex B for examples of LERs with different payload types).

The Payload Types that are most likely to be used are referenced in the Payload-specific normative reference above.

Values for other payload properties are as follows:

	Controlled vocabulary specifications
Payload Format (format)	The IANA Media Type of the payload as specified at https://www.iana.org/assignments/media-types/media-types.xhtml.
Payload Encoding (encoding)	Native - JSON-LD native encoding [JSON-LD] Multibase - Multibase as defined by [https://github.com/multiformats/multibase] String - JSON string per RFC8259 [JSON]
Payload Compression (compression)	None - *no compression* Gzip - Compression as specified by RFC1951

2.2. Proof

The proof makes the record tamper-evident and establishes the identity of the issuer. There are many types of cryptographic proofs including, but not limited to, digital signatures, zero-knowledge proofs, proofs of work, and proofs of stake. Issuers are free to use any proof mechanism as long as the trading partners agree to the proof(s) to be used. This design is intentionally open ended to support future innovations in cryptography. As long as future issuers and verifiers agree, new forms of proofs can be applied.

For example: A JSON-LD digital proof has these properties.

Property	**Definition**
type	The cryptographic signature suite that was used to generate the signature.
created	The date the signature was created.
proofPurpose	The required JSON-LD proof property.
verificationMethod	The identifier of the public key that can verify the signature.
JWS	A means of verifying that information in this LER hasn't changed since being signed. *

*Using JSON Web Signature (JWS) IETF-proposed standard (RFC 7515)

See Verification and Authentication Protocols and Annex D for details on how proofs work.

2.3. Verification and Authentication Protocols

LERs use modern cryptography to secure and protect personal information. LERs provide two key mechanisms for assuring that records are legitimate: proofs and proof-of-control.

Proofs

Proofs use cryptographic means to prove that the content of an LER or verifiable presentation has not been modified since creation by the issuer of the record. Using cryptography based on the public identifier of the issuer, the authenticity of the content can be mathematically verified. Technically, this means using a public key known to be associated with the issuer to check the signature in the proof section.

The data model described in this specification is designed to be proof format agnostic. LERs do not normatively require any particular digital proof or signature format. While the data model is a compatible profile of a VC, the proofing mechanisms for these are often tied to the syntax used in the transmission of the document between parties. As such, the proofing mechanism may vary depending on whether the proof is calculated against the state of the document as transmitted, against the transformed data model, or against another form. At the time of publication, at least two proof formats are being actively utilized by VC implementers. Additionally, the Verifiable Claims Working Group documented the following proof formats and how they are being used.

- Section § 6.3.1 JSON Web Token[8]
- Section § 6.3.2 Linked Data Proofs[9]

Proof-of-Control

Proof-of-control is used to establish a robust notion of identity for an individual. Proof-of-control ceremonies can be accomplished in a number of ways, but typically a simple challenge response is used, where the individual demonstrates that he or she controls a specific private key by signing a challenge string. Verifiers—who know the associated public key—can check the signature to prove it was made by someone in control of that private key.

Performing proof-of-control authenticates the current user as a controller of that identifier. For all reasonable purposes, proving someone controls the associated private cryptographic material proves they control the identifier, which means they are a legitimate representative of the subject of that identifier, and more typically, the identifier may be interpreted as referring to the entity that demonstrated proof-of-control.

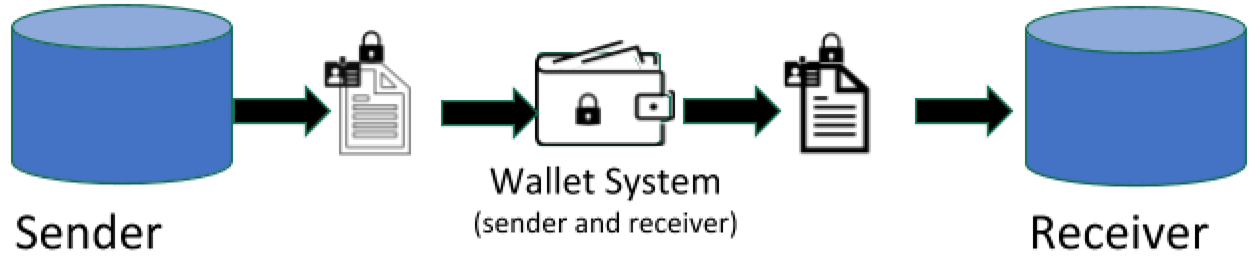
By applying proof-of-control before issuing an LER and then again when presenting an LER, it is established that the party claiming the record is the entity who earned it. This is how to avoid the fraudulent presentation of LERs by individuals who did not earn those records.

See Annex D – Verification and Authentication Details for more.

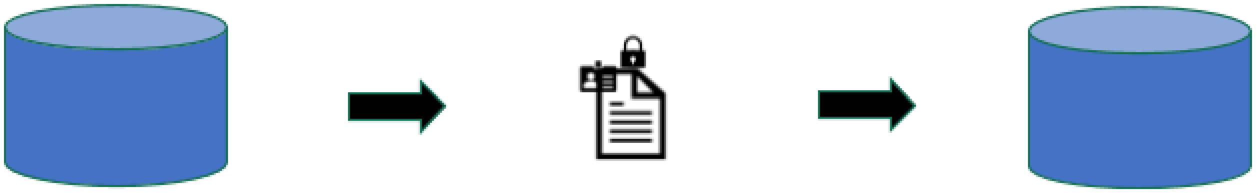
[8] https://www.w3.org/TR/vc-data-model/#json-web-token
[9] https://www.w3.org/TR/vc-data-model/#linked-data-proofs

3. Verifiable Presentation of Records to a Third Party

To support sending an LER from a holder to a third-party receiver, an additional layer based on W3C Verifiable Presentation may be used.



Scenario A—Self-sovereign LER Wallet



Scenario B—System to system transfer of LERs

Consider the two scenarios illustrated above: one with the LER Wallet and one without. In the wallet scenario (A), the individual is the intermediary in the exchange of records. In the other scenario (B), the individual is not involved as two organizations are directly sharing records.

In both cases, recipients must be able to decide whether or not the records should be treated as legitimate.

Verifiable presentations enable the recipient to have cryptographic proof of who gave them the record or records. This is vital because in Scenario A, it would be an identity fraud problem to assume the provider of a given LER is the subject.

In Scenario B, the case of system-to-system transfers, this mechanism allows entities to definitively know who provided a given record set, even when they are not the issuer of the underlying credentials. Other means of aggregation can be used, but Verifiable Presentations are a lightweight mechanism already specified in the VC specification. Verifiable Presentations can be used with or without the proof part, making them the simplest way to combine verifiable credentials, including LERs, into a single digital deliverable.

For example, an independent learning system could accumulate LERs issued by various schools, programs, and employers to a particular individual, which then may provide those credentials to a public sector employment service. This separation provides assurances that both the original records are authentic and that the most immediate source is known.

For the wallet transfer, things are more interesting. Presumably, the individual is the one providing the LER. It is imperative to discern between the individual who earned the record and an imposter who is attempting to claim a record as their own. In both cases, checking the proof of the presentation ensures both the integrity of the record set and the identity of the provider of that set. In the wallet case, we also get an additional layer of assurance: proof-of-control.

Verifying the presenter is in fact the person who earned an LER is known as identity-proofing. With VCs and LERs, a form of identity proofing is enabled by dual proof-of-control ceremonies: one prior to issuing the LER and one during presentation of the LER.

At both of these points, the individual demonstrates control over private cryptographic information (typically a private key), demonstrating a rigorous notion of identity using the latest, best practices in cryptography. This pattern of confirming proof-of-control before issuing a record and then again during presentation of that record is how VCs, and LERs ensure that the person who earned a given record is the same person who is presenting it as their own.

Verifiable Presentation Format:

```
{
  "@context": ["https://www.w3.org/2018/credentials/v1"],
  "type": "VerifiablePresentation",

// The following optional proof is to verify the holder has sent the set of learner records to the receiver
(not to verify the issuer) and that the content has not been tampered with.
  "proof": {
    "type": "RsaSignature2018",
    "created": "2018-09-14T21:19:10Z",
    "proofPurpose": "authentication",
    "domain": "http://www.example.com",
    "challenge": "e506f108-9c74-4c52-b84c-a7019c83328c",
    "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5XsITJX1CxPCT8yAV-
TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqsLfRoPsnsgxD-WUcX16dUOqV0G_zS245-
kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh4vGHSrQyHUGlcTwLtjPAnKb78"
  },

  "learnerRecordSet": [

// One or more LER Wrappers goes here

]
}
```

This presentation format may be used without a proof property for institutions communicating over a secure channel and transmitting any number of LERs in batches. Alternatively, senders and receivers who don't need the identity-proofing features of proof-of-control may simply send the LERs directly, without using a Verifiable Presentation.

INTENDED USE AND NEXT STEPS

The draft specification for the LER Wrapper and Wallet was developed as a future-proof and will continue to be reviewed and updated by the T3 Network's phase two project teams, including: Map and Harmonize Data Standards, Comprehensive Learner/Worker/Military Records Standards, and Management and Use of Individual-Level Data Records. When the LER Resource Hub is launched in 2020, this draft specification will be included on the Hub as a resource for LER pilot teams to voluntarily review and pilot-test. Findings from the LER pilot teams will help to improve and update the LER Wrapper and Wallet specification.

Additionally, the draft specification was developed in the public domain so that standards organizations, and other organizations, may review, further develop, and adopt the specification through their own organization's processes. This draft specification was developed through the T3 Network to embrace and leverage all learner, worker, and military standards, not replace them.

ANNEX A – PARTICIPANTS AND CONTRIBUTORS

Standards organizations who gave input on this document:

- Access for Learning Community - Larry Fruth
- Common Education Data Standards - Jim Goodell
- Dublin Core Metadata Initiative / LRMI - Phil Barker (also advising on metadata and schema.org)
- HR Open Standards Consortium - Kim Bartkus
- IEEE Learning Technology Standards Committee - Simone Ravaioli
- IMS Global - Andy Miller
- MedBiquitous - Johmarx Patton
- Postsecondary Electronic Standards Council - Michael Sessa
- Credential Engine - Stuart Sutton

Technical workgroup participants and reviewers:

- Rick Barfoot
- Avron Barr
- Yvette Cameron
- Deb Everhart
- Matt Gee
- Jeff Grann
- Tom Green
- Nick Hathaway
- Mike Hernandez
- Scott Hinkelman
- Colin Hutchison
- Jeanne Kitchens
- Phil Long
- John Lovell
- Andy Miller
- Joshua Marks
- Robby Robson
- Timothy Ruff
- Alan Davies
- Bob Sheets
- Stuart Sutton
- Joshua Westfall

Technical Advisors:

- Kim Hamilton-Duffy
- Jim Kelly
- Dave Longley

Editors:

- Jim Goodell
- Joe Andrieu
- Alex Jackl

NOTE: This document is being developed under a Creative Commons Attribution 4.0 International License by the T3 Innovation Network based on work at uschamberfoundation.org/t3-innovation. Participants and contributors listed in Annex A were responsible for notifying the other participants of any copyright or patent claims that are potentially essential to implementation of the proposed specification under consideration by the group that are owned or controlled by a participant and contributor or the entity he or she is from, employed by, or otherwise represent. For the benefit of the project any other participant who knows the identity of any holders of any other potential patent or copyright claims that are potentially essential to implementation of the proposed specification that have not already given assurance to support this openly licensed specification should inform the other participants so that appropriate action may be taken to resolve potential conflicts.

ANNEX B – JSON-LD CONTEXT FILE AND W3C VERIFIABLE CREDENTIALS (VC) ALIASES

This specification is based on and fully supports the VC 1.0 specification. It uses aliasing of JSON-LD terms to convey the broader applicability of payloads within the LER Wrapper and Verifiable Presentation. It also meets the minimum requirements to be processed as a VC.

Minimum requirements to have a VC Record

VCs **MUST** have:

1. @context (must be an array, start with https://www.w3.org/2018/credentials/v1)
2. type
3. Proof Type
4. credentialSubject (learnerRecord) id (pocId)
5. issuer (URI or JWK) (issuerId)
6. issuanceDate (date)

Minimum requirements to have a Verifiable Presentations

Verifiable Presentations must have:

1. @context (must be an array, start with https://www.w3.org/2018/credentials/v1)
2. type

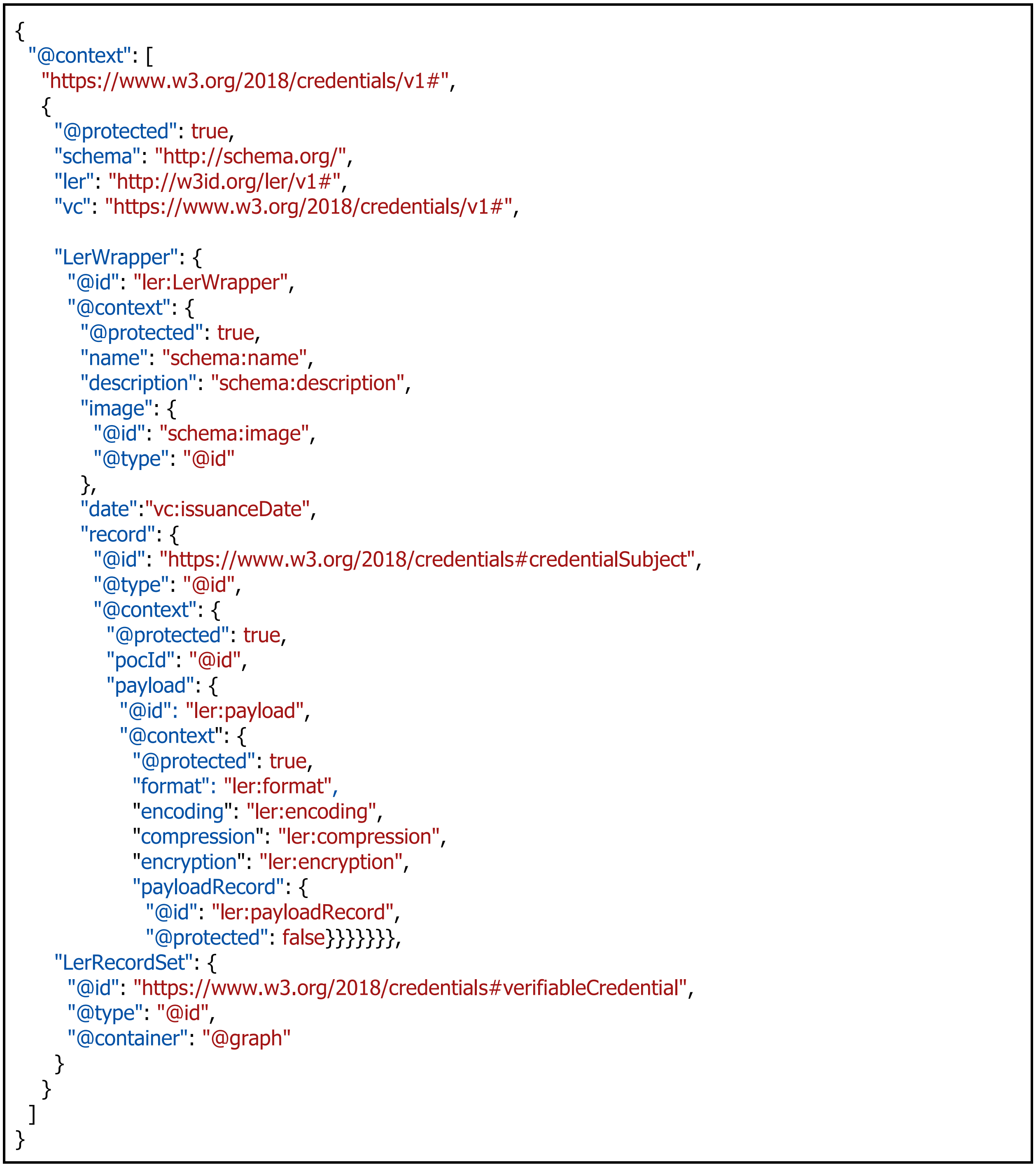
Aliases Used in the Specification

The following table lists aliased terms.

This Spec	VC Spec	Reason
record	credentialSubject	To reflect the broader applicability of records in the Wrapper beyond "credentials."
learnerRecordSet	verifiableCredential	To reflect the broader applicability of records in the Wrapper beyond "credentials."
pocId	id	Aliased "credentialSubject" as "Learner Proof of Control Identifier" to avoid confusion over the meaning of the term "subject" as the learner, not a topic or knowledge domain. This alias is also intended to introduce "proof of control" to avoid possible confusion that this is something like a student id number or social security number.
date	issuanceDate	To avoid confusion about records that are not credentials and misunderstanding that this might be the date that a credential was conferred rather than the date the LER was issued.

(Using method developed by Kim Hamilton Duffy : https://github.com/kimdhamilton/jsonld-alias/blob/master/README.md)

The Learning and Employment Record context file used for this specification (http://w3id.org/ler/v1).



```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1#",
    {
      "@protected": true,
      "schema": "http://schema.org/",
      "ler": "http://w3id.org/ler/v1#",
      "vc": "https://www.w3.org/2018/credentials/v1#",

      "LerWrapper": {
        "@id": "ler:LerWrapper",
        "@context": {
          "@protected": true,
          "name": "schema:name",
          "description": "schema:description",
          "image": {
            "@id": "schema:image",
            "@type": "@id"
          },
          "date":"vc:issuanceDate",
          "record": {
            "@id": "https://www.w3.org/2018/credentials#credentialSubject",
            "@type": "@id",
            "@context": {
              "@protected": true,
              "pocId": "@id",
              "payload": {
                "@id": "ler:payload",
                "@context": {
                  "@protected": true,
                  "format": "ler:format",
                  "encoding": "ler:encoding",
                  "compression": "ler:compression",
                  "encryption": "ler:encryption",
                  "payloadRecord": {
                    "@id": "ler:payloadRecord",
                    "@protected": false}}}}}}}},
      "LerRecordSet": {
        "@id": "https://www.w3.org/2018/credentials#verifiableCredential",
        "@type": "@id",
        "@container": "@graph"
      }
    }
  ]
}
```

ANNEX C - @CONTEXT FILES HOSTED BY STANDARDS ORGANIZATIONS

Each standards body will be able to manage the contexts for its own standards by hosting a JSON-LD context file on its domain. This master contact will include a label and URL for each of its standard/versions that will be specified as the payloadType for a learnerRecord.

Example master context file for a standards organization—pointing to separate context files for each standard

Master File—One Per Standards Organization (e.g. https://example.com/standards/)

```
{
  "@context": {
          "Alumni1.0" : "https://example.com/standards/Alumni1.0",
          "Alumni2.0" : "https://example.com/standards/Alumni2.0",
          "Alumni3.0" : "https://example.com/standards/Alumni3.0",
          "Alumni3.0-jsonld" : "https://example.com/standards/Alumni3.0-jsonld",

          "XYZDonorStandard3" : "https://example.com/standards/XYZDonorProspect1.0"
  }
}
```

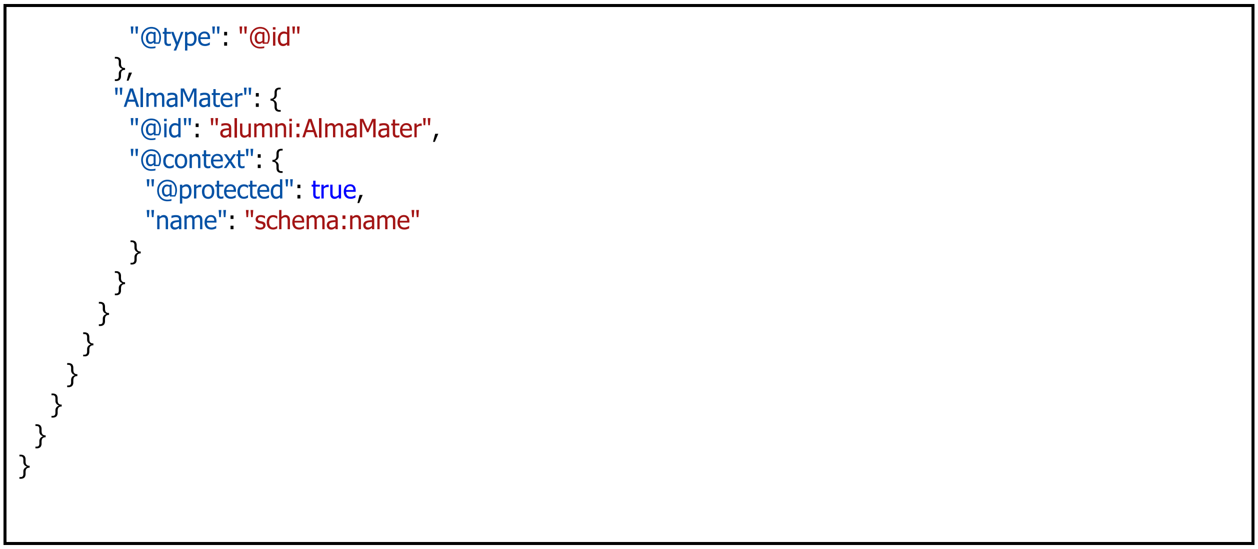
Example Context File For One Standard—Minimal example showing a context file for a fictitious standard (XYZ Standards Association's "Alumni" standard version 1.0) : https://example.com/standards/Alumni1.0

Context File—One Per Standard

```
{
   "@context" : {
      "alumni" : "https://example.com/standards/Alumni1.0/context#"
         }
}
```

Standard File—Context file for a fictional JSON-LD-based standard:
http://w3id.org/ler/alumni

```
{
  "@context": {
    "@protected": true,
    "schema": "http://schema.org/",
    "rdf": "http://www.w3.org/1999/02/22-rdf-syntax-ns#",
    "ler": "http://w3id.org/ler/v1#",
    "alumni": "http://w3id.org/ler/alumni#",
    "AlumniJsonLd-3.0": {
      "@id": "alumni:AlumniJsonLd-3.0",
      "@context": {
        "@protected": true,
        "payloadRecord": {
          "@id": "ler:payloadRecord",
          "@context": {
            "@protected": true,
            "alumniOf": {
              "@id": "alumni:alumniOf",
```



```
              "@type": "@id"
            },
            "AlmaMater": {
              "@id": "alumni:AlmaMater",
              "@context": {
                "@protected": true,
                "name": "schema:name"
              }
            }
          }
        }
      }
    }
  }
}
```

ANNEX D – VERIFICATION AND AUTHENTICATION DETAILS

There are five key questions that verifiable LERs help answer:

1. Is the record authentic?
2. Is the record from a credible authority?
3. Is the record timely?
4. Who provided the record?
5. Does the record apply to a known person?

The first question is answered by the cryptographic proof on the LER. This proof—typically a digital signature of the underlying record, uses cryptography to verify that the content of the record has not changed since the record was issued. A signed hash of the original record is compared against a computed hash of the received record. If those two hashes are identical, then the recipient knows the content of the record has not been tampered with.

The second question is answered by the public identifier of the issuer, typically a public key or a decentralized identifier (DID). This identifier (either directly or by resolving a DID to retrieve cryptographic material) uniquely identifies the issuer and provides the cryptographic anchor to verify the signature from the first question. The public identifier must be known or at least knowable to the recipient (e.g., it may be retrievable from a federated list of known accredited universities).

These IDs are typically large, complex numbers which are cryptographically authoritative but are otherwise arbitrary. If a recipient sees a record, issued by "did:example:abcxyz," asserting that Example University says "the Learner earned a bachelor's degree," it is imperative to have confidence that did:example:abcxyz is in fact under the control of Example University.

There are four common ways to do this:

- The set of acceptable identifiers could be recorded on an allow-list of those issuers the recipient recognizes for particular records. This puts the onus of making a quality determination of an issuer entirely on the recipient.
- Recipients may be part of a federated system which maintains a list of parties contractually bound to a shared governance framework. This puts the onus of quality determination of an issuer on the federation.
- The credential could have—or be linked to—endorsements by official organizations who have accredited the issuer for particular records. This puts the onus on demonstrating quality on the issuer, subject to the interpretation of the recipient.
- The issuer could be evaluated based on an as-yet-to-be-developed reputation system. Accreditation is one such formal system; however, a recipient could opt-in to a reputation system that is decentralized, peer-driven, or ad-hoc.

Through mechanisms like these, recipients must demonstrate to their own satisfaction that a given public identifier, in fact, is associated with the claimed issuer and that the issuer is a credible authority for the record (e.g., Harvard DayCare may be "Harvard" in a meaningful sense, the day care facilities are not going to be authoritative for higher degrees).

The third question, timeliness, can be determined using an optional status property in the LER, as provided by the issuer. This status mechanism provides a way for recipients to verify that the record, originally issued by a known authority, is still timely. For example, an individual may have had his or her license revoked. Distinct from a simple expiration date in the record, status allows dynamic changes to the state of a credential. It is up to the record issuer to provide a suitable status check service, if desired. Best practice is to use something like a cryptographic accumulator that allows checking if any records in an arbitrarily large set have been revoked without revealing the IDs of those credentials (and it is technically infeasible to check all IDs and derive that set).

The fourth question is answered by the identifier of the party who signed the Verifiable Presentation. Without a Verifiable Presentation, LERs can be passed through any digital channel but can't, on their own, establish or verify who it came from. In some transport protocols, this extra assurance is redundant, but in the absence of a secure communication channel between two known parties, the Verifiable Presentation structure concisely and simply proves who provided the credentials therein.

The fifth question, verifying the presenter is in fact the person who earned an LER is known as identity-proofing. With VCs—and hence with LERs—a form of identity proofing is enabled by dual proof-of-control ceremonies: one prior to issuing the credential and one during presentation of the credential.

At both of these points, the individual demonstrates control over secret information (typically a private key) provably associated with a public identifier (typically a public key or its equivalent). These secrets are fundamental to how modern cryptography works. They underlie the security of the web, bitcoin, and international banking transactions. By demonstrating proof-of-control of a secret, the individual is demonstrating a sense of identity using the latest, best practices in cryptography. With this proof of control, recipients have a robust demonstration that the person presenting an LER is actually the person who earned it.

An example flow of actions is below:

1. **Onboarding**: The issuer onboards the individual into their information system, performing whatever proof-of-personhood deemed appropriate. This could include verifying formal legal documentation, in person interviews, creating an account in the issuer's student information system, setting up two factor authentication, etc.

2. **Authentication at the issuer**: The individual logs into the issuer's system using the issuer's own authentication mechanism and requests an LER.

3. **Identifier challenge**: The Issuer asks for the proof-of-control identifier to be used for issuing the record. In practice, this happens in the background as an automated interaction between the issuer website and the wallet service. This request includes a domain and challenge string.

4. **Challenge response**: The wallet verifies the domain matches the domain name of the website making the request, then signs an empty Verifiable Presentation that includes the domain and challenge string, demonstrating that the person currently using this particular identifier has control over the secret that controls that identifier.

5. **Verified proof-of-control**: The issuer checks the Verifiable Presentation and once satisfied that the proof-of-control is demonstrated, issues a record with the provided public identifier as the individual's proof-of-control identifier.

6. **Storage**: The individual stores that record in his or her wallet.

7. **LER request**: Some time later, a recipient makes a request for an LER (often in response to an individual interacting on a website). This request also includes a domain and challenge string.

8. **Domain verification**: The wallet verifies the domain is the domain name of the recipient.

9. **User consent**: The wallet provides an interface for the individual to respond to the request, either by selecting one or more credentials to send, or declining the request.

10. **Verifiable Presentation**: The selected credentials are wrapped in a Verifiable Presentation, along with the domain and challenge and returned to the recipient.

11. **Verification**: The recipient can now verify
    1. The presentation is authentic.
    2. The presentation includes the challenge string.

3. The proof-of-control identifier for the presentation is the same as the Learner proof-of-control identifier in the LER.
4. Each individual credential is authentic (proof check).
5. Each individual credential is timely (status check).
6. Each individual credential is issued by a credible issuer (see question #2).

With this flow, using proofs and proof-of-control, LERs leverage current cryptographic techniques to ensure the legitimacy of such records when presented to a recipient.

ANNEX E – EXAMPLE CROSS-STANDARDS PAYLOADS

The following examples demonstrate different JSON-LD embodiments of working LERs, based on our initial draft context definitions. They likely contain errors and we expect them to be improved upon by future implementers and standards developers.

To be JSON-LD compliant the examples throughout this document would need to have all comments removed from these examples and the proofs properly generated. Also, the encoded data (e.g., PDF) would need to be complete; it was truncated in the examples. All the examples here may also be found in their unedited JSON-LD at the indicated URLs.

- E1 Alumni Standard Example (Not an established standard)
- E2 Alumni Standard Example with Two Formats
- E3 IMS CLR Example with CTDL Reference
- E4 PESC College Transcript Example
- E5 HR Open Candidate Record Example
- E6 EUROPASS Example

E1 Alumni Standard Example (Not an established standard)

EXAMPLE showing a simple JSON-LD payload asserting that Lila Erickson is an Alumni of Example University and using fictitious "alumni" data standards from the XYZ standards body (which has its files hosted at http://w3id.org/ler).

http://w3id.org/ler/simplest.json

[LER Wrapper]
LER

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "http://w3id.org/ler/v1",
    "http://www.w3id.org/ler/alumni"
  ],
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  "type": [
    "VerifiableCredential",
    "LerWrapper"
  ],
  "issuerId": "did:example:ebfeb1f712ebc6f1c276e12ec22",
  "date": "2010-01-01T19:73:24Z",
  "name": "Alumni of Example University",
  "description": "This record authenticates that the learner is an alum of Example University.",
```

[LER Wrapper].[Record]
ler.record

```
  "record": {
    "pocId": "did:example:ebfeb1f712ebc6f1c276e12ec23",
```

[LER Wrapper].[Record].[Payload 1]
ler.record[0].payload

```
  "payload": {
   "type": "AlumniJsonLd-3.0",
   "format": "application/ld+json",
```

[LER Wrapper].[Record].[Payload 1].[Payload Record]
ler.record[0].payload.payloadRecord

```
   "payloadRecord": {
    "name": "Lila Erickson",
    "alumniOf": {
     "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
     "type": "AlmaMater",
     "name": {
      "@value": "Example University",
      "@language": "en"
     }
    }
   }
  }
 },
```

[LER Wrapper].[Proof]
ler.proof

```
"proof": {
  "type": "RsaSignature2018",
  "created": "2010-01-01T19:73:24Z",
  "proofPurpose": "assertionMethod",
  "domain": "http://www.example.com",
  "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec22#keys-1",
  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5XsITJX1CxPCT8yAV-
TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqsLfRoPsnsgxD-WUcX16dUOqV0G_zS245-
kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh4vGHSrQyHUGlcTwLtjPAnKb78"
 }
}
```

Note: This example uses a custom context to define the properties in the Alumni record, as shown in Annex B (http://w3id.org/ler/alumni).

E2 Alumni Standard Example with Two Formats

EXAMPLE showing one record expressed in two different formats (JSON-LD and PDF) in the payload, both asserting that Lila Erickson is an Alumni of Example University and using fictitious "alumni" data standards from the XYZ standards body.

http://w3id.org/ler/hybrid.json

[LER Wrapper]
LER

```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "http://w3id.org/ler/v1",
  "http://www.w3id.org/ler/alumni"
 ],
 "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
 "type": [
  "VerifiableCredential",
  "LerWrapper"
 ],
 "issuerId": "did:example:ebfeb1f712ebc6f1c276e12ec22",
 "date": "2010-01-01T19:73:24Z",
 "name": "Alumni of Example University",
 "description": "This record authenticates that the learner is an alum of Example University.",
```

[LER Wrapper].[Record]
ler.record

```
  "record": [{
    "pocId": "did:example:ebfeb1f712ebc6f1c276e12ec23",
```

[LER Wrapper].[Record].[Payload 1]
ler.record[0].payload

```
    "payload": {
      "type": "AlumniJsonLd-3.0",
      "format": "application/ld+json",
```

[LER Wrapper].[Record].[Payload 1].[Record]
ler.record[0].payload.payloadRecord

```
      "payloadRecord": {
        "name": "Lila Erickson",
        "alumniOf": {
          "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
          "type": "AlmaMater",
          "name": {
            "@value": "Example University",
            "@language": "en"
          }
        }
      }
    }
  },
```

[LER Wrapper].[Record].[Payload 2]
ler.record[1]

```
    {
      "pocId": "did:example:ebfeb1f712ebc6f1c276e12ec23",
      "payload": {
        "type": "alumni-pdf-3.0",
        "format": "application/pdf",
        "compression": "gzip",
        "encoding": "multibase",
```

[LER Wrapper].[Learner Record].[Payload 2].[Record]
ler.learnerRecord[1].payload.record

```
      "payloadRecord":
"MH4sICATsoF4CA2V4YW1wbGVfYWx1bW5pX2NlcnQucGRmAIz7A5RtMdawC5dt27aNU7Zt27btU7Zt27Zt65Ttqnv67f
7u298/+r+j1xh7ZSVZwZzzSWaSvTepvLAoLSMdGyzpweHsIiwUEysBA4GdoSUsDw[...]"
```

[LER Wrapper].[Proof]
ler.proof

```
"proof": {
   "type": "RsaSignature2018",
   "created": "2010-01-01T19:73:24Z",
   "proofPurpose": "assertionMethod",
   "domain": "http://www.example.com",
   "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec22#keys-1",
   "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5XsITJX1CxPCT8yAV-
TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqsLfRoPsnsgxD-WUcX16dUOqV0G_zS245-
kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh4vGHSrQyHUGlcTwLtjPAnKb78"
  }
}
```

E3 IMS CLR Example with CTDL Reference

http://w3id.org/ler/ims_clr.json

[LER Wrapper]
ilr

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "http://w3id.org/ler/v1",
    "http://w3id.org/ler/clri"
  ],
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  "type": [
    "VerifiableCredential",
    "LearnerRecordWrapper"
  ],
  "issuerId": "did:example:ebfeb1f712ebc6f1c276e12ec22",
  "date": "2010-01-01T19:73:24Z",
  "name": "Atlas CLR",
  "description": "Comprehensive Learner Record from Atlas University (not a real school).",
```

[LER Wrapper].[Record]
ler.record

```
  "record": {
    "pocId": "did:example:ebfeb1f712ebc6f1c276e12ec23",
```

[LER Wrapper].[Record].[Payload 1]
ler.record[0].payload

```
    "payload": {
      "type": "clri",
      "format": "application/ld+json",
```

[LER Wrapper].[Record].[Payload 1].[Payload Record]
ler.record[0].payload.paylaodRecord

```
      "payloadRecord": {
        "id": "https://www.atlas.edu/clrs/4d756478-b0a2-40b4-900c-a6feb3c30566",
        "assertions": [
          {
            "id": "https://www.atlas.edu/assertions/7ac90e9a-cd67-43ce-bcf3-75c6a1d56934",
            "achievement": {
              "id": "urn:uuid:4315420c-07a4-4952-ab96-116b0fb61eca",
              "achievementType": "Certificate",
              "description": "This 6-course Certificate program introduces project management fundamentals to a professional in early state of PM career. Upon completion, the student will have fulfilled the educational requirements of the Project Management Consortium\u0027s Certified Project Management I credential (CPM-I), and be prepared to pass the CPM-I exam; receive a Professional Certificate issued by Atlas University and 12 units of continuing education academic credits; and be prepared to confidently direct project initiation, planning, and execution, and to apply proven project management tools at every stage of a project.",
              "name": "Project Management Introductory Certificate",
              "fieldOfStudy": "Project Management",
              "issuer": {
                "id": "urn:uuid:985366c7-ae5c-4f90-930a-c41deb20a833",
                "address": {
                  "addressLocality": "Portland",
                  "addressRegion": "OR",
                  "postalCode": "99999",
                  "streetAddress": "1429 Walnut Street, 10th Floor"
                },
                "email": "demo@atlas.edu",
                "name": "Atlas University",
                "telephone": "\u002B1 877-674-3122",
                "url": "https://www.atlas.edu",
                "verification": {
                  "type": "Verification",
                  "allowedOrigins": [
                    "www.atlas.edu"
                  ],
                  "verificationProperty": "id"
                }
              }
            },
            "issuedOn": "2020-04-22T00:00:00",
            "recipient": {
              "type": "email",
              "identity": "AliceSmith@email.com",
              "hashed": false
            },
            "verification": {
              "type": "Signed",
              "verificationProperty": "id"
            },
            "alignments": [
       {
        "type": "Alignment",
        "targetType": "CTDL",
        "targetName": "Project Management Introductory Certificate",
        "targetUrl": "https://credentialengineregistry.org/ce-registry/resources/ce-8def8fe1-e4ea-4a4d-
95b6-a4f71ff99c42"
       }
      ]
     }
    ],
    "issuedOn": "2020-04-22T00:00:00",
    "learner": {
     "id": "https://www.atlas.edu/urn/student/818727",
     "email": "AliceSmith@email.com",
     "name": "Alice Smith",
     "sourcedId": "818727",
     "url": "https://www.atlas.edu/urn/student/818727"
    },
    "publisher": {
     "id": "urn:uuid:985366c7-ae5c-4f90-930a-c41deb20a833",
     "address": {
      "addressLocality": "Portland",
      "addressRegion": "OR",
      "postalCode": "97229",
      "streetAddress": "1429 Walnut Street, 10th Floor"
     },
     "email": "demo@atlas.edu",
     "name": "Atlas University",
     "telephone": "\u002B1 877-674-3122",
     "url": "https://www.atlas.edu",
     "verification": {
      "type": "Verification",
      "allowedOrigins": [
       "www.atlas.edu"
      ],
      "verificationProperty": "id"
     }
    },
    "verification": {
     "type": "Hosted",
     "verificationProperty": "id"
    }}}},
```

[LER Wrapper].[Proof]
ler.proof

```
"proof": {
  "type": "RsaSignature2018",
  "created": "2010-01-01T19:73:24Z",
  "proofPurpose": "assertionMethod",
  "domain": "http://www.example.com",
  "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec22#keys-1",
  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5XsITJX1CxPCT8yAV-
TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqsLfRoPsnsgxD-WUcX16dUOqV0G_zS245-
kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh4vGHSrQyHUGlcTwLtjPAnKb78"
```

```
  }
}
```

Note: This LER uses a "connector" context, hosted at http://w3id.org/ler/clri to import the pre-existing JSON-LD context for CLRs. Alternatively, IMS could update the definition for CLRs to include a definition for a "payloadRecord" type. Using a connector context allows us to immediately use the existing work already done by IMS.

```
{
  "@context": {
    "@protected": true,
    "schema": "http://schema.org/",
    "rdf": "http://www.w3.org/1999/02/22-rdf-syntax-ns#",
    "ler": "http://w3id.org/ler/v1#",
    "ims": "http://w3id.org/ler/clri#",
    "clri": {
      "@id": "ims:clri",
      "@context": {
        "payloadRecord": {
          "@id": "ler:payloadRecord",
          "@context": {
            "@version": 1.1,
            "@import": "https://purl.imsglobal.org/spec/clr/v1p0/context/clr_v1p0.jsonld",
            "@propagate": true
          }}}}}}
```

E4 PESC College Transcript Example

http://w3id.org/ler/pesc_transcript.json

[LER Wrapper]
ler

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "http://w3id.org/ler/v1",
    "http://w3id.org/ler/pesc"
  ],
  "id": "http://example.edu/credentials/1872",
  "type": [
    "VerifiableCredential",
    "LerWrapper"
  ],
  "issuer": "https://example.edu/issuers/565049",
  "date": "2010-01-01T19:73:24Z",
```

[LER Wrapper].[Learner Record]
ler.record

```
  "record": {
    "pocId": "did:example:ebfeb1f712ebc6f1c276e12ec21",
```

[LER Wrapper].[Learner Record].[Payload 1]

ler.record[0].payload

```
    "payload": {
      "type": "PESCCollegeTranscript1.6",
      "format": "application/xml",
      "encoding": "string",
```

[LER Wrapper].Record].[Payload 1].[Record]
ler.record[0].payload.payloadRecord

```
ayloadRecord": "<?xml version=\"1.0\" encoding=\"UTF-8\"?> <!-- edited with XMLSPY v2010
 (http:\/\/www.altova.com) -->[...]"
 }
,
```

[LER Wrapper].[Proof]
ler.proof

```
"proof": {
    "type": "RsaSignature2018",
    "created": "2010-01-01T19:73:24Z",
    "proofPurpose": "assertionMethod",
    "domain": "http://www.example.com",
    "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec22#keys-1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5XsITJX1CxPCT8yAV-
TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqsLfRoPsnsgxD-WUcX16dUOqV0G_zS245-
kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh4vGHSrQyHUGlcTwLtjPAnKb78"
  }
}
```

PESC JSON-LD Context file is found at http://w3id.org/ler/pesc

```
{
  "@context": {
    "@protected": true,
    "ler": "http://w3id.org/ler/v1#",
    "pesc": "http://w3id.org/ler/pesc#",
    "PESCCollegeTranscript1.6": {
      "@id": "pesc:college-transcript.1.6",
      "@context": {
        "@protected": true,
        "payloadRecord": {
          "@id": "ler:payloadRecord"
        }}},
    "PESCCollegeTranscript1.7": {
      "@id": "pesc:college-transcript.1.7",
      "@context": {
        "payloadRecord": {
          "@id": "ler:payloadRecord"
        }}},
    "PESCCollegeTranscript1.8": {
      "@id": "pesc:college-transcript.1.8",
      "@context": {
        "payloadRecord": {
```

```
        "@id": "ler:payloadRecord"
      }}},
  "PESCHighSchoolTranscript1.6": {
    "@id": "pesc:high-school-transcript.1.6",
    "@context": {
      "payloadRecord": {
        "@id": "ler:payloadRecord"
      }}},
  "PESCEPortfolio1.0": {
    "@id": "pesc:eportfolio.1.0",
    "@context": {
      "payloadRecord": {
        "@id": "ler:payloadRecord"
      }}},
  "PESCCredentialExperientialLearning1.0": {
    "@id": "pesc:credential-experiential-learning.html#1.0",
    "@context": {
      "payloadRecord": {
        "@id": "ler:payloadRecord"
      }}}}}
```

E5 HR Open Candidate Record Example

http://w3id.org/ler/hr_open.json

[LER Wrapper]
ilr

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "http://w3id.org/ler/v1",
    "http://w3id.org/ler/hr_open"
  ],
  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
  "type": [
    "VerifiableCredential",
    "LerWrapper"
  ],
  "issuerId": "did:example:ebfeb1f712ebc6f1c276e12ec22",
  "date": "2010-01-01T19:73:24Z",
  "name": "Lauren Hoffma's HR Open Academic Candidate Record",
  "description": "This record contains details about Lauren Hoffman's accomplishments using the HR Open Academic Candidate Record standard.",
```

[LER Wrapper].[Record]
ler.record

```
  "record": {
    "pocId": "did:example:ebfeb1f712ebc6f1c276e12ec23",
```

[LER Wrapper].[Learner Record].[Payload 1]
ler.record[0].payload

```
    "payload": {
      "type": "Candidate_academic4.2",
      "format": "application/json",
```

[LER Wrapper].[Record].[Payload 1].[Payload Record]
ler.record[0].payload.payloadRecord

```
      "payloadRecord": {
        "documentId": {
          "value": "Candidate062",
          "schemeId": "SomeVendorAts"
        },
        "alternateIds": [
          {
            "value": "A-235674535",
            "schemeId": "SomeOtherVendorAts"
          }
        ],
        "uri": "https://hr-xml.org/lightweight_recruiting_example/getCandidate/61",
        "person": {}
[...]
      }}},
```

[LER Wrapper].[Proof]
ler.proof

```
"proof": {
    "type": "RsaSignature2018",
    "created": "2010-01-01T19:73:24Z",
    "proofPurpose": "assertionMethod",
    "domain": "http://www.example.com",
    "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec22#keys-1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5XsITJX1CxPCT8yAV-
TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqsLfRoPsnsgxD-WUcX16dUOqV0G_zS245-
kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh4vGHSrQyHUGlcTwLtjPAnKb78"
  }
}
```

This HR Open LER uses a shim context that simply defines the payload type with a "payloadRecord" property:

```
{
  "@context": {
    "@protected": true,
    "ler": "http://w3id.org/ler/v1#",
    "hr": "http://w3id.org/ler/hr_open#",
    "Candidate_academic4.2": {
      "@id": "hr:Candidate_academic4.2",
      "@context": {
        "@protected": true,
        "payloadRecord": {
          "@id": "ler:payloadRecord"
        }
      }
    }
  }
}
```

E6 EUROPASS Example

http://w3id.org/ler/europass.json

[LER Wrapper]
ler

```
 {
   "@context": [
     "https://www.w3.org/2018/credentials/v1",
     "http://w3id.org/ler/v1",
     "http://w3id.org/ler/europass"
   ],
   "id": "http://example.edu/credentials/1872",
   "type": [
     "VerifiableCredential",
     "LerWrapper"
   ],
   "issuer": "https://example.edu/issuers/565049",
   "date": "2010-01-01T19:73:24Z",
   "name": "Leuven's Europass EDCI Credential",
```

[Wrapper].[Record]
ler.record

```
   "record": {
     "pocId": "did:example:ebfeb1f712ebc6f1c276e12ec23",
```

[LER Wrapper].[Record].[Payload 1]
ler.record[0].payload

```
"payload": {
      "type": "Edci_credential.xml",
      "format": "application/xml",
      "encoding": "string",
```

[LER Wrapper].[Learner Record].[Payload 1].[Payload Record]
ler.record[0].payload.payloadRecord

```
      "payloadRecord": "<?xml version=\"1.0\" encoding=\"UTF-8\"?> <europassCredential
xmlns=\"http:\/\/data.europa.eu\/europass\/model\/credentials#\"
xmlns:xsi=\"http:\/\/www.w3.org\/2001\/XMLSchema-instance\"
xmlns:eup=\"http:\/\/data.europa.eu\/europass\/model\/credentials#\"[...]"
      }
    }
  },
```

[LER Wrapper].[Proof]
ler.proof

```
"proof": {
    "type": "RsaSignature2018",
    "created": "2010-01-01T19:73:24Z",
    "proofPurpose": "assertionMethod",
    "domain": "http://www.example.com",
    "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec22#keys-1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5XsITJX1CxPCT8yAV-
TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqsLfRoPsnsgxD-WUcX16dUOqV0G_zS245-
kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh4vGHSrQyHUGlcTwLtjPAnKb78"
  }
}
```

This example uses a simple shim to connect the JSON-LD semantics with the XML file: http://w3id.org/ler/europass

```
{
  "@context": {
    "@protected": true,
    "ler": "http://w3id.org/ler/v1#",
    "europass": "http://w3id.org/ler/europass#",
    "Edci_credential.xml": {
      "@id": "europass:Edci_credential.xml",
      "@context": {
        "@protected": true,
        "payloadRecord": {
          "@id": "ler:payloadRecord"
        }
      }
    }
  }
}
```