The Design of Proseline

This document outlines the designs of Proseline's data model, protocol, and service architecture.

Projects

The basic unit of organization in Proseline is the **project**.

The main **work** in a project takes the form of **drafts**. Each draft contains the complete content of one version of a document, along with information on who created it, when, and its **parents**—up to two other drafts that it was based on.

Participants can add **marks** to drafts to give them names, such as "current" or "rewrite". Participants can move marks from draft to draft over time.

Participants can add text **notes** to parts of drafts, mostly to share comments.

Participants can add **replies** to notes and the replies of others.

Participants can publish **corrections** to the texts of notes and replies.

Participants

Each project has one or more **clients**, of three types:

1. **Distributors** can share work in the project with others, but can't read the work or contribute to it.

2. **Readers** can read the work in the project, in addition to distributing it.

3. **Writers** can contribute work to the project, in addition to reading and distributing it.

The proseline.com JavaScript application is a client that can distribute, read, and write.

The proseline.com server application is a client that distributes customers' projects.

A person may use one or more **devices**, each of which may run one or more clients. When a person joins a project with at least one client, that person is a **member** of the project.

A person may or may not pay for a proseline.com **account**.

Distributing

Participants contribute work to a project by creating and sharing project-specific **logs**. Each log consists of **entries** for contributions to the project made with that particular client.

One member of a project may contribute to the project with multiple clients. For example, they might use the proseline.com web app on their laptop, smartphone, and desktop.

Accounts

The proseline.com server application provides services to paying customers:

1. The server distributes work on all of their projects, so all members of the customer's projects can download and share it, even when other members aren't online.

2. The server invites all of the customer's clients to all of the customer's projects, so they can work on projects across devices without inviting themself manually.

3. The server stores **invitations** to all the customer's projects, so they can access them even if they lose all their clients.

The server stores keys for reading and writing to projects, encrypted with the customer's **privacy key**.

The server stores the customer's privacy key, encrypted so that the customer can decrypt it using their **privacy phrase**. Participants never send privacy phrases to the server.

People connect their clients to their paid accounts by logging in via links e-mailed to them by the server. The client signs login requests for using its client key.

Cryptography

On starting for the first time, a client generates a **client signing key** for signing requests to the proseline.com server application.

On creating a new project, a client generates:

- a random **project distribution key** for stream encryption of data distribution
- a **project discovery key**, the digest of the distribution key, for finding other clients of the project without disclosing the distribution key
- a random **project read key** for encrypting log entries
- a random **project write key pair** for signing entries to all project logs

On joining a project, a client generates a random **log key pair** for signing entries to the client's project log

Participants wrap each entry to each project log in an **envelope**. Each envelope includes:

- a signature with the project write secret key
- a signature with the log write secret key
- the entry, encrypted with the project read key

Each entry includes a monotonically increasing index, starting with zero. Each entry after the first includes the cryptographic digest of the prior entry in the log.

Each invitation stored by the proseline.com server application includes:

- the project distribution key
- the project write public key
- optionally:
  - the project write secret key, encrypted with the customer's privacy key

  - the project read key, encrypted with the customer's privacy key
  - a title for the project, encrypted with the customer's privacy key

Links

To add someone to a project, users share links generated by their clients:

- links for **distributors** include just the distribution key.
- links for readers also include the project read key and project write public key.
- links for writers also include the project write secret key.