
Q&A

- Q: Do guardians need to be Status users when they are selected?

  A: No, they just need an Ethereum account.

- Q: What happens if the user loses their password? This could be an argument for using a form with questions instead of a password for account recovery?

  A: When a user loses their password they can reconfigure their Social Recovery. There could be periodic sanity checks to remind users to verify that they have their Social Recovery Secret Set and Password. If a user loses access to account and secret set or password, then user is locked out.

- Q: Is it correct to assume that social recovery is compatible with the user also backing up via seed phrase e.g. the user could both backup a seed phrase and set up social recovery? And if this is the case, is it also correct to assume that if such a user performs social recovery they would then also need to backup a new seed phrase (as the old account is subsumed into a new account at the end of the social recovery process)? Or would the seed phrase they had previously written down still work to recover the account *after* the user had performed a social recovery?

  A: This works in parallel with the seed phrase. Seed phrase give access to the “keys”, which might be a key of an account contract. If the Social Recovery is performed, the keys are changed, therefore the User would have to backup the seed phrase for this new key.

- Q to Ricardo: For the password, in your opinion would letting the user re-use their Status password be sufficient, or would the user also need to enter additional information like FullName as mentioned in eip-2429.md ?

  A: Yes, there is no problem in letting the user use the same password as they use in the Status App, because if this password is discovered, an attacker still needs the confirmation from guardians.

- Q to Ricardo: Is it correct to assume that when setting up social recovery, gas is required when the system generates the secret and Recovery URL?

  A: The gas cost is not exactly for generate secret and recover url, but to commit the setup yes.

  Q: so no gas required to setup social recovery, but gas required to execute a social recovery, is this correct? Also is gas required to setup a new contract wallet?

  A: Anytime the social recovery needs to be setup, it needs gas, even the first config, or updates to the config. It's a cheap operation, but needs a transaction that costs ETH.
  This should be the last thing to happen in the process, after user backed up and confirmed they have backed up, then Status sends a transaction setting this up.

- Q to Ricardo: Question about initiating recovery. I assume the user needs to enter a second piece of information in addition to their password to initiate recovery? In the eip-2429.md doc it mentions that a 'Recovery Secret Set URL' needs to be entered. So am I correct in assuming that the user needs to enter a URL in addition to a password to initiate recovery? Is there anything else they need to enter to initiate recovery? Reason I'm asking is that the user will need to remember/record somewhere all information needed to initiate recovery otherwise they will not be able to recover, and as such any design will need to prompt the user keep a note of these things. Thanks!

  A: Yes. The Recovery Secret Set URL is a big string (containing the list of guardians, and other important information) that needs to be saved somewhere else, can be in user "dropbox" or e-mail. This information alone does not allow recovery, it also needs the password.

- Q to Ricardo: Question about how messages are sent to Guardians informing them that they have been requested to perform Guardian actions. Initially I was assuming the message to Guardians would be sent out by whatever communication medium is most convenient (probably email), but then I noticed this comment https://github.com/ethereum/EIPs/pull/2429#issuecomment-569867606 where in step 3. you say "and wallets must check this before notifying someone to help recover (avoids spam);". So are you thinking that a message would be sent to Guardian wallets via the ethereum blockchain informing them that a recovery had been requested? This would of course need explicit support at the Guardian wallet end, but it would enable a better Guardian UX for wallets where it is supported. Also am I correct in assuming that sending such a on chain message would be in addition to the email? And also any ideas where would the gas payment for sending this message could come from, given that a user performing a social recovery is locked out of their wallet and therefor may not have easy access to ETH?

  A: Guardians can verify if the requestor "knows" about the secret. This is important, otherwise this communication channel can be used for SPAM, specially if seamlessly integrated in Status Wallet together with Tribute-to-Talk.

  For guardians outside Status, this don't applies, but we can send the proof anyway.

  No transactions are needed for this stage.

  Transactions are required only for submitting the guardian signatures, and yes, this is a UX problem to yet be solved.

- Q to Ricardo: is the recovery request code the same for all Guardians of a specific user, or does each Guardian have a different recovery request code (for the same user)?

  A: No, the recovery request code is different for each guardian. Actually, this code is actually more than one code, and one is different per guardian and other is the same for all. The one which changes is the merkle leaf of guardian, and the other is a knowledge proof of the secret (used as an automated of proof identity, which enables the guardian help request in the first place).

  Q: In practice, are these two codes concatenated together, or could they be concatenated together?

A: They can be provided in a single URL, but essentially they are separated.

- Q to Ricardo: Is is possible to see which of the selected Guardians have so far responded, and which have not yet responded? If so, this information could be displayed to the User to help them know which of their Guardians they need to chase to complete their recovery.

  A: Yes, the Status App could perform this. When user is recoverying an account contract, they would create a new identity, which would communicate with guardians and get response through Status Network.

- Q from Simon: When a user is in the process of performing an recovery and they are waiting for Guardians to respond… At this point, when Guardians are inactive for a longer period of time and blocking the User from the account recovery, A) would user be able to "stop" the process of recovery and assign new Guardians? B) Would user be able to swap inactive Guardian for another Guardian?

  A from John: Good point, I'll add a variation to this use case to cover this scenario (see variation titled "User cannot get enough Guardians to respond and therefore needs to request recovery from different Guardians") Hopefully it won't often be a problem in practice, because a recovery can be unlocked with only a % of Guardians responding, and we could nudge the user in this direction by having a default value of say "60%" of Guardians required (obviously also depends on the number of Guardians).

- Q to Ricardo re. the usecase titled "Guardian Friend assists with a recovery" how does this draft flow look to you?

  Q from Simon: What if at the point of implementing this feature status wont have video call feature. How can you substitute it?

  A from Ricardo: Simon, Let's say its not a video call, but a "manual identity validation", which could be aided by a video call, in status or any app supporting it.
  John, is possible for the guardian to pay the gas of their validation, but I think that's not what we want. Instead, the guardian will generate a signature and answer back.

  A and another Q from John: If we go for the Guardian generating a signature and answering back, this communication from the Guardian will have to happen via some communication medium. If the Guardians use Status then this communication could be via Whisper, however for Guardians that don't use Status I can't see an obvious frictionless communication channel. Can you see any way around this problem? If the Guardian answers back on chain, then the process might be easier, at the cost of some gas expenditure. What are your thoughts?

  A from Ricardo: Yes, we can allow both cases. But they can answer back the signature via email, or any other media where they were requested this. This signatures are aggregated and submitted once. If is within Status, everything can be integrated and automatic.

- Q to Ricardo: Have you had any thoughts on how the message informing the User that someone has initiated the social recovery process for the User's account will be sent to the User? As we want to preserve the user's right to anonymity we won't know the user's email address or phone number. So I assume the user's wallet will need to watch the Ethereum blockchain to see if a

change to the guardian list has been requested, and if it sees this action happens on the blockchain then the wallet would display a message to the user. Is this correct?

Then if a user has decided to sacrifice some anonymity by using a Guardian Service and has revealed an email address or phone number to the Guardian Service, then the Guardian Service could provide an additional service whereby they watch the blockchain for Guardian list change requests for the wallet and then email or txt the User when they see a Guardian list change request event take place.

A: If someone else asked to change guardian list, then user must change their keys. Changing keys don't need to go through social recovery, the key itself can ask to be replaced.

Yes, we don't send e-mails. Wallet watches a singleton smart contract (shared instance) for events (update of merkle root of guardians), and also smart contract wallet for events (update of recovery system).

- Q to Ricardo: Can the user change their social recovery password without a delay? If someone tries to attack the user by initiating a recovery this means that the social recovery password has been compromised and the user needs to change it asap

  A: Yes, the user can change their password without a delay, but they need to go through the recovery process. Because when a recovery is completed, it allows the reconfiguration of the recovery.

  Unfortunately there is no better way, because it's impossible to tell who is the honest owner of the account being recovered, so this case needs to be settled by the guardians.

- Q from Simon: It’s not clear to me how an attacker can initiate the social recovery process for another User

  A from John: the request could be made by an attacker who has stolen the User's password and recovery URL. A difficult attack in practice, because the Attacker then needs to fool a sufficient number of Guardians into thinking they are the User.

- Q to Ricardo: Am I correct to assume that once the user has changed their keys they then need to setup social recovery again?

  A: Yes, but they would be able to reuse the same setup if they want.

  Q: If they use the exact same social setup, will the recovery URL change or could it remain exactly the same as it was before?

  A: It wouldn't change, if used the same social setup, the same recovery URL is used. The social recovery url contains the list of guardians among other parameters.