Creating approved claims that are universally private

In the DID standard a claim signed by the issuer and the approver can be added to an identity and presented as proof. No one, to the exception of the issuer and the approver, can trace the private version of the claim back to its content. If the claim is properly encoded (e.g. in a merkle tree) it is possible to selectively disclose information and preserve the ability to verify the correctness of the approval.

But if the claim should be kept secret from all, including the approver, we run into a challenge. How to create a proof that even the approver can not recognize. There are two possible solutions:

1. The approver can delegate the signature of the approval to a third party and thus remove the temptation to store the proof for future reference.
2. The issuer create a zero knowledge version of the proof.

Delegating approval

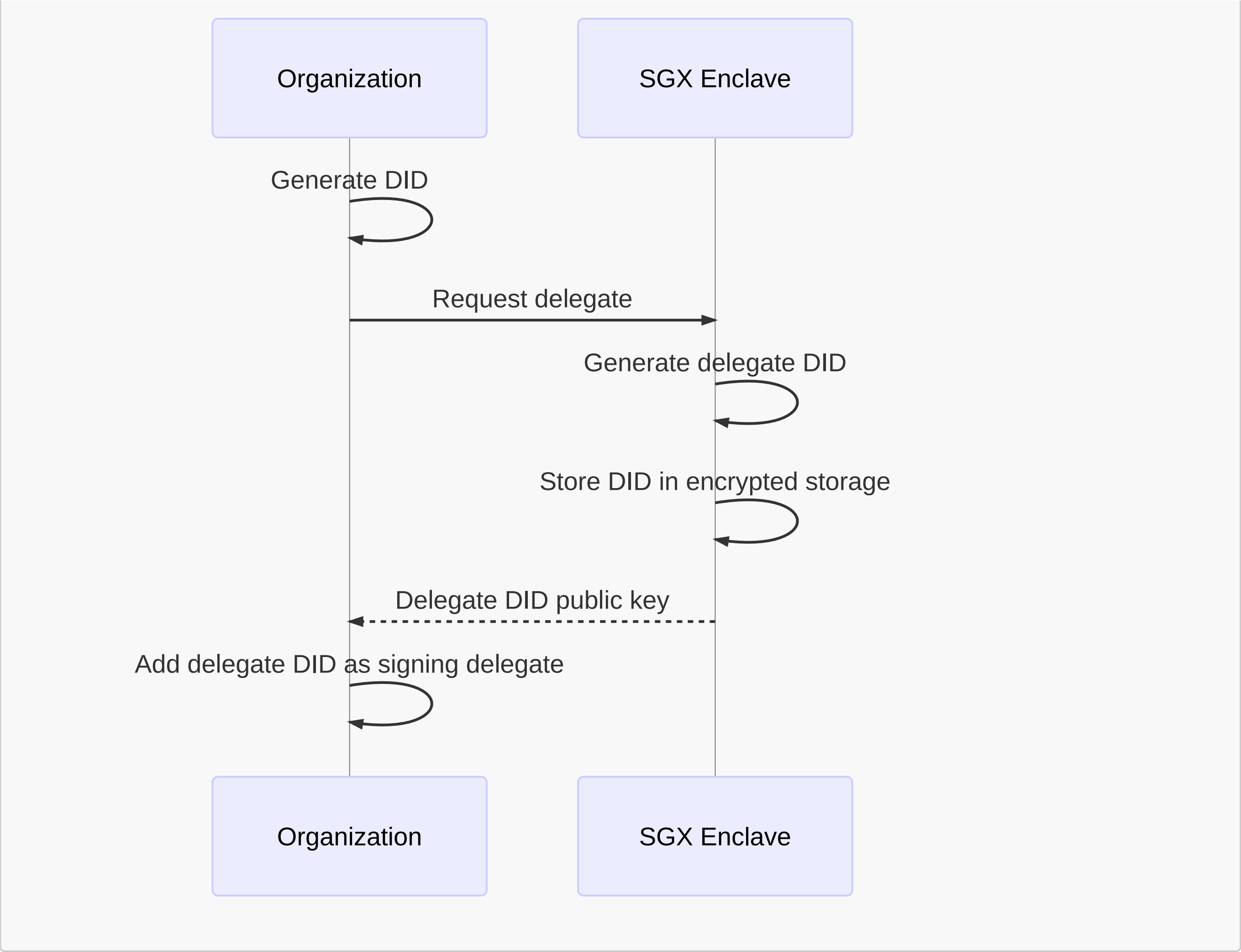
In this document we will concentrate on the first solution: delegating the signature to a trusted third party.

Authorizing the third party to sign on behalf of the `Organization` until the delegation is revoked is a major security risk for the `Organization` which requires a lot of trust. This is why we propose to setup the third party in a secure SGX enclave.

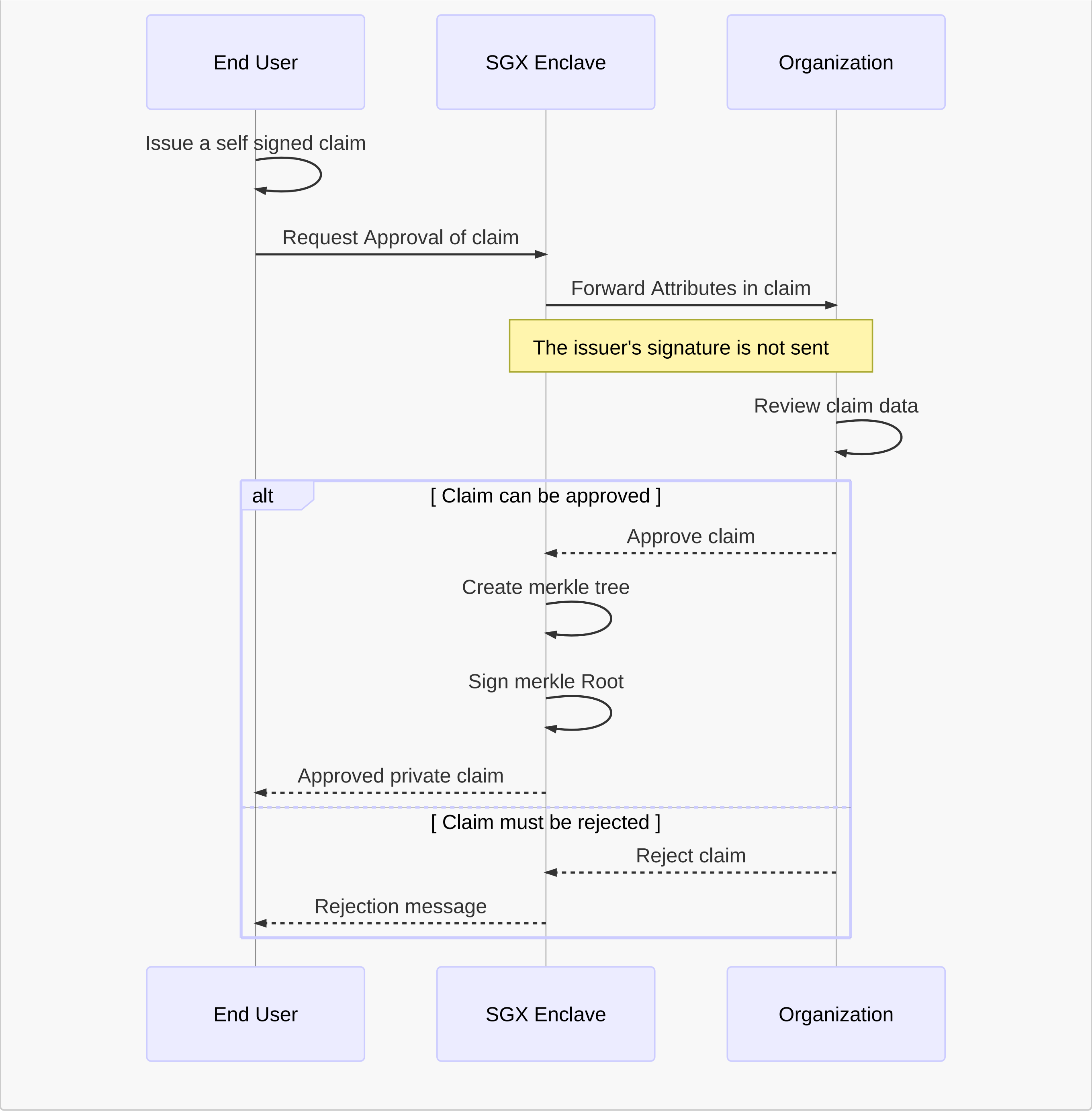
As SGX is certified by Intel, Intel serves as the guarantor and hence the source of trust. But Intel does not have the power to reveal any information, it does only certify that the software deployed to the enclave is correct.

Process

The following diagrams depict the sequence of events which allow to create a fully anonymous private claim.



The trust issue aside, this solution allows us to create an approved claim which the approver will have no knowledge of:



What can be seen in this sequence is that the Organization keeps control over which claim gets approved and which get rejected, as the data is submitted to its review. But because the merkle proof and the signature happen in the SGX Enclave there is no way for the organization to link the end-user and their claim.

The result is that the end-user can present the claim to the organization without giving the organization the ability to recognize them. They can reveal only the parts of the claim which are relevant to the process they want to participate in without revealing any identifying information.

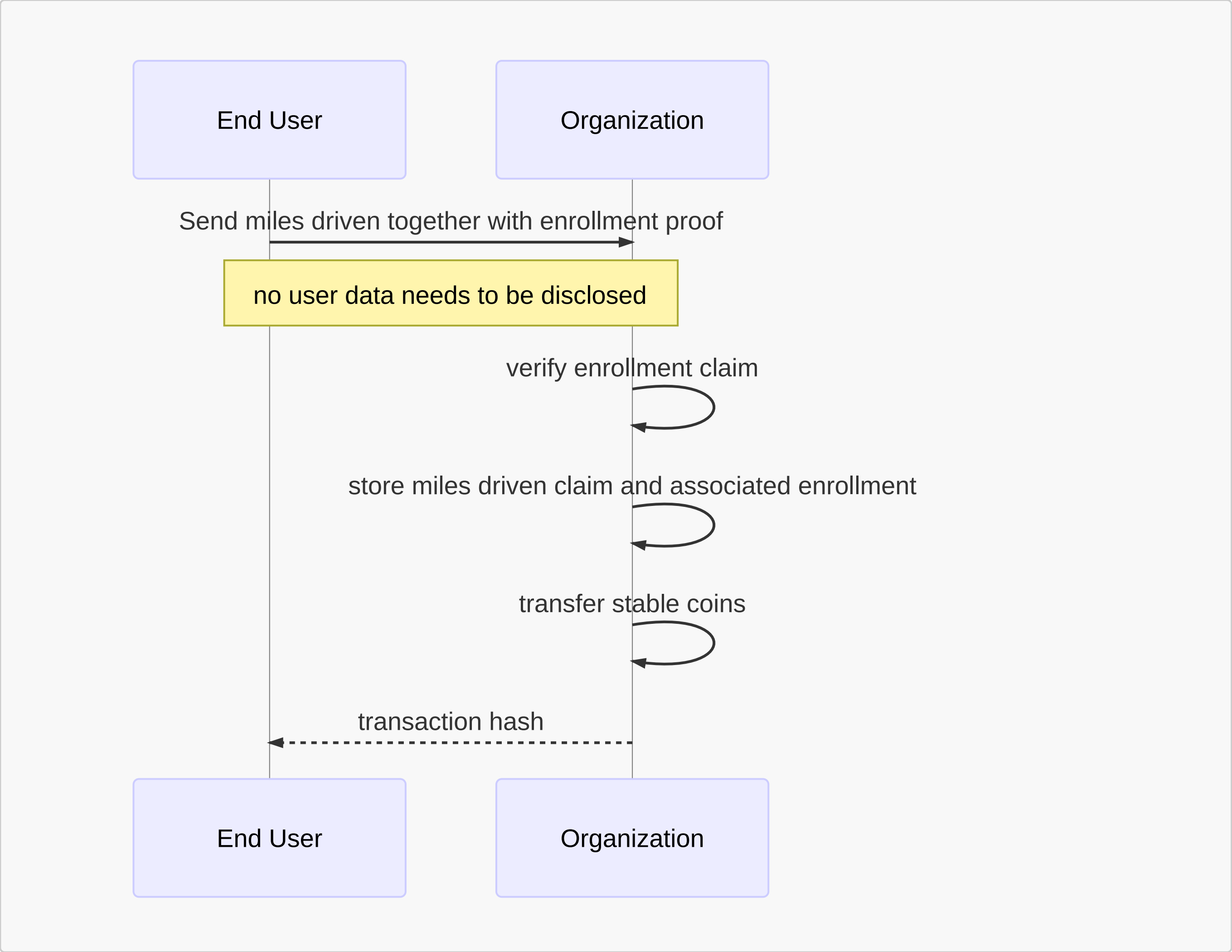
Use Case

The first use case is enrolling EV drivers in a subsidy scheme without knowing who the drivers are but making sure that each driver can only enroll once.

When the driver sends information to claim subsidy they include:

- Proof of charge operation. I.e. CDR with signature from CPO

- Anonymous proof of enrollment in program
- EWC address to transfer the reward to


End User
Organization
Send miles driven together with enrollment proof
no user data needs to be disclosed
verify enrollment claim
store miles driven claim and associated enrollment
transfer stable coins
transaction hash
End User
Organization

The organization can verify that

- Only enrolled users can submit requests
- A request can not be submitted twice in the same time period
    - The session ID from te CDR can be checked
    - The enrollment proof serves as unique identifier for the anonymous user
- It can not discover the user's identity with the EWC address where the tokens are sent to

This process allows for a fully anonymous and secure with no need for a trusted party.