Working with @skeletor-spaceman and team, we run into the issue of how to transfer a private note owned by someone else, assuming you get their authorization, given you cannot “see” it. We’re sharing here the design we arrived at, to gather comments from the community.

While not the specific use case, for the sake of the discussion let’s assume we’re dealing with an order-based swap, where a maker

posts an order to sell 100 tokens A, in exchange for 100 tokens B. We want the taker

who executes the swap to be able to transfer the maker’s note worth 100 As to themselves as they execute the swap.

The code for the swap is simple: it calls transfer_from

on the token A and B contracts to move the funds from one user to the other. Doing the transfer from the taker to the maker is easy, since it’s executed by the taker, who can see their own notes and can produce an authwit for the transfer on the fly.

For enabling the transfer from the maker to the taker, we propose the following flow:

- The maker

creates a note for exactly 100 tokens A. This note’s nullifier secret is embedded as part of the note, instead of being sourced from the user’s secret key (see here for an example). This allows more than a single party to nullify the note. Note that this is the only change we need to do to the Token contract as it stands today to support this flow.

- The maker

creates an authwit to be consumed by the token A contract that allows the swap contract to transfer that note. This means that only the swap contract will be able to trigger the private transfer, and not someone else directly.

- Once a taker

shows up, the maker

sends them off-chain

both the authwit and the note preimage. The taker can verify that both are valid.

- The taker

registers both the authwit and the note in their own PXE, and execute the swap. The taker’s PXE will now be able to “see” the note owned by the maker (since it has the unencrypted note preimage), will be able to trigger a transfer (since it has the authwit), and will be able to nullify it (since the nullifier is embedded within the note as randomness).

Thoughts…?

The information set out herein is for discussion purposes only and does not represent any binding indication or commitment by Aztec Labs and its employees of the structure and/or any potential operation of the Aztec protocol or the protocol roadmap. In particular: (i) nothing in these posts is intended to create any contractual or other form of legal relationship with third parties who engage with such posts (including, without limitation, by submitting a proposal or responding to posts), (ii) by engaging with any post, the relevant persons are consenting to Aztec Labs’ use and publication of such engagement and related information on an open-source basis (and agree that Aztec Labs will not treat such engagement and related information as confidential), and (iii) Aztec Labs is not under any duty to consider any or all engagements, and that consideration of such engagements and any decision to award grants or other rewards for any such engagement is entirely at Aztec Labs’ sole discretion. Please do not rely on any information on this forum for any purpose - the development, release, and timing of any products, features or functionality remains subject to change and is currently entirely hypothetical.