

EGOIST MACHINES

AI Passport Ideathon

PARTICIPANT GUIDE

A guide for choosing a track, shaping an entry, and submitting a clear proposal through the form.



AI Passport Ideathon

7-12
August

One week to define where portable trust should show up first.



Trust should travel

AI Passport is a way for a person, team, creator, organisation, or AI system to carry verified context and permissions between different tools.

We built the passport. Your job is to find one strong application for it, explain why it matters, and show how it would work in the real world.

The core question

Where can AI Passport be used best?

A strong entry is clear enough that a stranger can understand the problem, the person affected, the moment it is checked, and the first version that should exist.





For people who want to own their context

This ideathon is for students, builders, designers, writers, researchers, and young people who think personal context should belong to the person it describes.

Most systems treat context as something institutions collect, lock away, and use to make decisions about us. AI Passport starts from a different belief: people should be able to carry useful context, grant access on purpose, and take it back.

Students

Start from places where school, work, platforms, or communities ask people to prove something.

Builders

Show a prototype, mockup, schema, or flow that makes the passport moment concrete.

Designers

Make the consent, verification, access, or revocation moment easy to understand.

Researchers

Explain the problem, the risk, and why user control changes the outcome.





One week. One first move.

AUG 07

Kickoff + Session 1

AI Passport understanding.
What it is, what it is not, and
why portable trust matters.

AUG 08

Session 2

How to come up with ideas
and reject them. Turn broad
concepts into specific entries.

AUG 09

Session 3

Understanding AI and privacy.
Consent, misuse, minimal
disclosure, and what should
not be collected.

AUG 10

Session 4

How to submit a winning entry.
Structure, clarity, judging, and
form submission.

AUG 11

Work day

Finalise your entry, ask
questions, polish the
argument, and prepare the
submission form.

AUG 12

Winners announced

Winners announced by track.
Winning teams are invited to
interview for the internship
opportunity.





Each session is live and recorded

1. AI Passport understanding

Leave knowing what the passport carries, who can request access, and how receipts and permissions shape the product.

2. Ideas and rejection

Generate many directions, then cut weak ones. A good entry is narrow, concrete, and tied to a real problem.

3. AI and privacy

Learn the difference between useful context and invasive collection. Design for consent, expiry, and revocation.

4. Winning submission

Shape the final answer for the form: problem, user, claim, workflow, risks, and why this should exist.





Build the thing. Or make the case.

You will submit through a form. Judges read the form first, so your answer needs to stand alone.

Build lane

A prototype, mockup, workflow, schema, or demo.
Show the moment where AI Passport is used.

Concept lane

A deck, memo, brief, policy note, market analysis, or product proposal. Make the case for what should be made and why.

Submit: team name, track, lane, short summary, problem, user, passport claim, how it works, risks, and any file or link.





Track winners get prizes

Work

Winner gets a Kindle. Runners up get a notebook bundle.

Creative

Winner gets Sony headphones. Runners up get a book bundle.

Agents

Winner gets a Pocket. Runners up get Frontier lab merch.

Identity

Winner gets a camera. Runners up get Audible subscriptions.

All winners get 1:1 mentorship and Egoist Machines merch. All runners up get merch too. Winners in each category will interview with Egoist Machines. One winner or winning team will be selected for an internship opportunity with a YC-backed team.





For Work

This track is about jobs, learning, teams, hiring, freelancing, credentials, and workplace permissions. Ask where people need to prove what they can do, what they are allowed to access, or how AI helped them work.

INSPIRATION

- Problem: AI-assisted schoolwork is hard to judge. Passport solution: carry a record of process, sources, and review.
- Problem: freelance reputation is trapped on one platform. Passport solution: carry verified work history between tools.
- Problem: team assistants need access without permanent accounts. Passport solution: grant one task, one folder, one expiry.
- Problem: hiring asks for too much private evidence. Passport solution: prove training or skill without exposing full accounts.





What a strong entry should show

Possible directions

- A portfolio passport for AI-assisted work.
- A training proof for safe AI use in a workplace.
- A contractor reputation pass that travels across platforms.
- A permission flow for a team assistant.
- A student skills record that does not become surveillance.

Before submitting

- Name the worker, learner, team, or verifier.
- Say what is currently hard to prove.
- Define the passport claim.
- Explain why the claim should travel.
- Show how the person stays in control.





For Creative

This track is about authorship, consent, licensing, attribution, likeness, synthetic media, remix, and provenance. Ask where creators need their rights and intentions to travel with their work.

INSPIRATION

- Problem: creative work gets reused without clear permission. Passport solution: attach allowed uses to the file or profile.
- Problem: voice, likeness, and samples can spread fast. Passport solution: grant limited permission with expiry.
- Problem: creators need proof without revealing private drafts. Passport solution: verify authorship while keeping notes private.
- Problem: platforms need to know if work can train models. Passport solution: carry a consent receipt that can change.





What a strong entry should show

Possible directions

- A consent pass for training data.
- A licensing receipt for remix or commercial use.
- A creator page that lets platforms request rights.
- A provenance trail for AI-assisted media.
- A limited likeness permission that expires.

Before submitting

- Name the creator and the work.
- Say what permission or proof is missing today.
- Define what travels with the work.
- Explain how consent can be changed or withdrawn.
- Avoid treating creators as a content database.





For Agents

This track is about AI systems acting for people or organisations. Ask how another service knows an agent is allowed to act, what it can do, when permission ends, and how activity is logged.

INSPIRATION

- Problem: agents need to spend or book within limits. Passport solution: carry budget, scope, and expiry.
- Problem: account access is too broad. Passport solution: grant one task, then remove access automatically.
- Problem: services cannot tell who authorised an agent. Passport solution: show a signed permission before action.
- Problem: people need to review agent work. Passport solution: create receipts for actions, access, and refusals.





What a strong entry should show

Possible directions

- A spending permission for a shopping or travel agent.
- A temporary account-access pass.
- A revocation system for agents across tools.
- A receipt trail for agent actions.
- A verifier screen for services receiving agent requests.

Before submitting

- Name the agent, holder, and verifier.
- Set the permission scope.
- Set expiry or revocation rules.
- Show the action receipt.
- Explain what happens when the agent goes outside its scope.





For Identity

This track is about proving the minimum necessary fact. Ask where someone needs to prove they are human, eligible, qualified, affiliated, or unique without exposing more than the situation requires.

INSPIRATION

- Problem: human checks often demand legal identity. Passport solution: prove humanness without showing legal ID.
- Problem: eligibility checks ask for extra records. Passport solution: prove only the required fact.
- Problem: communities need one person per account. Passport solution: verify uniqueness without public names.
- Problem: affiliation can expose private context. Passport solution: prove membership while hiding unrelated details.





What a strong entry should show

Possible directions

- Human proof for online communities.
- Age or eligibility proof with minimal disclosure.
- Role or affiliation proof for a closed group.
- Pseudonymous proof for people who need safety.
- A one-person-one-account system that avoids public identity.

Before submitting

- Name the fact being proved.
- Explain why less disclosure is better.
- Define who verifies the claim.
- Say what is never revealed.
- Explain how mistakes can be appealed or corrected.





What judges look for

- A real problem, not a vague idea.
- A specific person, team, organisation, or system affected by the problem.
- A clear passport claim: what is proved, carried, requested, or revoked.
- A reason this should travel across tools instead of staying inside one app.
- A privacy-aware design that avoids collecting more than it needs.
- A clear next step for the first version.





Final submission checklist

- Can someone understand your entry in one minute?
- Have you named one track and one lane?
- Have you explained the problem without hype?
- Have you defined the passport claim?
- Have you shown who controls access and what can be revoked?
- Have you explained the first version clearly?
- Have you included every required link or file in the form?

End with one sentence: This entry is for [user], who needs to prove [claim] to [verifier] so they can [outcome] without giving away more context than necessary.

