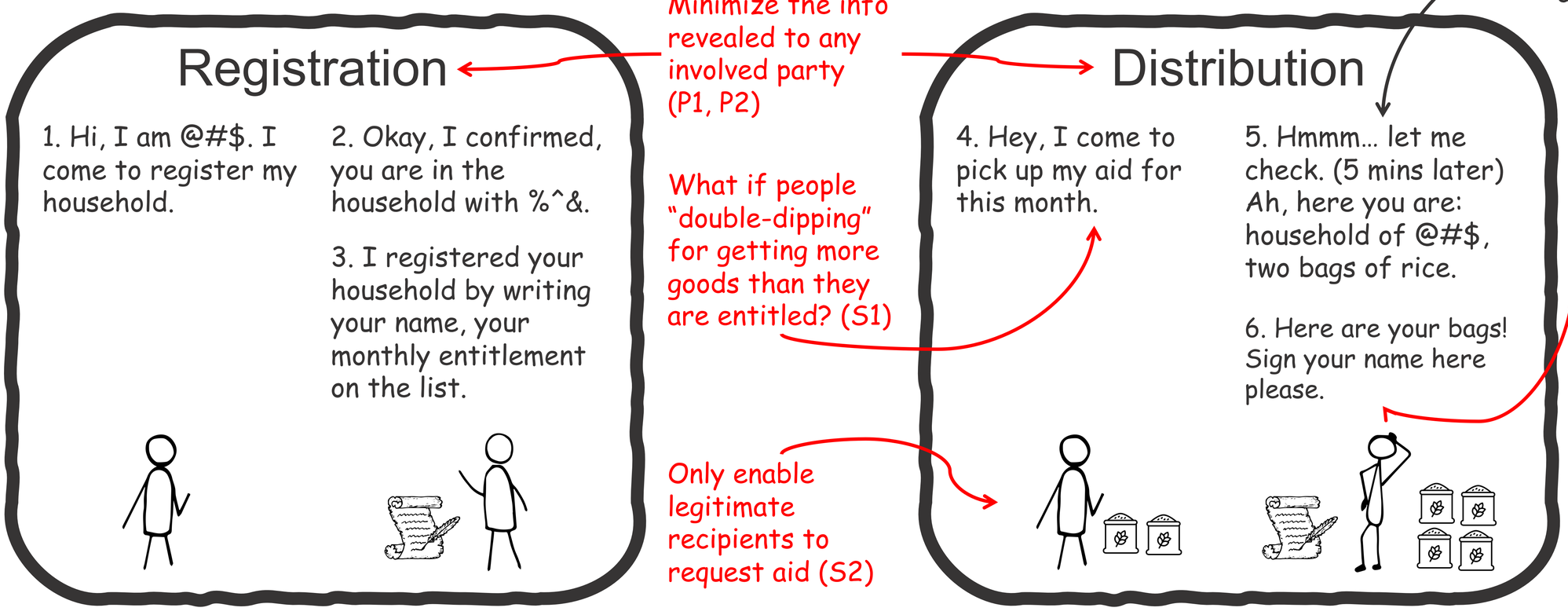
Not Yet Another Digital ID:
Privacy-Preserving Humanitarian Aid Distribution

Aid Distribution & Challenges

Humanitarian organizations distribute physical goods to people in need. Traditional aid-distribution systems are paper-based, which do not scale to large populations. **Considering the special working context, humanitarian organizations must digitalize aid-distribution systems without harm.**

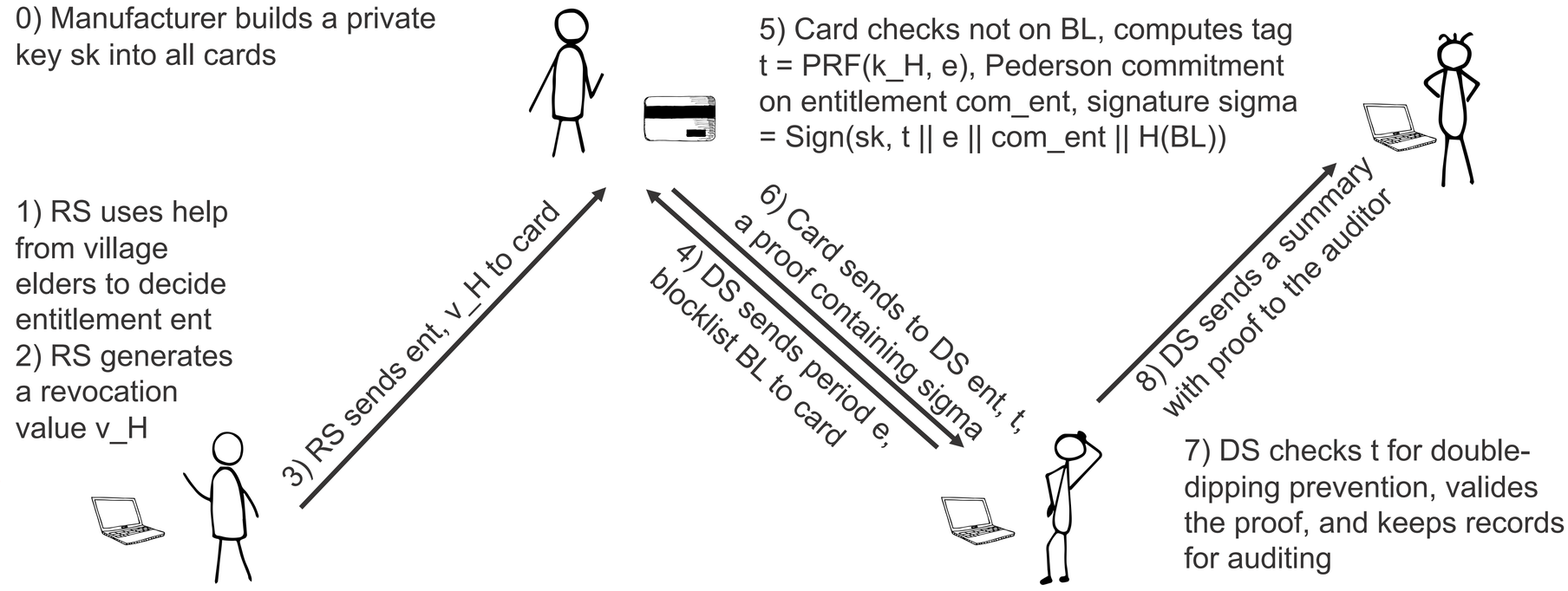


Apart from **S**ecurity&**P**rivacy concerns, there are other **F**unctional and **D**eployment requirements as well:
F1: Distribute per household.
F2: Enable modification.
F3: Periodic distribution.
D1: No stable connectivity.
D3: Robust distribution.
D4: Usability.

A Token-based Design

Main Ideas

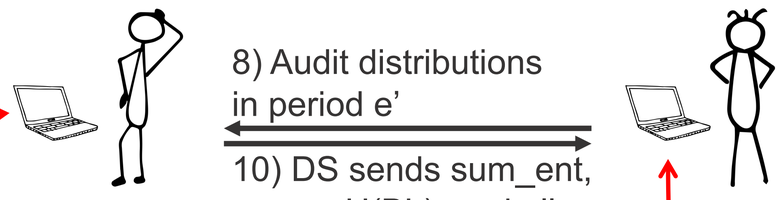
Decentralization by putting personal info into tokens, people can opt out by destorying e.g., the smartcard
Modification via blocklist-based revocation and re-issurance to adpat to changes
Double-dipping prevention by checking tags, the tag is random but unique per household in one distribution period
Trusted Execution Environment* (TEE) to ensure correctness of the computation



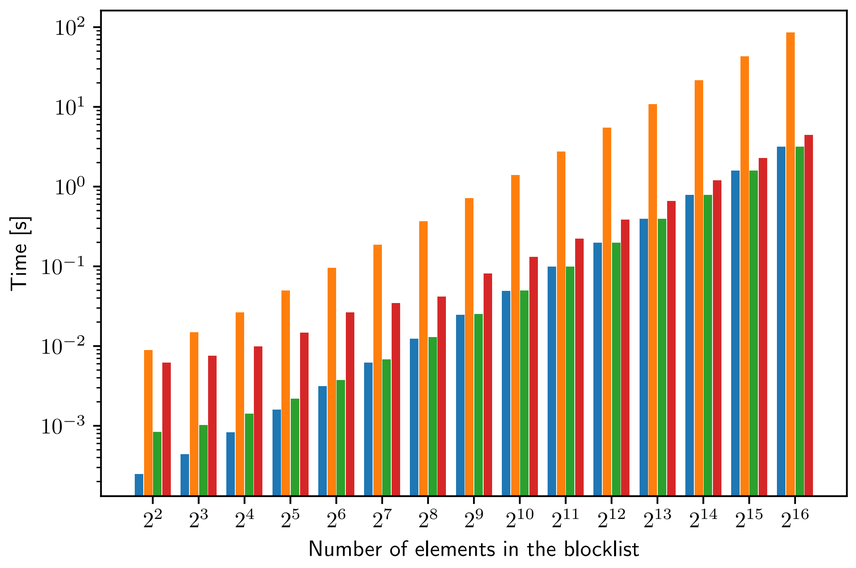
*What if there is no TEE? In some areas where aid distributions happen, smartphones are available at least per household. It is practical to use phones as tokens. However, phones are not tamper-resistant, and hence, cannot be treated as TEE. To make sure the correctness of computation happen in the phone without compromising user privacy, we incorporate **A**ttribute-**B**ased **C**redential (ABC) scheme into the solution. The phone runs ABC with RS to get a credential at registration, then shows the credential with zero-knowledge proofs at distribution. Talk with us for more details!

Towards Accountability & Deployment

Privacy-preserving Auditing for Accountability



Performance Evaluation



Our anaylsis shows the card solution can finish in seconds even with 1024 enties on BL. The figure shows the phone solution also finishes fast enough.

Not Yet Another Digtial ID: Privacy-preserving Humanitarian Aid Distribution. Boya Wang (EPFL), Wouter Lueks (CISPA), Justinas Sukaitis (ICRC), Vincent Graf Narbel (ICRC), Carmela Troncoso (EPFL). To apprear in 2023 IEEE S&P.