# 81.https://stackoverflow.com/questions/73044316/digital-signing-smart-contract-erc721

**T:**Digital Signing Smart Contract ERC721

**Q:**Without using allow lists, is there a way to avoid or reduce bots from minting large numbers of tokens automatically directly via the contract? As in they have to be a real person. Ive heard digital signing helps, but can bots circumvent this? What is the more secure practice here? (I know this might be considered an opinion based question, but I feel this knowledge could be useful to users here)

1 **Answer**

**A1:**As in they have to be a real person. Ive heard digital signing helps, but can bots circumvent this?  
  
You will need to have some sort of prove of liveness for every mint call and then limit them by external offchain checks.  
  
This is a good pattern:  
  
 ● Make people to sign up on a website  
  
 ● Each sign up needs to be confirmed with a mobile phone number, as it is unlikely bot farms will attempt to burn a large number of mobile phone numbers to attack minting  
  
 ● No mobile phone number reuse - only one user per number  
  
 ● Minting needs to happen through a website, each mint() call takes a server-side generated user signature, disallowing signature reuse  
  
 ● mint() verifies from the signature that the user is server-side checked  
  
Whatever is your server-side check (mobile phone number, passport, Facebook profile) may vary.  
  
Here is an example implementation for ICO smart contracts.

**C1:**But all that can be bypassed minting directly from the contract, right?

**C2:**No, the mint() function can check a signature from your server and cannot be bypassed. Please read and study the linked example code.