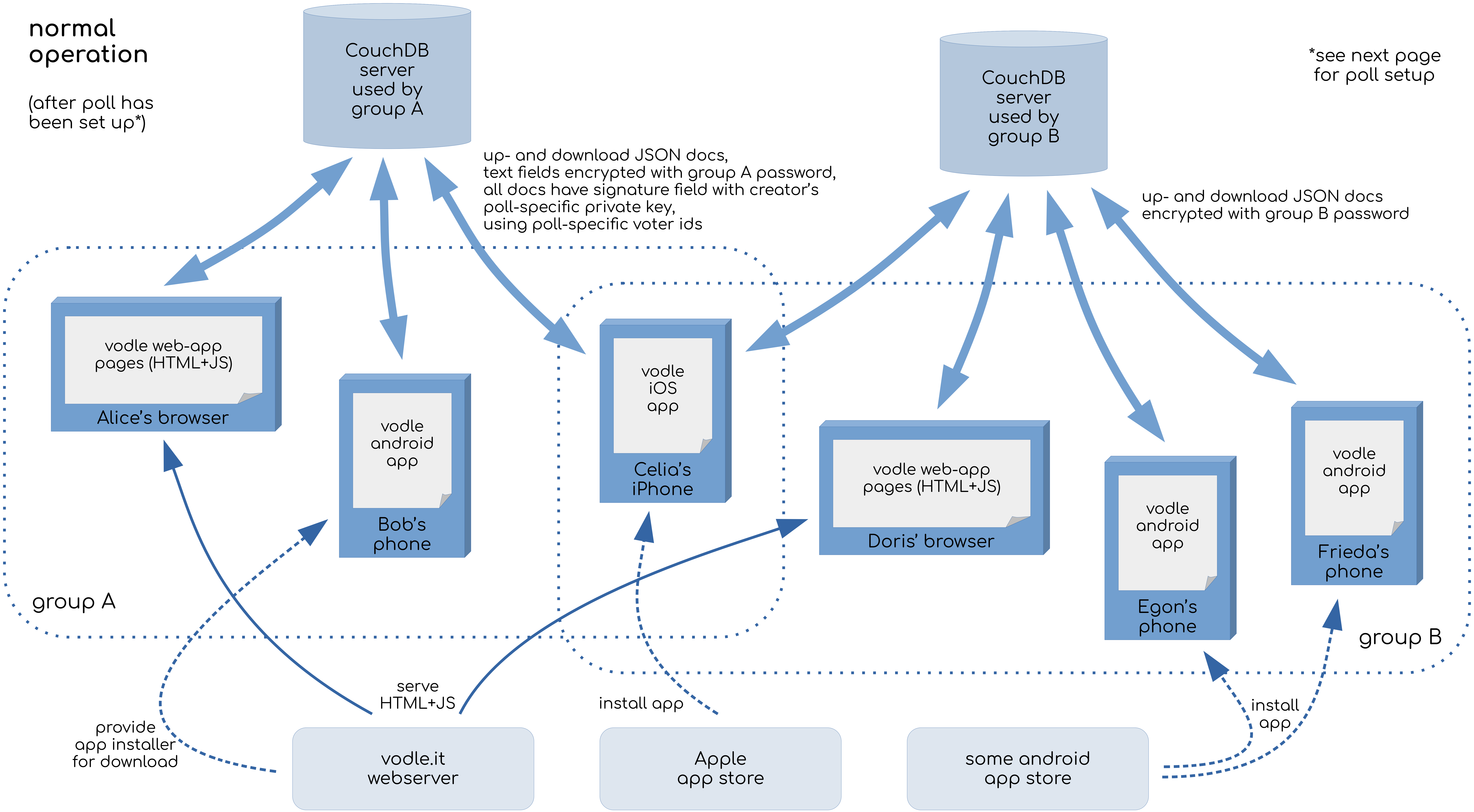
normal operation

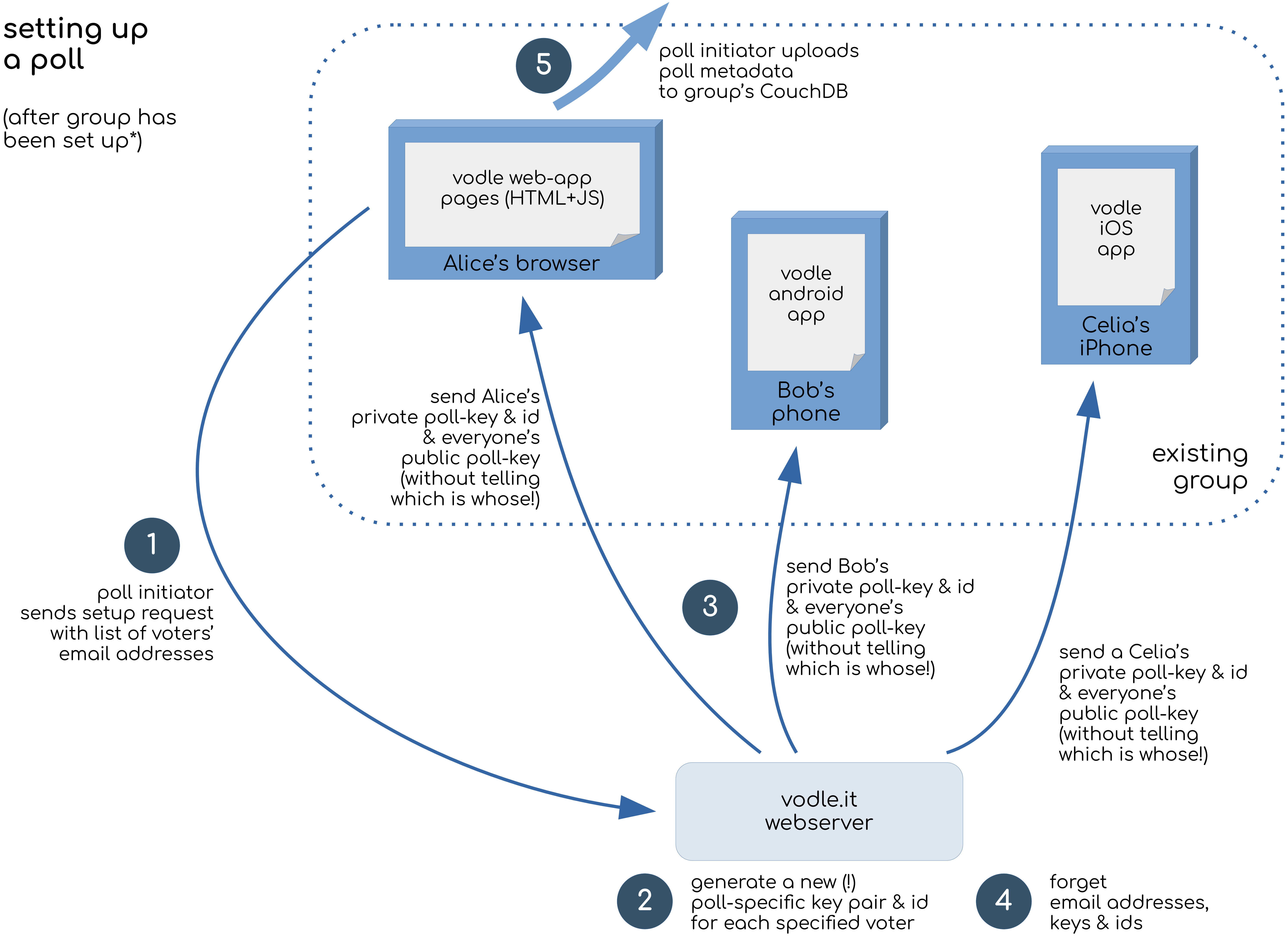
(after poll has been set up*)

*see next page for poll setup


CouchDB server used by group A
CouchDB server used by group B
up- and download JSON docs,
text fields encrypted with group A password,
all docs have signature field with creator’s
poll-specific private key,
using poll-specific voter ids
up- and download JSON docs
encrypted with group B password
vodle web-app pages (HTML+JS)
Alice’s browser
vodle android app
Bob’s phone
vodle iOS app
Celia’s iPhone
vodle web-app pages (HTML+JS)
Doris’ browser
vodle android app
Egon’s phone
vodle android app
Frieda’s phone
group A
group B
serve HTML+JS
install app
provide app installer for download
install app
vodle.it webserver
Apple app store
some android app store

setting up a poll

(after group has been set up*)



1 poll initiator sends setup request with list of voters' email addresses

2 generate a new (!) poll-specific key pair & id for each specified voter

3 send Alice's private poll-key & id & everyone's public poll-key (without telling which is whose!)

send Bob's private poll-key & id & everyone's public poll-key (without telling which is whose!)

send a Celia's private poll-key & id & everyone's public poll-key (without telling which is whose!)

4 forget email addresses, keys & ids

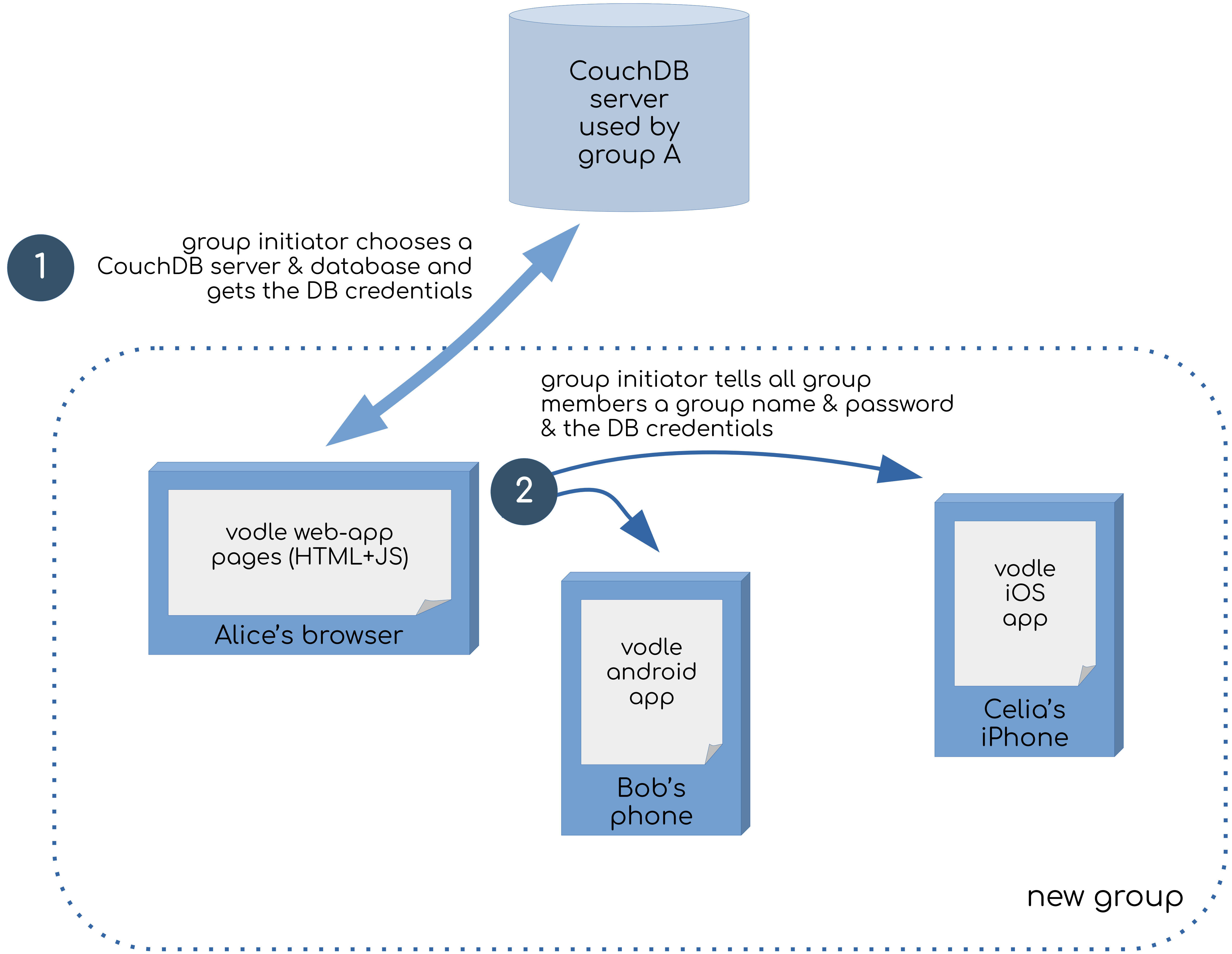
5 poll initiator uploads poll metadata to group's CouchDB

*see next page for group setup

rationale:

- all exchanged data (individual text fields) is encrypted with group password, only group members but no server knows the password.
- all uploaded data document is signed with a poll- and voter-specific private key, all members know the set of corresponding public keys but not which key is whose.
- each poll uses new voter ids
- hence every member can verify data is from some authorized poll voter but not from whom, and cannot correlate data from same voter across polls
- vodle server knows only the identity of the voters but not which DB server they use and cannot access any data
- CouchDB does not know identity of voters or content of data

setting up a group



CouchDB server used by group A

1 group initiator chooses a CouchDB server & database and gets the DB credentials

2 group initiator tells all group members a group name & password & the DB credentials