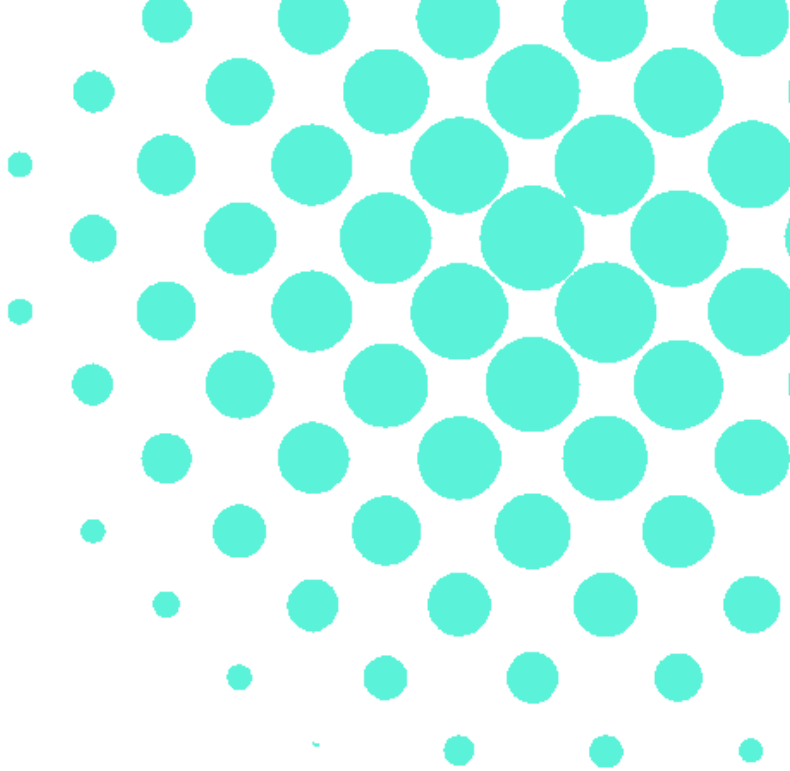


Kiva Protocol

Technical White Paper

Last updated: June 2021

Table of Contents

1. Overview

This white paper provides an overview of the technical infrastructure of Kiva Protocol. It is meant as a primer for stakeholders to understand how Kiva Protocol provides a highly-scalable platform capable of supporting a range of financial inclusion initiatives.

1.1 The Problem

Affordable and accessible financial services are a critical requirement for economic growth and resilience, but approximately 1.7 billion people worldwide remain excluded from the formal financial system[1].

Drawing from Kiva's 15 years of experience facilitating micro-lending across more than 90 countries worldwide, we have a deep understanding of the systemic and structural barriers to financial inclusion. Through our work with a global network of financial service providers serving some of the most marginalized communities, we've seen first-hand how a reliance on manual processes and physical documentation drives prohibitive operational costs and compliance risks, creating seemingly intractable barriers to expanding financial access.

For most financial institutions, the operational and compliance costs of following KYC and CDD regulations create strong disincentives to serving lower-income and previously-unbanked customers; the expected revenue from these accounts simply does not cover the costs of providing service. Similarly, in markets without modern and robust credit reporting ecosystems, the high costs and risks associated with using available financial data leave many consumers without access to credit and other basic financial services.

Forward-thinking governments and regulators are tackling these and similar systemic challenges as part of broader digital modernization initiatives, often with new investments in updated national identification systems and e-government services. Unfortunately, most such projects implement outdated technical approaches, deploying proprietary, monolithic technical systems that create strong vendor lock-in and are difficult and expensive to extend to support new use cases over time. Also, despite growing recognition of privacy risks and increased data protection regulation, most legacy approaches rely on centralized architectures and outdated notions of consent instead of truly embracing the user-centric philosophy of "privacy by design."

1.2 The Solution

Kiva Protocol is a modular, open source technology platform that extends existing systems with modern digital infrastructure, enabling remote digital authentication and secure transaction capabilities. When deployed at national scale, and implemented in conjunction with modernized regulatory and policy frameworks, Kiva Protocol is designed to enable rapid implementation of

[1] World Bank Group: Global Findex (2017)

financial inclusion initiatives, as well as the sustainable development of an ecosystem of private-sector FSPs to more adequately and equitably serve the entire population.

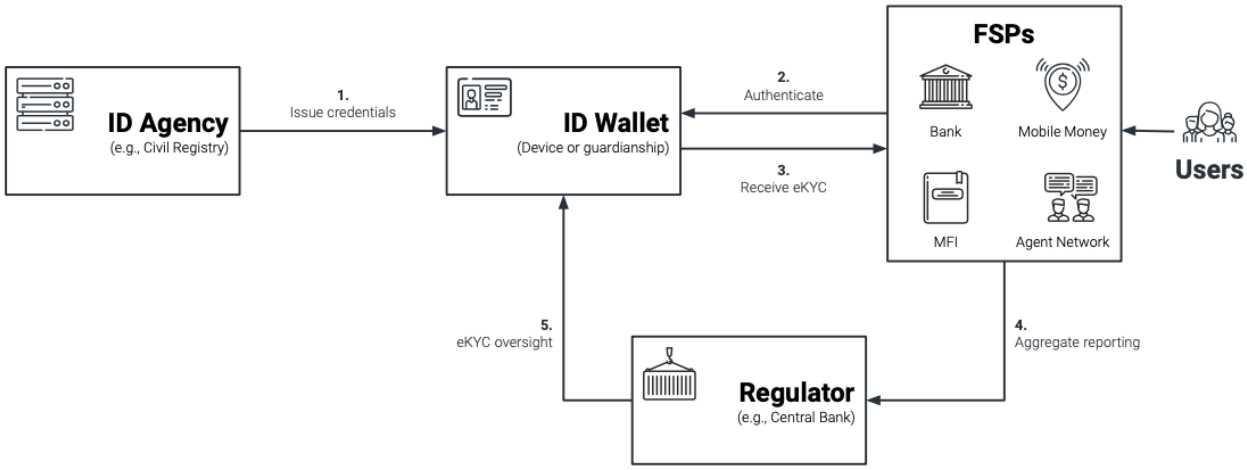
Using the open source decentralized frameworks, Kiva Protocol provides a secure, privacy-preserving authentication layer that spans existing legacy technical infrastructure, enabling government agencies, FSPs, regulators, and individuals to share cryptographically verifiable information in a way that is fast, cheap, secure, and compliant with all national regulations and policies.

Practically speaking, most implementations of Kiva Protocol involve provisioning individual end-users with Wallets that contain government identification Credentials. This base configuration is powerful: it enables financial service providers or public sector agencies to quickly authenticate an Individual with a high level-of-assurance, allowing remote eKYC customer onboarding as well as access to government services.

Kiva Protocol also provides a framework for recording and sharing verifiable financial or credit histories, including from banks, microfinance institutions, humanitarian agencies, or other informal sources. Storing Credentials of these data to an Individual's Wallet creates a trusted, portable, user-centric record that the Individual can use to prove financial history or creditworthiness to other institutions at their discretion. The inherently portable and durable nature of Kiva Protocol Wallets can provide important benefits to refugees and other forcibly-displaced populations where cross-border migration is typically a precondition.

Thanks to Kiva Protocol's decentralized architecture, Individuals are able to self-manage their Wallets through a mobile device; for populations or contexts where self-management is not viable and/or desirable, Kiva Protocol provides a Guardianship modality where a trusted entity can act as fiduciary and provide account management services to Individuals to remotely access the platform under a governance framework.

Fig. 1. Kiva Protocol operational model.



By dramatically reducing both operational cost and compliance risk for FSPs, Kiva Protocol allows fast, cheap, and secure service delivery to traditionally underserved customers. Specifically, Kiva Protocol enables FSPs to transition from manual, time-consuming KYC processes that have high potential for fraud to near-instant, digital eKYC processes that virtually eliminate the possibility of document fraud. This reduces operational costs of customer onboarding as well as compliance costs and risks. For example, instead of storing physical copies of KYC documentation that include personally identifiable information, FSPs can store only the record of a successful KYC check, meeting regulatory responsibilities without the liability of storing unnecessary sensitive customer data.

The result is “Inclusive Integrity”[2]: a system which improves financial access through secure, low-cost customer onboarding while maintaining financial system integrity through robust identity verification.

[2] AFI: KYC Innovations, Financial Inclusion and Integrity in Select AFI Member Countries (2019)

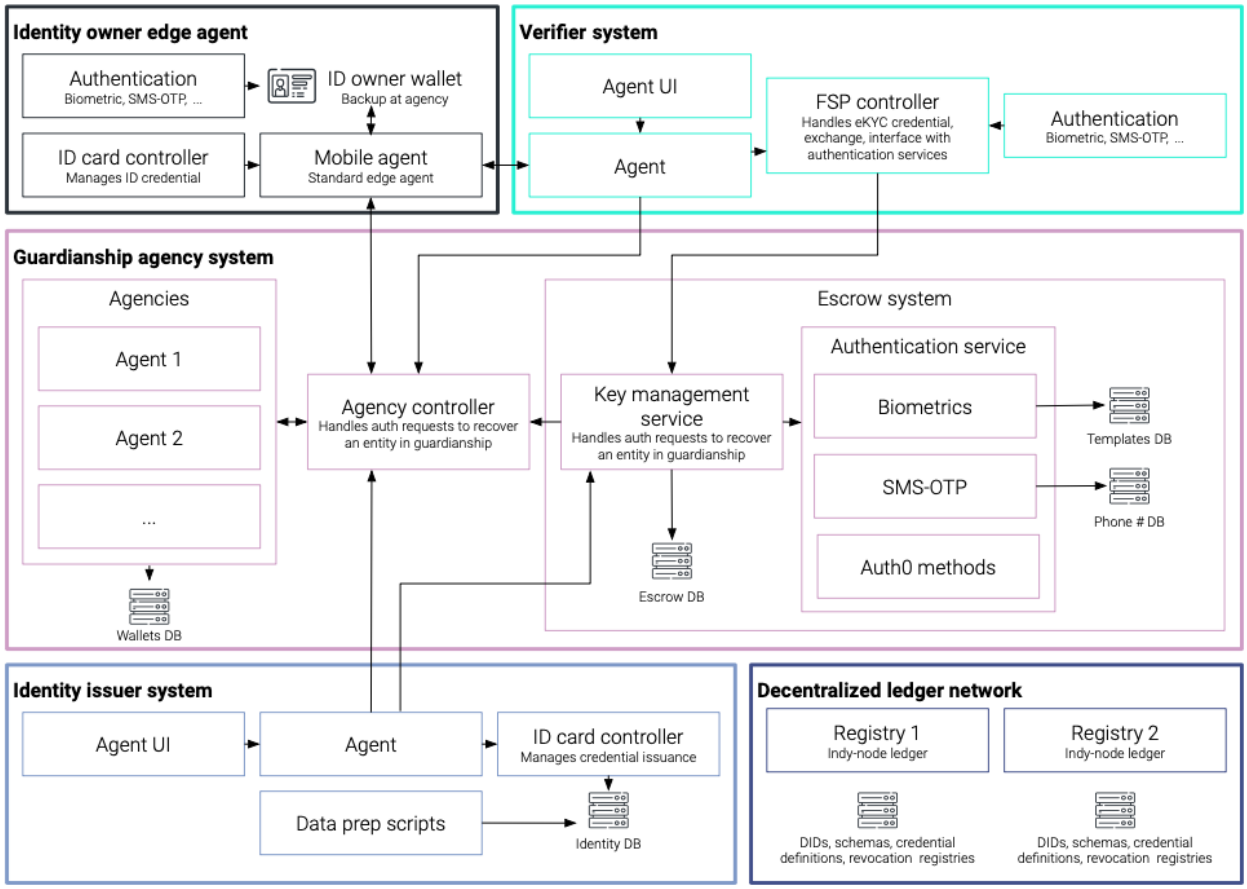
2. Kiva Protocol Technical Overview

Kiva Protocol is built using multiple open source and open-standards communities, especially three projects from Hyperledger: Aries, Indy, and Ursa. Additional open source code is hosted by Kiva in its open source repositories. (Read more about our Commitment to Open Source.)

2.1 Overview of System Components

Kiva Protocol's platform consists of several components, outlined in **Fig. 2** below:

Fig. 2. Overview diagram of the baseline Kiva Protocol architecture



1. Decentralized Ledger Network.

   Sometimes referred to as a Verifiable Data Registry, the Decentralized Ledger Network records DIDs with their authorized cryptographic keys, describes the schemas of Credentials to be issued, and defines how an Issuer will sign and, when desired, revoke Credentials. This enables Verifiers to validate Credentials when they are presented by a Holder.

2. Identity Issuer System(s).

   This system allows the issuance of Credentials that can later be used by Holders for identity verification purposes. This component consists of data import and synchronization scripts as well as an Agent which is used to issue Credentials and represent the Issuer in encrypted communications with other Agents. It is important to note that, although the Agent in this component acts as an Issuer, it may also serve other functions across the platform, including holding Credentials to prove to Verifiers, and requesting proofs from other Agents as a prerequisite for issuing Credentials to a Holder.

3. Guardianship Agency System(s).

   This system hosts Agents on behalf of Holders who are unable or do not desire to self-host. This component of the system is configured to interact with Verifier Agents using predefined policy configurations that define valid authentication mechanisms for Holders. This portion of the system represents Holders who can provide the authentication mechanism. All data is encrypted so that only the Holder can provide access to the data via a valid authentication mechanism. Authentication is provided by the escrow system, which is also configured to provide Wallet backup and recovery mechanisms for Holders who opt to self-host their Wallets on their own device or through another Guardianship Agency System.

4. Identity Owner Edge Agent.

   This system is a mobile application, provided by Kiva Protocol or whitelabeled per implementation or use case, allows the Holder to control their cryptographic keys and interact directly with other Agents in a peer-to-peer manner according to their own interests and policies.

5. Verifier System(s).

   This system represents Entities requesting proof of Attributes contained in Holder Credentials. For example, an FSP could act as a Verifier and request proof of a valid government-issued identification Credential in order to fulfill an eKYC requirement for account opening. Upon receipt of the Attributes, the FSP can validate the revocation status of the Attribute using the Revocation Registry hosted in the Decentralized Ledger Network.

2.2 System Design and Implementation

Kiva Protocol is designed to extend, not replace, existing identification infrastructures. It can span across legacy identification systems, providing new functional capabilities while preserving and relying on the underlying data and processes of the government agencies whose mandate includes identification systems. For example, a government identification agency can maintain existing processes for identity proofing, establishing eligibility, management, revocation, and similar operational processes, while enabling a fast, cheap, secure digital interface for remote authentication and identity verification for the financial sector and otherwise.

Kiva Protocol accommodates a wide range of implementation designs that can be adjusted to handle even the most nuanced stakeholder requirements. The most common configuration, eKYC verification for account opening, is described below for reference. (For other examples, see Additional Configuration Options.)

The default eKYC setup entails the following steps:

1. Ensure an appropriate regulatory environment.

   Successful implementations require the development and implementation of appropriate financial and data protection policies and regulations. Importantly, prudential regulators must ensure that Credentials may be used by FSPs to satisfy KYC and CDD requirements. Modernized regulatory frameworks will include eKYC guidelines that are set by the prudential regulator or the FIU.

2. Determine credential data source(s).

   Creating digital versions of government identification Credentials can be as simple as replicating an existing identity database within a government agency that receives updates when the main database is updated (e.g., when an Individual has died, or a passport has been revoked). Alternatively, the Issuer's Agent software can be integrated with an existing data store or sent batch updates to issue, revoke, or update Credentials. Importantly, Kiva Protocol supports multiple Issuers without requiring harmonization between systems; for example, national identity, driver's licenses, and social protection benefits eligibility Credentials can each be issued independently into a Holder's Wallet.

3. Register the Credential Issuer(s).

   Once the data has been collected and prepared, the Issuer Agent is initialized and four objects are written to the distributed ledger layer: (i) the public DID of the Issuer; (ii) the Credential Schema; (iii) the Credential definition that describes the signing keys; and (iv) and the Revocation Registry. None of these data fields contain any Individual PII, and are foundational for the system as they enable Verifiers to confirm validity and provenance of Credentials when they are provided by a Holder for eKYC or CDD verification.

4. Establish Guardianship governance.

   The Guardianship Agency system creates a fiduciary role for an entity (public or private sector) to act as a trusted intermediary for Individuals who cannot, or prefer not to, manage their digital Credentials directly. For example, Individuals who do not have internet or device access can rely on a Guardianship Agency to help manage and share their Credentials with participating Verifiers. The Guardianship Agency system also provides account recovery and authentication services as part of the Escrow System. These critical functions require robust governance frameworks to establish data protection policies as well as termination of the Guardianship role (e.g., when an Individual assumes full control of their Credentials and no longer relies on the Guardianship Agency).

5. Determine authentication method(s).

   Kiva Protocol supports a variety of common authentication methods, including biometrics (e.g., fingerprints), SMS-OTP, or any other suitable mechanism that can be relied upon for verifying the physical presence of the identity Owner at the time of authentication. In order to build a Key Guardian Service, a user must initially authenticate to establish identity ownership to claim control of a Wallet, and then subsequently authenticate anytime they wish to use the Guardianship Agency to interact on their behalf. The same mechanism can also be used to recover an Individual's Wallet in the event that they require such support.

6. Issue Credentials.

   The Issuer creates digital versions of its identity Credentials, placing them into each Individual's Wallet. The process of issuing Credentials creates an Agent for each Individual hosted in the Guardianship Agency System, which can be used to share data with the Individual's consent via remote authentication. Authentication factors such as the biometric template data or phone numbers are sent to the Key Guardian Service, enabling authorized Verifiers (e.g., FSPs) to provide remote authentication services (e.g., fingerprint scan at an FSP branch office).

7. Onboard participating FSPs.

   When an FSP enrolls in the program, it installs the Verifier system at the point of physical interface with its customers, for example at a branch teller terminal. This way, authentication may be processed at the point of transaction, and the FSP's Verifier Agent can obtain the requested proof based on the digitally-verified consent of the Individual. The Verifier Agent can also use the Revocation Registry of the Decentralized Ledger

Network to verify the authenticity and validity of the provided Attributes using cryptographic signatures.

2.3 Summary of Authentication Flow in eKYC Use Case

We summarize here how Kiva Protocol manages the baseline use case of customer eKYC and onboarding at an FSP. This use case is applicable to both in-person and fully-remote onboarding workflows.

1. Authentication Request.

   To verify that the Individual is present, the FSP sends a request to the Key Guardian Service containing Authentication information that confirms Individual presence. As an example, FSPs using Kiva Protocol in Sierra Leone have fingerprint scanners that send an Individual's fingerprint template to the Key Guardian Service.

2. Wallet Unlock.

   The Authentication data (e.g., fingerprint template) is routed through the Key Guardian Service and matched (e.g., in a fingerprint template database) to confirm which specific Individual has authenticated. This unlocks the Individual's identity Wallet and ensures that the Individual Agent is ready to handle requests on behalf of the Individual. Once the API has loaded an Individual Agent, a secure connection is established by exchanging cryptographic keys tied to private pairwise identifiers (peer DIDs). This information can be used to locate the correct Individual Agent and initiate a secure communication channel, which is controlled using a set of APIs from either the FSP Agent UI or via integration with their existing MIS.

3. eKYC Verification Request.

   Using the secure communication channel, the FSP requests Credentials and proofs from the Individual Agent. The Individual Agent verifies that the FSP is a trusted party making a valid request, and presents a one-time proof showing the requested identity data and verifying it was issued by a valid Issuer and has not been revoked. For Individual-controlled Agents, the Individual may be prompted with a notification of the requested data to be shared, enabling seamless, explicit Individual consent.

4. Individual Agent Responds.

   If the eKYC verification request satisfies the conditions and policies established by the Guardianship Agency System (e.g., a valid request from an authorized FSP), the Individual Agent responds with the requested data and cryptographic proof that the data was issued by the Issuer and that the Credentials are not currently revoked.

5. FSP Logs Compliance.

   With the data and cryptographic proof, the FSP can log process compliance with applicable eKYC requirements and then rely on the presented data Attributes as authentic and valid. Instead of having to scan copies of identity documents, transpose them into data objects, and then store them on a server, FSPs can store a simple proof of compliance with the user's profile in their administrative system. This has collateral benefits of data minimization and high privacy compliance for FSPs.

2.4 Additional Configuration Options

In its simplest terms, the core capability of Kiva Protocol is the provisioning of a user-controlled digital wallet, into which organizations can record information in a way that is secure, verifiable, and privacy-preserving. The baseline use case of eKYC discussed above is a foundational application of this to enable digital financial services at population scale.

As a modular, highly scalable technology stack, Kiva Protocol can be configured to enable a wide range of additional use cases. Virtually any information can be issued as a Credential, such as identity documentation, financial history, social benefits vouchers, health records, educational records, property ownership, and many more. Some of these configurations are presently available out-of-the-box, while others are under development both at Kiva Protocol and within the open source community. Below is a brief summary of a few select additional configuration options:

1. Financial Transaction Histories.

   The digital Wallet provided by Kiva Protocol isn't limited to identity Credentials. For example, it can also hold verifiable records of financial transactions, enabling Individuals to demonstrate their financial history to FSPs, employers, or other organizations. Each transaction (e.g., loan repayment) is sequentially recorded into the Individual's Wallet as a Credential, where 3-way cryptographic signatures offer proof that the transaction history is complete (i.e., no missing Credentials). Like all Credentials stored in the Wallet, these transaction histories are portable with the Individual, allowing access and sharing at any point in the future.

2. Shared eKYC Utility.

   The baseline eKYC use case for digital authentication at FSPs can be extended to create a market-wide eKYC utility, where standardized CDD processes allow FSPs to leverage KYC/AML verifications from other participating FSPs. Once an Individual passes an eKYC check and is onboarded to a participating FSP, that FSP can issue a Credential to the Individual's Wallet attesting to the successful eKYC. If permitted, this

new eKYC Credential can be used at other participating FSPs as they authenticate and/or onboard the Individual, removing the need for duplicate verifications and contributing to strong data minimization.

3. G2P Payments.

   Social protection and benefit programs have become even more critical infrastructure in the Covid era. These programs are often challenged with incomplete beneficiary targeting, lack of payment verification, and high service delivery cost. Kiva Protocol enables payment issuers to accurately verify recipient eligibility and securely issue payments through a variety of payment channels, including bank transfer, mobile money, and even voucher-based redemption. This allows fast, cheap, and secure payments to reach beneficiaries, and also provides the foundation for hyper-targeted programs to reach beneficiaries who are not reached by intended payments.

3. Commitment to Open Source

Kiva Protocol is an open source, interoperable platform that includes the efforts of multiple other open source and open standards communities. Kiva Protocol adheres to the high-level Principles on Identification for Sustainable Development[3] which call for open standards and vendor neutrality in the design of digital identity systems to encourage innovation and ensure financial and operational efficiency and sustainability. A strong advantage of this type of standardized identity protocol derives from the interoperability, efficiency, and network effects that can be achieved by working together:

1. No vendor lock-in.
   Because Kiva Protocol is entirely open source software, the implementing Entity is not reliant on a single vendor to maintain the system. Any proficient Entity, internal to the system or a local vendor, can help operate and maintain the system with or without any support from Kiva Protocol.

2. Standards.
   Technical standards and terminology are shared across the open source community. This greatly simplifies integrating Kiva Protocol into existing or new systems for governments, FSPs, and other authorized entities, as there are no domain-specific terminologies or standards to accommodate.

3. Interoperability and extensibility.
   Kiva Protocol is built to support additional use cases beyond eKYC verification, if desired. Adding adjacent services such as business Entity registration, digital driver's licenses, digital voter identity, social protection eligibility, portable health data, and verifiable education records are just a few examples. Moreover, because Kiva Protocol extends the functionality of existing identity systems instead of seeking to replace them, it is typically deployed much faster and without interruption to existing public and private sector programs.

4. Resilience.
   The decentralized architecture of Kiva Protocol makes it resilient in that no external party can revoke the ability to use the system. In addition to removing vendor lock-in, even if all external access to the system was terminated, local operators would retain a then-current copy of the ledger data, and clients would be able to continue with new local-only transactions until a time when updates can be merged back into the upstream system.

Kiva Protocol is proud to operate as part of the open source ecosystem and welcomes all contributions supporting Kiva Protocol and the technologies incorporated therein.

[3] Principles on Identification for Sustainable Development: Toward a Digital Age (2017)

Appendix A: Community Resources

Kiva Protocol is architected and implemented using primarily open source software frameworks, and is itself hosted by Kiva as an open source project. This section contains references to the most common community resources relevant to understanding and using Kiva Protocol.

A.1 Kiva Protocol

As mentioned, Kiva Protocol is an open source platform. Much of the underlying code is available in various open source Hyperledger repositories (see below). New infrastructure and systems built and maintained by Kiva are in the Kiva Protocol Github repository.

A.2 Hyperledger

Much of the foundational code used in Kiva Protocol is hosted at the Linux Foundation within the Hyperledger Project. Especially relevant sub-projects within Hyperldeger are:

1. Hyperledger Identity Working Group: discussion, research, and documentation of methods to capture, store, transmit, and use identities in blockchain, specifically for projects within Hyperledger.

2. Hyperledger Indy: tools, libraries, and reusable components for providing digital identities rooted on blockchains so that they are interoperable across administrative domains, applications, and any other silo.

3. Hyperledger Aries: a shared, reusable, interoperable tool kit designed for solutions focused on creating, transmitting, and storing verifiable digital Credentials in blockchain-rooted peer-to-peer interactions.

4. Hyperledger Ursa: a shared cryptographic library to avoid duplicating other cryptographic work and increasing system security.

In order to maintain compatibility across independent implementations, the Hyperledger community maintains a directory of ratified message types and protocols that are generally accepted as necessary, should the software in question support the functionality. The current state of interoperability can be found in the Aries-RFC directory, and is described in the Aries Interoperability Profile RFC.

A.3 Trust Over IP Foundation

Kiva is a founding member of the Trust over IP Foundation, a Linux Foundation project that is working to define a complete architecture for Internet-scale digital trust that combines both cryptographic trust at the machine layer and human trust at the business, legal, and social layers.

Appendix B: Glossary of Terms

Agent	A software program or process used by or acting on behalf of an Individual or Entity to interact with other Agents. Agents require access to a Wallet in order to perform cryptographic operations on behalf of the Entity they represent.
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
API	Application Programming Interface
Attribute	An identity trait, property, or quality of an Entity.
Authentication	The process of establishing confidence that a person is who they claim to be. Digital Authentication generally involves a person electronically presenting one or more “factors” to “assert” their identity: that is, to prove that they are the same person to whom the identity or Credential was originally issued. These factors can include something a person knows (e.g., a password or PIN), has (e.g., an ID card, token, or mobile SIM card), or is (e.g., their fingerprints) (adapted from NIST 800-63:2017 and World Bank Group, Identification for Development Practitioner’s Guide 2019).
CDD	Customer Due Diligence
Individual	Any natural person deemed eligible to participate in an identity program.
Claim	An assertion about an Attribute of a Subject. Examples of a Claim include date of birth, height, government ID number, or postal address—all of which are possible Attributes of an Individual. A Credential consists of a set of Claims.
Credential	A digital assertion containing a set of Claims made by an Entity about itself or another Entity. Credentials are a subset of Identity Data. A Credential is based on a Credential Definition. The Entity described by the Claims is called the Subject of the Credential. The Entity creating the Credential is called the Issuer. The Entity holding the issued Credential is called the Holder. If the Credential supports Zero Knowledge Proofs, the Holder is also called the Prover. The Entity to whom a Credential is presented is generally called the Relying Party, and specifically called the Verifier if the Credential is a Verifiable Credential. Once issued, a Credential is typically stored by an Agent.
DID	Decentralized Identifier. A globally unique identifier developed specifically for decentralized systems as defined by the W3C DID specification.

Entity	A resource of any kind that can be uniquely and independently identified, as per IETF RFC 3986, Uniform Resource Identifier (URI).
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSP	Financial Services Provider
Guardianship	The process of controlling an Agent on behalf of a user. For Kiva Protocol implementations, typically the identity Issuer uses a Guardianship agency (e.g., the Central Bank) to hold Individual Agents in Guardianship. This allows for straightforward oversight and regulatory enforcement, and also a pathway to enable inclusion efforts that may necessitate delegation of Guardianship to a regulated FSP or otherwise.
Holder	An Entity that is issued a Credential by an Issuer. The Holder may or may not be the Subject of the Credential. If the Credential supports Zero Knowledge Proofs, the Holder is also the Prover, as per the W3C Verifiable Credentials Working Group.
Hyperledger	A Linux Foundation project that develops and hosts open source distributed ledger technologies, found here.
Hyperledger Indy	An open source Hyperledger project for decentralized identity systems, found here.
Issuer	An Entity that issues a Credential to a Holder, as per the W3C Verifiable Credentials Working Group.
Key Guardian Service	A service that holds a copy of a cryptographic key in order to allow an identity owner to use the service without managing the cryptography themselves.
Key Management System	A system for securely backing up and recovering cryptographic secrets used to store or protect other information such that it can only be unlocked and recovered by its owner.
MIS	Management Information System
OTP	One-Time Password, typically sent via SMS text message.
PII	Personally Identifiable Information
Prover	A role played by an Entity when it generates a Zero Knowledge Proof from a Credential. The Prover is also the Holder of the Credential.

Revocation Registry	An online repository of data needed for Revocation defined, in turn, as the act of an Issuer revoking the validity of a Claim or a Credential.
Schema	A machine-readable definition of the semantics of a data structure. Schemas are used to define the Attributes used in one or more Credential Definitions.
Subject	The Entity whose Identifiers are asserted by DIDs and whose Attributes are asserted by Credentials.
UI	User interface
Verifiable Credential	A Credential that includes a Proof from the Issuer. Typically this proof is in the form of a digital signature. A Verifiable Credential uses Zero Knowledge Proofs by default and can usually be verified by the Issuer Public Key stored in the Credential Definition on the Sovrin Ledger. Based on the definition provided by the W3C Verifiable Claims Working Group.
Verifier	An Entity that requests a Credential or Proof from a Holder and then verifies it in order to make a trust decision, as per the W3C Verifiable Claims Working Group.
Wallet	A software module, and optionally an associated hardware module, for securely storing and accessing private keys, other sensitive cryptographic key material, and other private data used by an Entity. A Wallet is accessed by an Agent.
Zero-Knowledge Proof	A cryptographic method where an Entity can prove to another Entity that they know a certain value without disclosing the actual value.