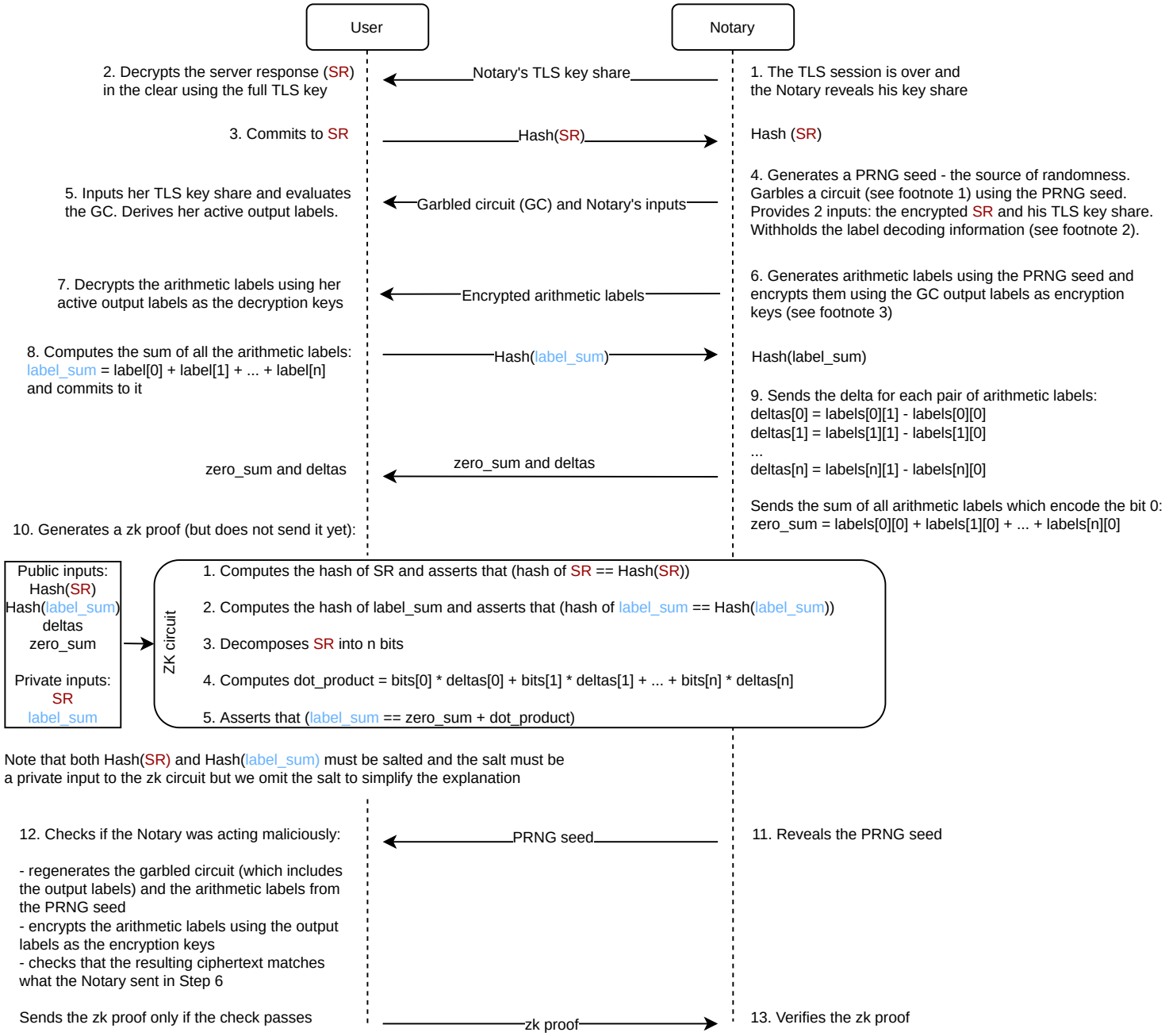
The goal of the AuthDecode protocol is for the User to convince the Notary that a hash of the server response is valid without revealing the actual server response.
At the beginning of the protocol the parties have their shares of the TLS key and the encrypted server response.



Note that both Hash(SR) and Hash(label_sum) must be salted and the salt must be a private input to the zk circuit but we omit the salt to simplify the explanation

Footnote 1:

The decryption circuit takes 3 inputs:
- the ciphertext to decrypt
- the Notary's decryption key share
- the User's decryption key share

The circuit does the following:
- combines the key shares into a full key
- decrypts the ciphertext with the full key
- outputs the plaintext

Footnote 2:

This is a reminder how Yao's garbled circuits work.
The plaintext output of a garbled circuit is encoded by the garbler. Each plaintext output bit has 2 potential encodings: one encodes the bit's value 0, the other encodes the bit's value 1. Each of those encodings is called a "label".
The garbler knows all label pairs for each plaintext output bit.
After evaluating the circuit, the evaluator learns only one label from each pair, called his "active label".
The evaluator cannot learn the plaintext output of the circuit until the garbler sends him the label decoding information.

Footnote 3:

Since the garbled circuit's output labels are correlated by a global XOR delta, we cannot use them directly in the protocol, but we need to break the correlation between each label pair.
One way to do it is for the garbler to pick 2 random labels (since they are random, there is no correlation between them) and to encrypt the first and the second random labels using the first and the second (respectively) circuit's output labels as the encryption keys.
The garbler then sends the encrypted random labels to the evaluator who can only decrypt one random label (since she only has one active output label).

We call those random labels "arithmetic labels" to distinguish them from the circuit's output labels.