# Two Known Open Issues

- Provider control over unauthorized apps
- Configuration file
  - How credentials for registration are kept
  - Especially when the user has more than one provider (separate Telephone Numbers)

# Unauthorized Apps

- Providers want control over what apps get access to their infrastructure
- In closed systems (e.g. iOS) this is usually done by signing code, where the program loading system only will load signed code
- We don’t have a closed system so we can’t use that (except on iOS)
- The alternative, widely used is “API Key”

# API Key

- Long string, given to app provider after code is tested
- String is sent encrypted as part of app start up
- Only apps that have been approved will have a valid API Key
- Can be per provider
- Typically sent as a header or xml/json object in an HTTPS transaction
- We could do that, or also send as a SIP header (maybe Call-Info?) in REGISTER
- Is this an acceptable mechanism?

# Configuration file

- Currently envisioned as a local file with sections for each provider
- Currently described as having account userid/password in cleartext
  - That is not acceptable
- Note that all VoIP devices have a local storage of username/password and most store more than one (“multi-line phone”), as well as the other info in the config file.
  - This is not in any way, a new idea
- Lots of ideas have been discussed, including OpenId, SAML, local login that unlocks an encrypted file
- What do we want to do?