Digital Signature

15 August 2017 02:41 PM

Requirements:

1. Only you can sign
2. Tied to document
3. Any one can verify

(sk,pk) = generateKeys(keysize) -- Randomized
Sign = sign(sk,msg) -- Randomized
Isvalid = verify(pk,msg,sig) -- Determistic

Cannot forge a signature -- Game played by adversary
Application :

Can sign Hash pointer to secure the entire block chain

Bitcoin uses ECDSA standard
Elliptic Curve Digital Signature Algorithm

Public Key == Identity

To speak on behalf of pk we must know the matching sk.

You control identity because you know sk, if pk looks "random" H(pk) then no body knows who you are.

Decentralized Identity management -- No one in charge. These are called Address in Bit coin Jargon.

Privacy?
Not connected to real world. But observer can connect the activity over time and make inferences.