Anonymous Petition-Signing

Contributors (in reverse alphabetical order):
Ying Tong, Voboda, Kentrell, Janabel

💪🏿 You, a Worker (W)

Want to sign a petition

Want anonymity

Want proof of anonymity

📜 Petition Organizer (PO)

Want signatures

Want proof of employment

Want proof of uniqueness



The Employer (E)

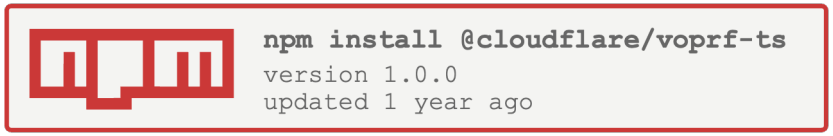
Wants know who signed

Wants to invalidate the petition

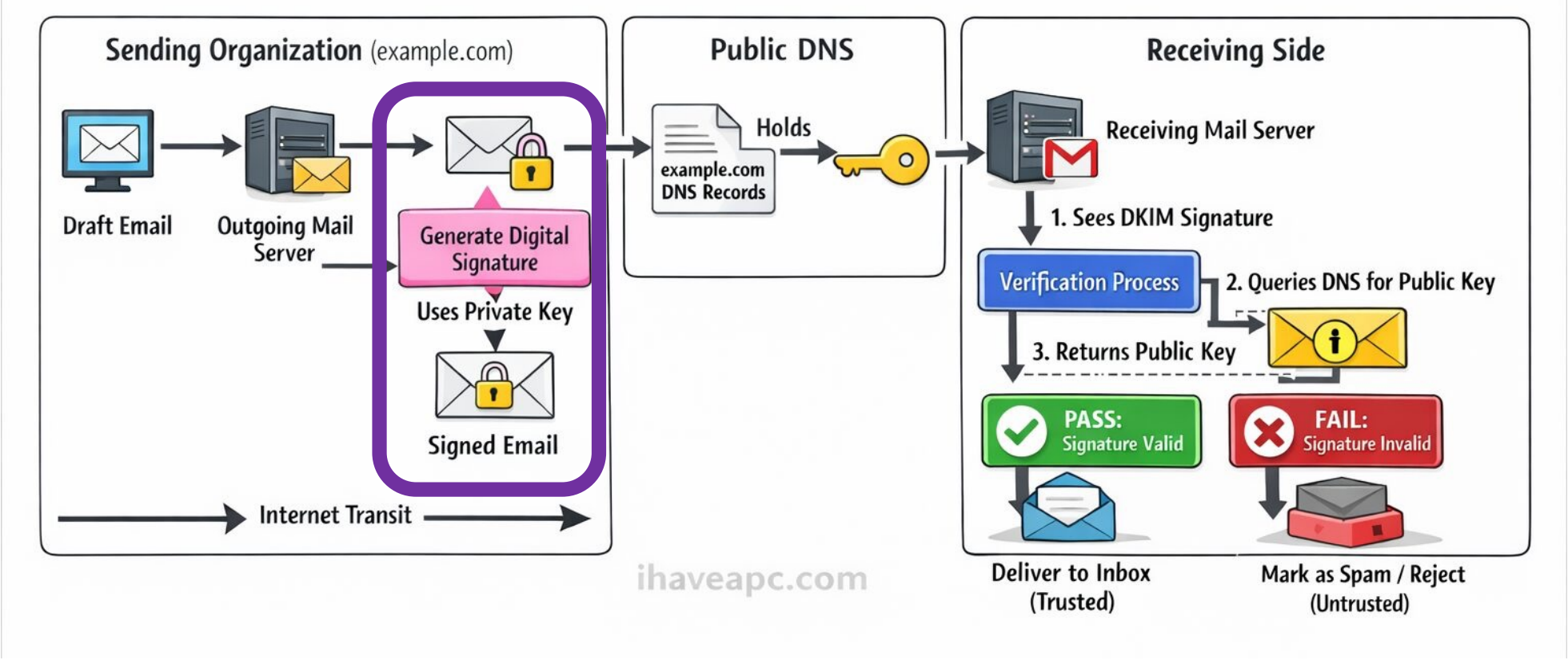
There are three primary design requirements

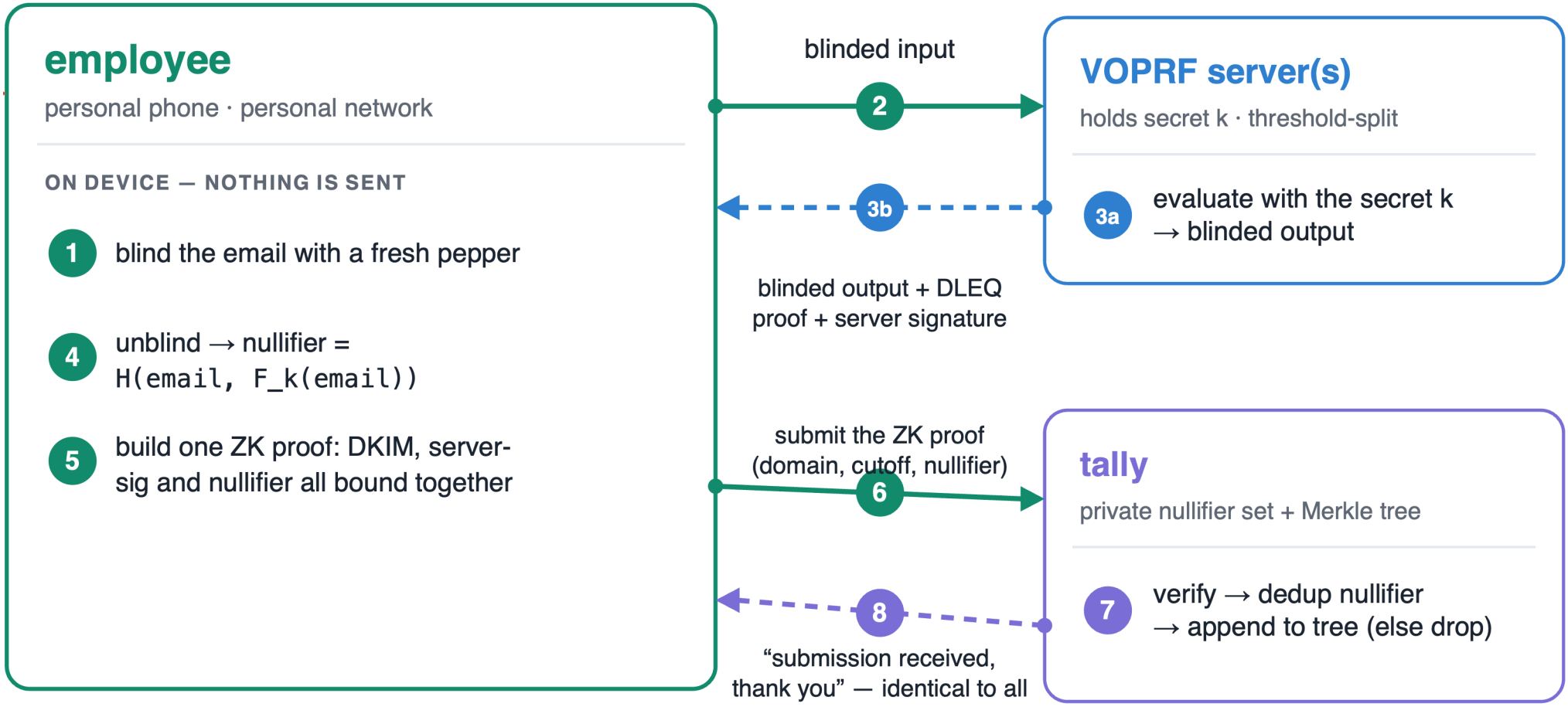
1) Prove that the person signing the petition is an employee
    1) We propose using zk-email (Blueprint SDK)
2) Keep records of petition-signings in a way that prevent double-counting but also doesn't leak that an employee has already signed
    1) We create a nullifier using a Verifiable Oblivious Pseudorandom Function (VOPRF); this prevents employers from doing dictionary attacks
3) Verifiability
    1) A third-party must be able to validate that our count is legitimate





DomainKeys Identified Mail (DKIM)




employee
personal phone · personal network
ON DEVICE — NOTHING IS SENT
1
blind the email with a fresh pepper
4
unblind → nullifier =
H(email, F_k(email))
5
build one ZK proof: DKIM, server-sig and nullifier all bound together
blinded input
2
3b
blinded output + DLEQ proof + server signature
VOPRF server(s)
holds secret k · threshold-split
3a
evaluate with the secret k → blinded output
submit the ZK proof (domain, cutoff, nullifier)
6
8
"submission received, thank you" — identical to all
tally
private nullifier set + Merkle tree
7
verify → dedup nullifier → append to tree (else drop)

After the petition we have to delete “k” from the VOPRF

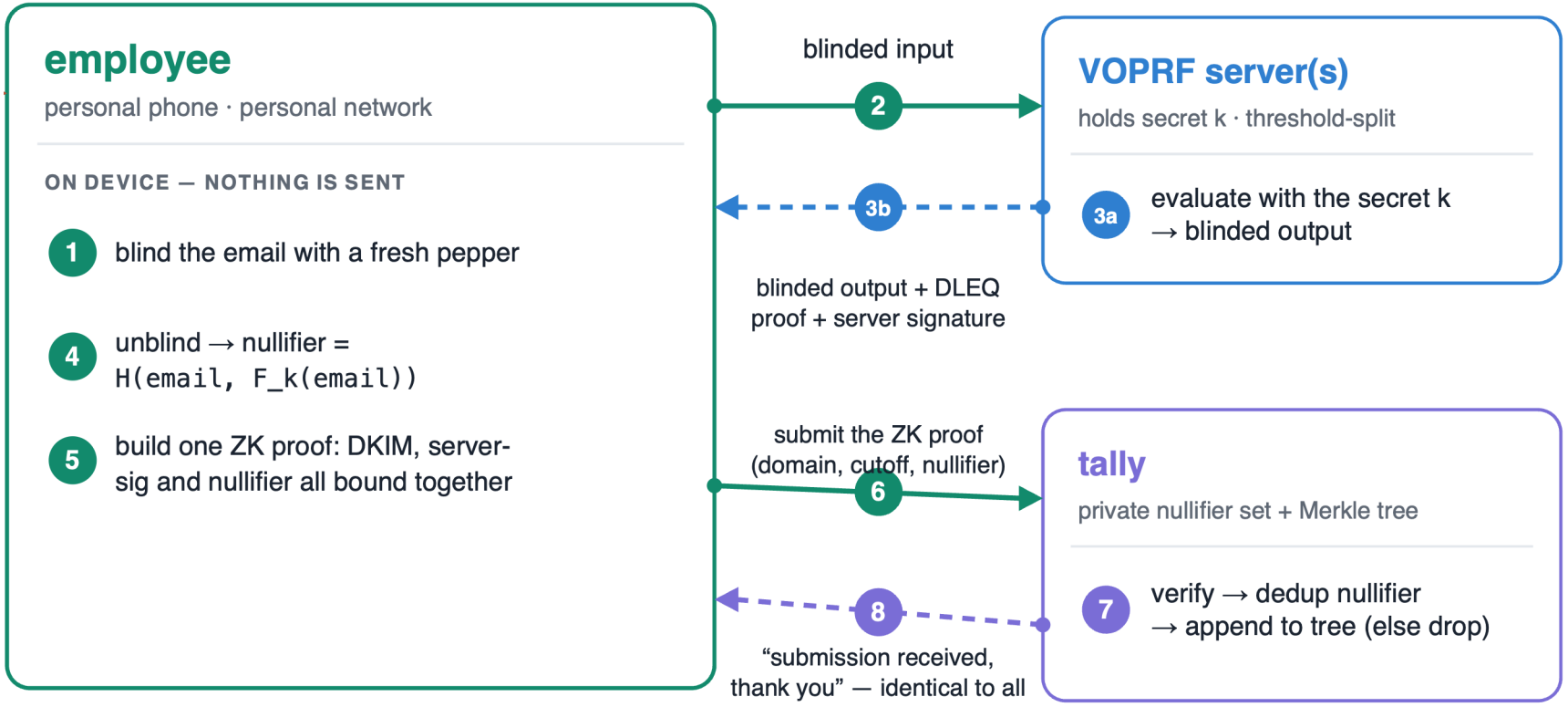
- This prevents anyone from ever de-anonymizing the nullifiers
- We can only publish the Merkle tree and the final tally after the petition is closed to prevent timing attacks
- Need another ZKP to prove that the tally functioned properly

Open challenges/questions

- Big
  - Legal audience and evidentiary standard
  - Getting the email/DKIM information onto a personal device in a non-traceable manner
  - Can we prove that that k has been deleted?
- Tiny
  - Which email class to use as the qualifying artefact
  - Computational cost

Anonymous Petition-Signing

Contributors: Ying Tong, Voboda, Kentrell, Janabel



Thank you for your time. Questions? Suggestions? Praise?