Digital identity on a SIM card

A digital identity and zero-interest microlending system built for people with a phone number and no documents. How registration, verification and lending actually work.

> Most identity systems assume a document to verify against. This one assumes a community that already knows who you are.

THE PROBLEM IT WAS BUILT FOR

Financial exclusion is usually described as a lack of access to banks. More precisely, it is a lack of the thing banks require before access begins: a verifiable identity. A person without a birth certificate, national ID or utility bill in their name cannot open an account, cannot borrow, and cannot build the record that would let them borrow later. The requirement is reasonable on its own terms and excludes roughly a billion people.

The conventional answer is to issue documents, which is slow, expensive, and dependent on state capacity that is often the reason the documents are missing. The project took a different premise: in the communities where this bites hardest, identity is not actually unknown. It is well known locally and simply not written down anywhere a bank will accept.

So the system was designed to capture the knowledge that already exists rather than to manufacture a new document, and to run on the one piece of infrastructure that is close to universal: a mobile number.

REGISTRATION, AND WHY IT IS PEER-VERIFIED

A person registers with a phone number and receives a PIN. Verification of who they are does not come from a document; it comes from existing verified members of the community attesting to them. Each attestation is recorded, and an identity becomes usable once it carries enough of them.

This inverts the usual trust direction. A conventional system trusts a central authority that issued a document and distrusts the individual. A peer-verified system trusts a web of local attestations, which is weaker against a coordinated group and considerably stronger against the ordinary case of a real person with no paperwork.

The obvious attack is collusion: a group vouching for identities that do not exist in order to extract loans. The design answer is that attestation is not free. Vouching for someone ties the voucher’s own standing to their repayment, so manufacturing identities degrades the standing of the people doing it.

RUNNING WITHOUT A SMARTPHONE

A prototype was built as a conventional application, and then rebuilt around SMS, because the population it targets disproportionately does not have a smartphone or reliable data. A system that requires an app to reach the unbanked excludes a large share of them at the first step.

In the deployed form a person registers at a community checkpoint and receives a SIM card, then messages the service through WhatsApp or WeChat: a photograph of themselves, a name, and the details a checkpoint has already witnessed. Those inputs are hashed into a signature recorded on a permissioned ledger, which is what stands in for the document. The stack is deliberately unglamorous - Hyperledger Fabric for the ledger, PGP for encryption, image hashing so a photograph is never itself the record - because every component had to work over a text channel on a feature phone.

The SIM-based version treats the phone number as the account and text messages as the interface. Registration, balance, repayment status and requests all work over a channel that functions on a feature phone, on a weak network, with no data plan.

This is the constraint that shaped most of the rest of the design. An interface of a few characters cannot present terms and conditions, so terms have to be simple enough to state in a sentence. That is a limitation, and it is also the reason the lending product is a zero-interest fixed amount rather than something with a rate structure.

HOW THE LENDING WORKS

Capital begins in community funds rather than with a bank, which matters because it means the first loan does not require a partner institution to accept the identity. Repayment history accumulates against the identity, and that history is the asset the system is really producing.

Each account opens with an interest-free microloan of roughly fifty to a hundred dollars. The account pays interest rather than charging it: once a holder has spent twenty-five, the balance earns about a third of a percent monthly. The direction of that arrangement is the whole design. A conventional product would price the risk of an undocumented borrower into a rate; this one treats the first loan as the cost of manufacturing a credit record that does not exist yet.

Loans are zero-interest and small. The purpose is not to run a lending business; it is to generate a repayment record for someone who has none, so that a partner bank later has something conventional to underwrite against.

The intended path is that the identity graduates. Peer attestation and repayment history together constitute the evidence a regulated institution needs, at which point the person moves into the formal system and the microlending layer has done its job.

WHO BUILT IT, AND WHAT IT RAN ON

The team as submitted was twenty-four people, and the composition is worth stating because it is unusual: eleven of them were advisors drawn from the unbanked communities the system was built for, alongside seven research and engineering advisors and six from banking. A product that depends on local attestation cannot be designed at a distance from the people doing the attesting, and the team was structured to make that difficult to forget.

It ran in Enugu, Nigeria and in the United States, funded entirely by grants and awards, roughly a hundred and fifty thousand dollars. The intended revenue was a share of what partner banks earn on the accounts the system brings them. Partner and advisory relationships spanned banks, card networks and UN agencies. It was submitted to MIT Solve's 2023 Solv[ED] Youth Innovation Challenge, which is where the figures on this page come from.

WHAT WE WOULD FLAG ABOUT IT

Peer verification is a real trust model with real failure modes, and the honest framing is that it trades one attack surface for another. It resists the common case of a person without documents and is weaker against organised collusion than a document check.

An identity system holds exactly the data that is most dangerous if it leaks: who someone is, who vouches for them, and what they owe. Minimisation is not optional in that setting.

Any system that produces a record used to grant or refuse credit is a system that can encode exclusion. If attestation networks track existing social advantage, the credit record produced will track it too.

SOURCES

01 Fidutam Digital ID Project Guide - Perrin & Fidutam, archived

02 Fidutam, solution record, Solv[ED] Youth Innovation Challenge 2023 - MIT Solve