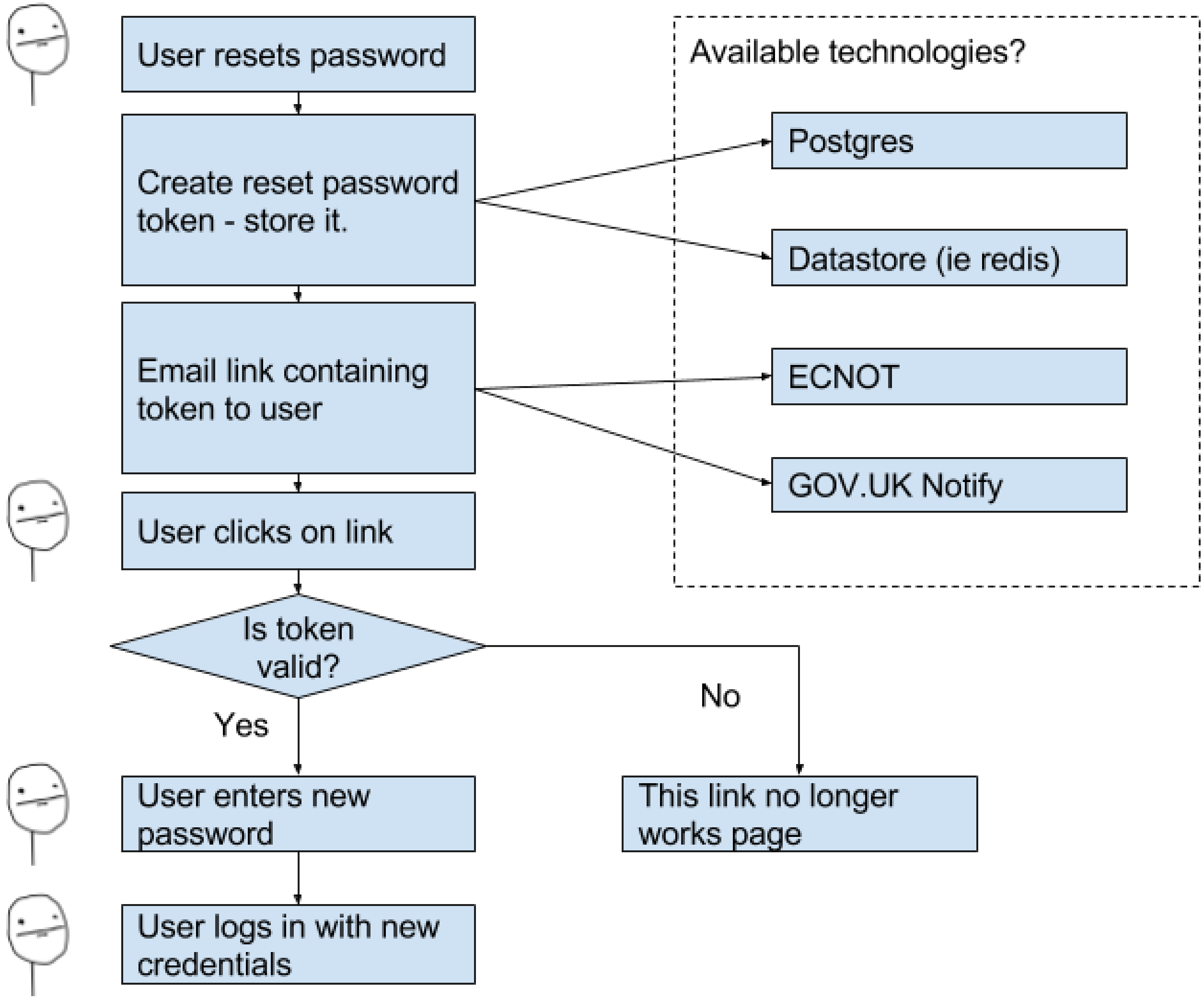
Reset passwords with links.

Our aim is to allow the user to receive a password reset link in an email. Rather than what we do currently which is to send out a temporary password in text via email.

The reason for the change is to improve the security of the password reset link as emails are vulnerable to interception and plaintext password can therefore be gathered.

The following diagram shows the flow of the reset password on the left. On the right shows possible technologies we could use.



Option 1

The path of least resistance, we create a new table in postgres to store the token and a timestamp. We continue using ECNOT to send out the password reset emails.

Pros:

- Setting up a new table is simple and quick.
- We know what to do, less room for mistakes.
- ECNOT changes only needed for a new email template.
- Not introducing new tech that the team has to pick up, more stable

Cons:

- We would have to consider clearing out the postgres table occasionally or have a job to do it.
- A datastore could be faster and lighter than postgres.
- Still linked up with DB2 and current systems such as ECNOT

Option 2

Complete change - let's use a datastore such as Redis or Memcache, and while we are at it, lets use GOV.UK Notify as well.

Pros:

- Datastores could be quicker than using postgres
- We would be decoupling ourselves a bit from current systems/DB2.
- GOV.UK Notify seems simple to use and we already have a working example (albeit not in production)

Cons:

- We no longer have control over the thing that sens out emails - we would have to agree SLA's etc with GOV.UK Notify team.
- We are introducing another technology, and we still don't use elasticsearch that well.
- The likes of Redis is fast, however do we need that for the amount of reset passwords we deal with?

Possible further options

Option 3

Introduce a datastore instead of Postgres.

Cons:

- Overall for the time and effort this wouldn't bring too much overall benefit due to the performance needed from reset password functionality.

Option 4

Start using GOV.UK Notify instead of ECNOT.

Pro:

- A move away from current systems/DB2.
- We wouldn’t have to consider creating or hosting an app to send out emails.

Cons:

- We wouldn’t be in control of emails being sent out, SLA’s would have to be agreed etc.

Preferred option.

For the moment Option1 is the preferred option to ensure delivery. However we should consider moving to Notify at least in the not too distant future.