StudentReader Learner to Earner Governance Framework

Version 1.0

2023-04-06

1 Primary Document

This document is the Governance Framework for StudentReader.io.

Authors

- Laura Brugioni – StudentReader.io
- Chris Prudhomme
- Darrell O'Donnell, Continuum Loop Inc.

Contributors

- Tony Rose
- Anushka Soma-Patel
- Darryn Brugioni
- Chris Prudhomme
- Christine Martin, Continuum Loop Inc.

Revision History

- beta - was circulated in Fall 2022 to drive understanding and adoption.

Sign Offs

Version Name and Title Date

- beta Laura Brugioni - CEO, StudentReader 11/05/2022
- 1.0 Laura Brugioni - CEO, StudentReader _____

Terms of Use

This document intends to establish a Governance Framework and is a learning tool for the StudentReader.io Learner to Earner Program. StudentReader.io is the Governing Authority of this Governance Framework (GF). StudentReader.io delegates the authority to issue Student ID Credentials described in this Governance Framework. Delegated issuers agree to follow the rules outlined in this Governance Framework for identifying and issuing Student ID Credentials. Upon consent from the Holder of a Student ID Credential, Verification of the Credential should align with the process outlined in this Governance Framework. The Cardano community MAY use this document as a reference implementation when drawing up their ecosystem governance frameworks.

THESE MATERIALS ARE PROVIDED “AS IS.” The Trust Over IP Foundation, established as the Joint Development Foundation Projects, LLC, Trust Over IP Foundation Series ("ToIP"), and its members and contributors (each of ToIP, its members and contributors, a "ToIP Party") expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to the materials. The entire risk as to implementing or otherwise using the materials is assumed by the implementer and user.

IN NO EVENT WILL ANY ToIP PARTY BE LIABLE TO ANY OTHER PARTY FOR LOST PROFITS OR ANY FORM OF INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THESE MATERIALS, ANY DELIVERABLE OR THE ToIP GOVERNING AGREEMENT, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND WHETHER OR NOT THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This document is based on ToIP-Governance-Metamodel-Specification-V1.0. It has been modified to fit into the Trust Continuum™.

1.1 Introduction

This **governance framework** (GF) provides a set of guidelines and principles for the governance of the StudentReader Learner to Earner (SRLE) **trust community**. This GF outlines the roles and responsibilities of the **governing authority** and **governed party**, as well as the processes and procedures for managing the SRLE **ecosystem** in a secure, transparent, and accountable manner.

This GF has been structured following the Trust Continuum methodology. It is partially based on the ToIP Foundation’s Governance Metamodel Specification. The ToIP Foundation and the ToIP stack play a critical role in advancing the field of decentralized identity, and this GF is designed to align with the foundation's principles and objectives.

1.2 Terminology and Notation

The following conventions are used in this document:

1.2.1 Words and abbreviations that are in bold font have a specific meaning in this document and are defined in the Glossary. All terms and patterns or mental models used in this document SHALL be defined in the Glossary, a **controlled document** of the **governance framework (GF).**

1.2.2 The **GF** is written in plain language.

1.2.3 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119

ToIP Governance Requirements Glossary

requirement	In the context of a governance framework (GF), a requirement states a condition that an actor (human or machine) must meet in order to be in conformance. In ToIP-compliant GFs, all requirements MUST be expressed using RFC 2119 keywords.
mandatory	A requirement expressed using one of the following RFC 2119 keywords: "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT."
recommendation	A requirement expressed using one of the following RFC 2119 keywords: "SHOULD," "SHOULD NOT," "RECOMMENDED."
option	A requirement expressed using one of the following RFC 2119 keywords: "MAY", "OPTIONAL."
human-auditable requirement	A requirement expressed in a human language that can only be fulfilled by a human actor performing a set of processes and practices against which conformance can only be tested by an auditor of some kind. In a ToIP-compliant governance framework, human-auditable requirements are expressed as policies.
machine-testable requirement	A requirement written in a machine-readable format such that conformance of a software actor implementing the requirement can be tested by an automated test suite or rules engine. In a ToIP-compliant governance framework, machine-readable requirements are expressed as rules in a rules-based language.
policy	A human-auditable requirement that specifies some set of processes and practices that an actor must follow in order to be in conformance with the requirement.
process	A specified set of actions that an actor must take in order to be in conformance with a policy. A process may consist of a set of practices.
practice	A specified activity that an actor must perform as part of a process.
rule	A machine-testable requirement written in a machine-readable language that can be processed by a rules engine.

specification	A document or set of documents containing any combination of human-auditable requirements and machine-testable requirements needed to produce interoperability amongst implementers. Specifications may be included in (as controlled documents) or referenced from a governance framework.

1.3 Localization

The official language for this GF is currently English (IETF BCP 47 language tag “en”) and there are currently no translations. Should a translation be required, any person or entity MAY create the translations. Submissions should include the contact details for creators, co-creators, and the trust community (if applicable) so that future updates can get translated. StudentReader.io MUST approve translations of this GF and ensure that translations get added to the official GF website.

1.4 Governing Authority

The Governing Authority for the StudentReader.io, Learner to Earner Program Credential Governance Framework is StudentReader.io, specifically Laura Brugioni within StudentReader.io.

StudenReader.io is the governing authority responsible for developing, maintaining and implementing this GF:

- Legal entity: Laura Brugioni laura@studentreader.io
- Entity Name: StudentReader.io
- **Jurisdiction**: California, US
- **DID**: did:prism:a63f61665328d456924988cd64d9cdae643b64eb1a7ae88cae6b7a7c55c6ccc6’

This GF MUST be available on the StudentReader.io website. The published GF MUST clearly state the version history and what has changed so the trust registry (TR) reflects the latest accurate version of the GF used within particular ecosystems.

1.5 Administering Authority

At inception the administering authority and governing authority are both StudentReader.io. Legal and contact details are listed in 1.4. Governing Authority.

As the ecosystem prepares to separate the duties of administering and governing, the following delineation is being considered and operationalized.

The **administering authority** is responsible for the administration of SRLE in accordance with the GF. This includes:

- Managing the list of Issuers that are authorized to issue various credential types under this GF.
- Manage and maintain the studentreader.io site and related applications.

The **governing authority** retains overall responsibility for the governance of SRLE, including:

- Managing the **credential types** that are controlled under this GF.
- Making decisions to add/remove/suspend an Issuer where operating procedures aren't clear.

The **administering authority** is authorized to make decisions related to their delegated administrative responsibilities, subject to oversight and approval by the **governing authority**. The **administering authority** will provide regular reports to the **governing authority** regarding their activities, and will consult with the **governing authority** on any issues or decisions that may impact the overall governance of the SRLE ecosystem

1.6 Purpose

This GF will serve as a starting point for establishing the Student Reader Learner to Earner Trust Ecosystem of learning institutes, education providers, education content developers, digital wallets, scholarship programs, and other verifiers as appropriate to support the learning and earning journey of learners who enter into the ecosystem. The GF is aimed at a closed-loop ecosystem, which will be opened up after the first pilot project.

1.7 Scope

The scope of this GF is limited to a closed-loop pilot project, focused on issuing of scholarships to learners that have completed requirements. It demonstrates simple use cases guided by StudentReader.io, to demonstrate to Issuers, Verifiers, and Learners how self-sovereign identity (SSI) operates in practice within the SRLE Program.

This GF covers the following components:

- Learners - the wallet application and how it is used to receive and use the various credentials that are managed in the SRLE ecosystem.
- Learning Insitutitions - are able to issue verifiable credentials for the learner identity (Student ID Credential) and course completion (Course Completion Credentials).

1.7.1 Key Roles

The following Key Roles will participate in this GF as Governed Roles

- **Learning Institution** - The insitution that is provided access to a learning course. they are responsible for registering learners and issuing course completion credentials.
- **Learner** - An individual that is on a learning journey and taking various courses to improve their skills and knowledge.
- **Verifier** - Organizations and their systems that need to consume the credentials that are in the SRLE ecosystem to meet their needs. The closed-loop pilot is focused on awarding scholarships to students that hold a Student ID Credential from PLP and a AP101 Course Completion Credential.

1.7.2 Key Processes

The following processes will participate in this GF as Governed Roles:

- **Student ID Issuance** - the process by which a learning institution issues identification credentials to its learners.
- **Course Completion Credential Issuance** - the process by which StudentReader issues a credential to a learner who has successfully completed a course.

1.7.3 Out of Scope

- The use of **SRLE credentials** by anyone for any purpose other than for scholarship funding closed-loop pilot project.

1.8. Objectives

This GF SHOULD achieve the following concrete outcomes.

- Allow members of the SRLE ecosystem to understand the credentials types that are controlled by this GF.
- Allow members of the SRLE ecosystem to determine if an issuer is authorized to issue a particular credential type.
- Allow a closed-loop pilot that will help inform the future direction of this GF.

1.9 Principles

Encourage Learners

The GF should always keep the learning path of learners in mind.

Minimal Control

The GF should impose the least governance feasible.

Leverage, Don’t Invent

Whereever possible the GF will leverage already existing systems that are in place. These systems must align with the principles of the SRLE ecosystem GF. (e.g. leverage OpenBadges format in the future assuming alignment with other standards is handled).

Open By Default

The SRLE ecosystem is intended to operate in the open and will embrace an open-by-default posture. Only under exceptional circumstances will information be private.

Open By Design

The SRLE ecosystem should provide open design in its architecture, governance, and community approach.

1.10 Revisions

This GF is subject to periodic revisions to ensure that it remains up-to-date and effective in governing the SRLE ecosystem. The GF can change for the following reasons (non-exhaustive):

- Changes in laws or regulations
- Changes proposed by the existing community
- Changes proposed by potential new community members.

To facilitate transparent and collaborative revision management, revisions to this GF will be managed using GitHub's Pull Request process. The Pull Request process on GitHub provides a transparent and accountable platform for stakeholders to provide feedback and suggest revisions to the GF. All revisions to the GF will be subject to the review and approval of the **governing authority**. The **governing authority** retains the final authority to approve, reject, or modify any suggested revisions to the GF.

1.11 Extensions

At this time, this GF is not allowing extension. However, the governing authority intends to allow for extension in the future. When extension is allowed the GF will follow the general pattern for GF extension that Trust Over IP recommends. This approach will include:

- Specifying the requirements an extension GF must meet to be approved.
- Specifying the approval process by which a GF extension will get created.
- Defining requirements for registration, activation, and deactivation of an approved extension GF.

- Defining the requirements for notification of trust community members about activation or deactivation of an approved extension GF.

1.12 Schedule of Controlled Documents

The following **controlled documents** are included in this document as appendices:

- **Glossary**
  - see Appendix A - Glossary for the glossary of terms.
- **Credential Types** - are managed, versioned and available in this GF.
  - Appendix B - Technical Artifacts.
- **Authorized Issuers** - are managed in this GF.
  - Appendix B - Technical Artifacts.
- **Information Trust Requirements** - defines the requirements that all governed parties must meet.
  - Appendix C - Information Trust Requirements.
- **Growth and Evolution** - As the SRLE ecosystem grows and evolves beyond the closed-loop pilot there are some key principles and approaches being applied.
  - Appendix D - Growth & Evolution

Appendix A - Glossary

This GF includes a glossary that includes terms in the following three general

Categories:

- ToIP core terms that describe the common components of the ToIP model and MUST be used consistently across all ToIP deliverables and ToIP-compliant GFs. These terms are defined in the ToIP Core Glossary.
- ToIP governance terms are specialized terms used to describe ToIP governance concepts. They are defined in the ToIP Governance Glossary.
- <<Self-Sovereign Identity (SSI) terms as defined in the *eSSIF* Glossary>>
- GF-specific terms are terms needed in the context of this GF.

The following list of terms from the ToIP Core Glossary are used in this document:

administering authority	The party tasked with operating the management of a particular governance framework. The administering authority may or may not be the governing authority. For example, a government may be the governing authority for a governance framework administered by an NGO as the administering authority.
ecosystem	A Ecosystem is a set of at least two (autonomous) parties (the members of the ecosystem) whose individual work complements that of other members, and is of benefit to the set as a whole.
governing authority	The party responsible for governing a particular governance framework. The governing authority may or may not be the administering authority. For example, a government may be the governing authority for a governance framework administered by an NGO as the administering authority.
governed party	A party whose actors perform in a [role] defined by a governance framework.
governance framework	A set of business, legal, and technical [definitions], [policies], [specifications], and contracts by which the members of a trust community agree to be governed in order to achieve their desired objectives. ToIP-compliant governance frameworks follow the ToIP governance metamodel.
self-sovereign identity	Self-Sovereign Identity (SSI) is a term that has many different interpretations, and that we use to refer to

	concepts/ideas, architectures, processes and technologies that aim to support (autonomous) parties as they negotiate and execute electronic transactions with one another..
trust registry	A repository which contains a machine-readable listing of approved governed parties deemed compliant by a governing authority over its attributable criteria of its governance framework.
verifiable credential	A tamper-evident credential whose authorship by an issuer can be cryptographically verified. Verifiable credentials can be used to build verifiable presentations, which can also be cryptographically verified. The claims in a credential can be about different subjects.

The following terms are used within this GF and defined by eSSIF:

credential type	the specification of the contents, properties, constraints etc. that credentials of this type must have/comply with.
Holder	Has the capability to handle presentation requests from a peer agent, produce the requested data (a presentation) according to its principal's holder-policy, and send that in response to the request.
Issuer	Has the capability to construct credentials from data objects, according to the content of its principal's issuer-Policy (specifically regarding the way in which the credential is to be digitally signed), and pass it to the wallet-component of its principal allowing it to be issued.
Verifier	Has the capability to request peer agents to present (provide) data from credentials (of a specified kind, issued by specified parties), and to verify such responses (check structure, signatures, dates), according to its principal's verifier policy.

The following terms are used within and are specific to this GF:

Authorized Issuers	learning insitutions that have been granted permission to issue credentials, including Student ID and Course Completion Credential

Compatible Issuer tool	A compatible issuer tool is one that is used by an issuer or verifier that enables the issuing of VCs, receiving of verifiable presentations and the verification of the verifiable presentation for Atala PRISM enabled VCs.
Compatible wallet	A compatible wallet is one that is used by a holder or issuer that enables the issuing, storing and verifying of vCredentials, vNFT's and Ada.
Dependent Processes	Processes that are dependent on the credentials issued and verified within this GF.
Issuer tool	The application/tool a party uses to issue VCs.
Learner	Learners that hold a vCredential from an authorized learning institution.
Publisher	the party responsible for creating and releasing the course reader and related documents as vNFT.
SRLE credentials	set of verifiable credentials that recognize an individual's progression from being learner to an earner through the successful completion of a course.
Student ID Credential	identification credential issued by a learning institution to learners.
Trust Community	The parties that participate in a GF to enable a trusted ecosystem amongst parties that issue, hold and verify VCs.
Verifiable Presentation	The schema/set of data requested from a holder by a verifier.
Verified Credentials	Refers to a verifiable credential issued for the completion of Atala AP101 course

Appendix B - Technical Artifacts

The following technical artifacts are governed and managed in this GF:

- Credential Types
- Authorized Issuers
    - Issuers are authorized to issue specific credential types.

B.1 Credential Types

The following credential types are in use in the SRLE:

- Student ID Credential (SIC) - Issued by a **learning institution** to current learners.
- Course Completion Credential (CCC) - Issued by a learning institution to a learner that has completed a particular course.
    - note: In future versions this credential may be replaced by OpenBadges 3.0 compliant credentials.

The following table indicates the structure of required data attributes along with their data types:

Designator	**Name**	**Description**	**Schema**
SIC	Student ID Credential		Attributes: *FirstName* *LastName* *EmailAddress* *StudentIDNumber* *IssuingInstituteName* *IssuingInstituteDID* *IssuanceDate* *ExpiryDate*
CCC	Course Completion Credential		Attributes: *IssuingInstituteDID* *LearnerEmail* *LearnerFirstName* *LearnerLastName* *CourseName* *CourseVersion*

Designator	Name	Description	Schema
			CourseID *IssuanceDate*

B.2 Issuer List

Each entity will be listed with a name and their Issuer DID along with a list of the **credential types** that they are authorized to issue.

- Power Learning Program - John Kamara
- Atala Prism Pioneer Program - Tony Rose

Issuer Name, Jurisdiction, and DID	Credential Types Authorized
Power Learning Program ● Issuer DID: did:prism:a63f61665328d456924988cd64d9cdae643b64eb1a7ae88cae6b7a7c55c6ccc6	● SIC (Student ID Credential)
Atala Prism Pioneer Program ● Entity name: Atala PRISM (Canvas LMS) ● Issuer DID: did:prism:7031c1b1a755687a2fdd351e2bcdf2d9bce60ac469b08d2e9c37b2de5ff8297d	● CCC (Course Completion Credential)

Appendix C - Information Trust Requirements

The following requirements apply to all **governed parties**.

C.1 Information security

Governed parties must ensure that the information they are responsible for is protected against unauthorized access, use, disclosure, modification, or destruction. This includes implementing appropriate technical, physical, and administrative safeguards to prevent security incidents and promptly responding to any security incidents.

C.2 Information availability

Governed parties must ensure that the information they are responsible for is available when needed by authorized users. This includes implementing appropriate backup and recovery procedures to minimize downtime in the event of an outage or disaster and monitoring system performance to identify and address issues that could impact availability proactively.

C.3 Information processing integrity

Governed parties must ensure that the information they are responsible for is accurate, complete, and valid. This includes implementing appropriate controls to prevent errors, omissions, or unauthorized modifications to information and ensuring that data is processed consistently and reliably.

C.4 Information confidentiality

Governed parties must ensure that the information they are responsible for is kept confidential and only disclosed to authorized parties on a need-to-know basis. This includes implementing appropriate access controls to prevent unauthorized disclosure and monitoring access logs to detect and investigate suspicious activity.

C.5 Information privacy

Governed parties must ensure that the information they are responsible for is handled per applicable laws and regulations related to privacy. This includes implementing appropriate privacy policies and procedures to govern the collection, use, disclosure, and disposal of personal information and ensuring that individuals are provided with clear and transparent information about how their personal information is being handled.

Appendix D - Growth & Evolution

As the SRLE ecosystem moves beyond the closed-loop scholarship pilot, more and more of the ecosystem governance will be codified.

Key areas that are being considered are:

D.1 Risk Assessment

Identifying key risks, assessing them, and identifying vulnerabilities is crucial as the SRLE ecosystem grows. Creating a risk treatment plan will assist in mitigating, accepting, avoiding, and transferring risks.

D.2 Trust Assurance and Certification

Establishing levels of assurance and the conformance and compliance criteria that support those levels of assurance will require formalization of much of the ecosystem. As the trust assurance and certification are created auditors will be engaged to assist in building out a solid conformance and compliance scheme.

D.3 Governance Requirements

As the closed-loop pilot is run, the StudentReader.io founders and other trust community members will be gathering and formalizing requirements.

D.4 Business Requirements

After the closed-loop pilot is run, the trust community will be consulted to determine where value is being created and how that should be recognized.

D.5 Technical Requirements

In the initial “closed loop” stage all technical requirements are under consideration. Specific tools will be used, while interoperability will be considered for the SRLE as it goes beyond the “closed loop” pilot.

Key limitations:

- Wallet application will be limited to ProofSpace.
- Issuing will be done using ProofSpace, which will use Atala Prism v1.4
- Interactions will be proprietary.

All of the key interactions will eventually be open standard/open protocol based.

D.6 Inclusion, Equitability, and Accessibility Requirements

StudentReader.io is committed to promoting fair and equal access to the SRLE ecosystem for all individuals and organizations. Our GF will enable and promote inclusion, equitability, and accessibility.

D.7 Legal Agreements

StudentReader.io will enter into legal agreements with relevant stakeholders as necessary. These agreements will be developed and executed as components of the GF. They will be reviewed and updated as necessary to ensure ongoing compliance with the GF specifications.

These agreements may include but are not limited to service-level agreements with vendors and suppliers, data processing agreements with processors, and confidentiality agreements with partners and clients. StudentReader will develop all legal agreements with the assistance of legal counsel to ensure compliance with applicable laws and regulations.