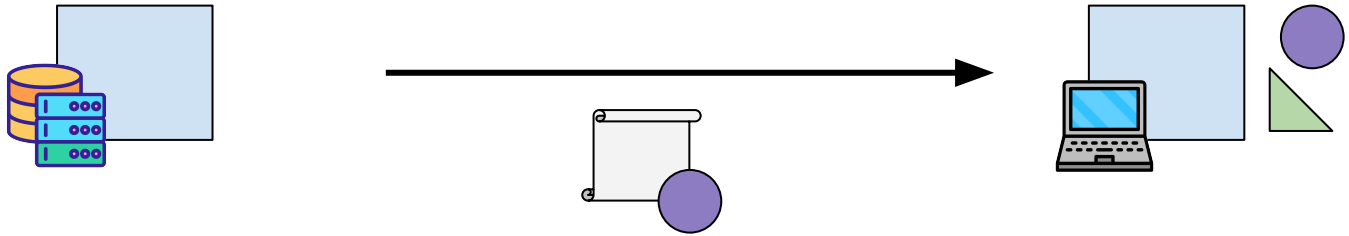
# ACME Profile Sets

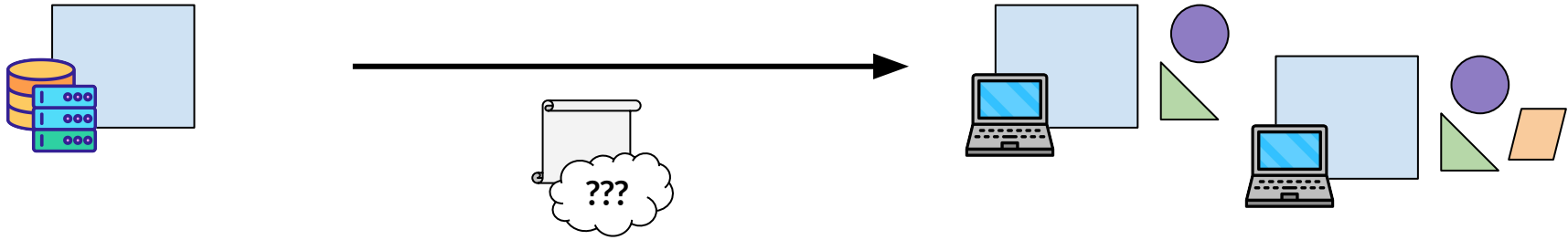
draft-davidben-acme-profile-sets

# Find a CA the client trusts, get a certificate



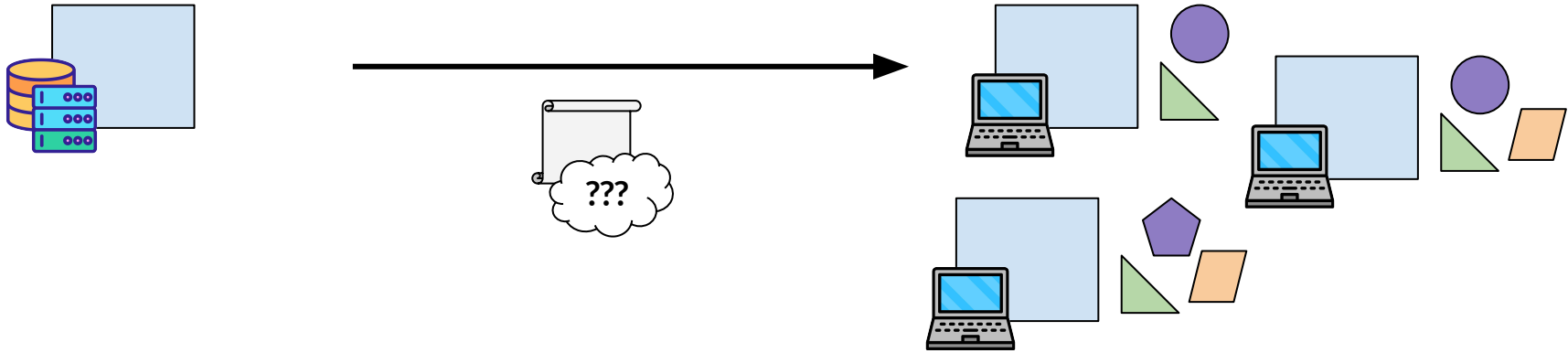
All done, we can go home now

# There is more than one client out there



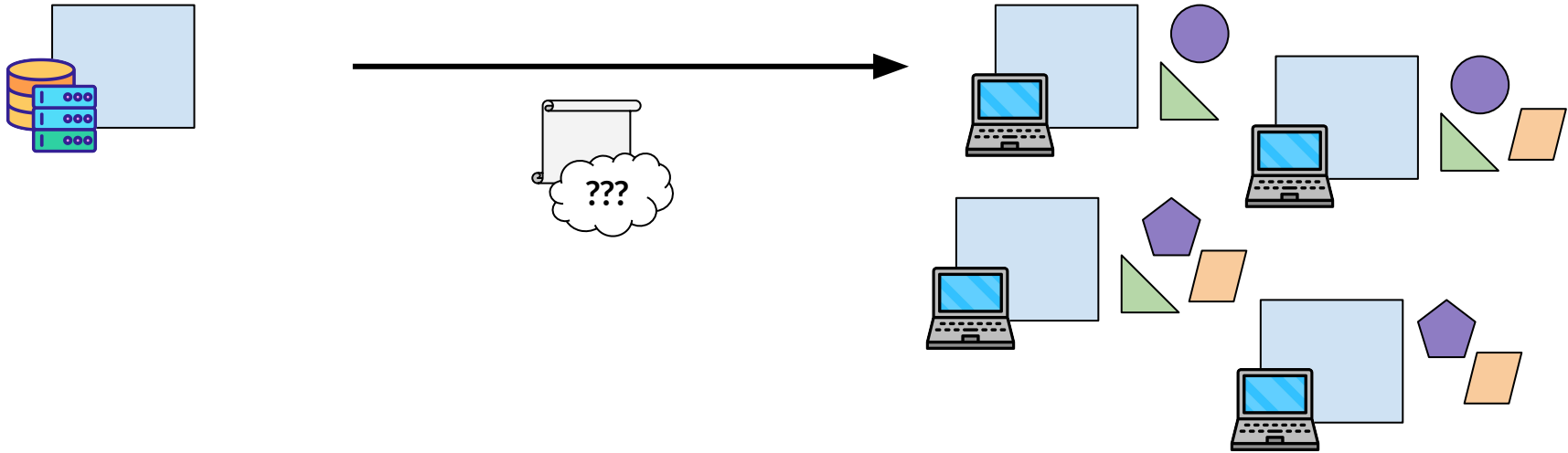

Oh, ECDSA is smaller, would be nice to use it...

# There is more than one client out there.



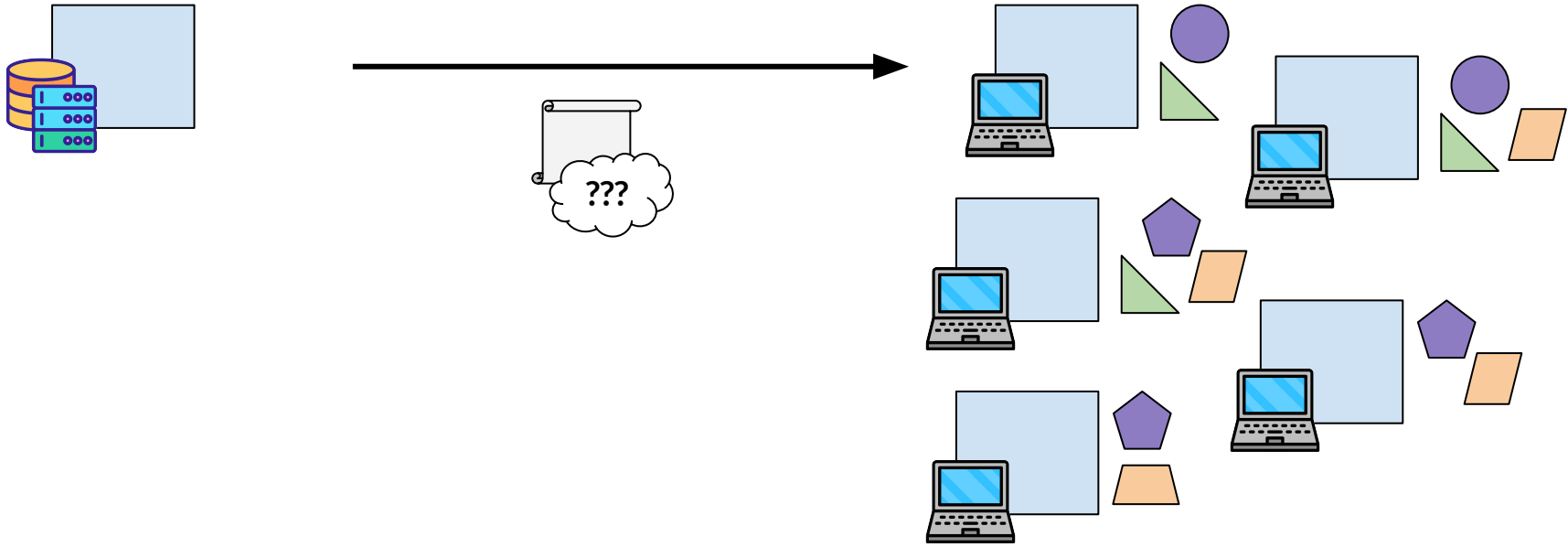

Oops, that key got compromised! Make a new one...

# There is more than one client out there..



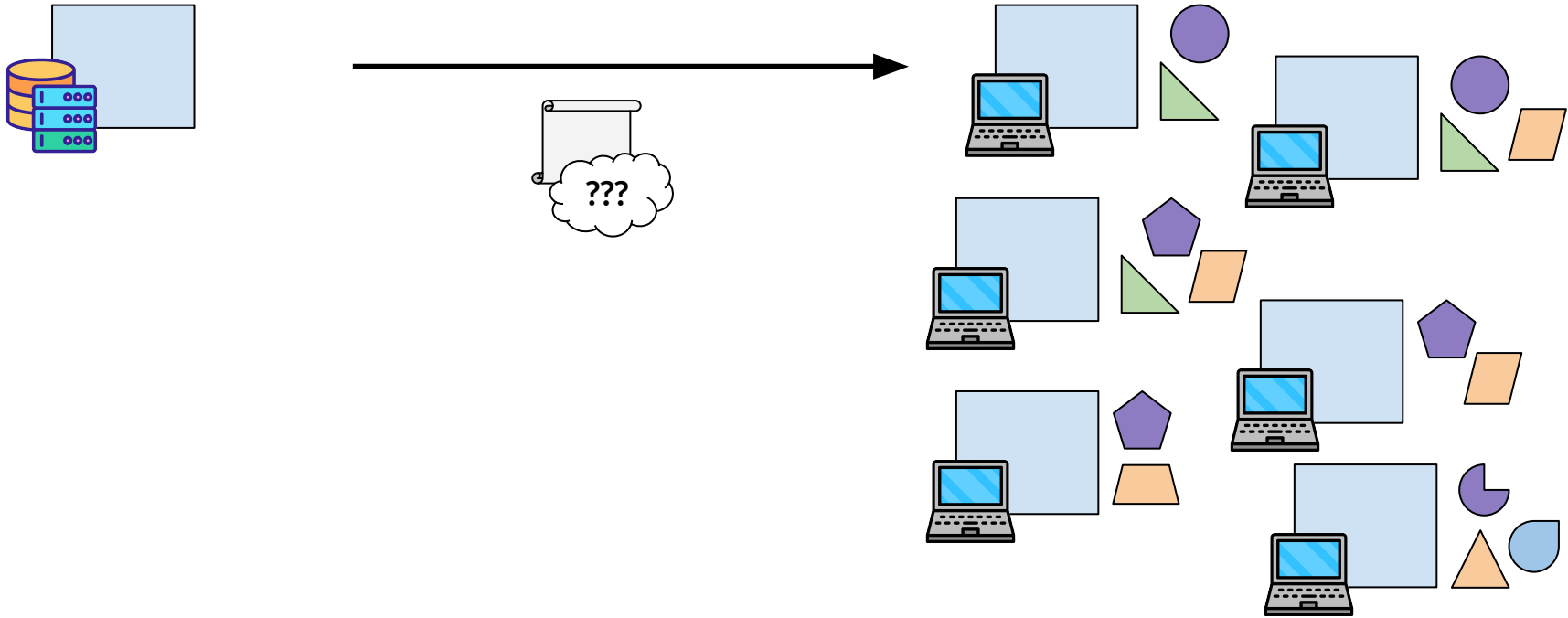

Turns out that CA operator was just untrustworthy...

# There is more than one client out there...



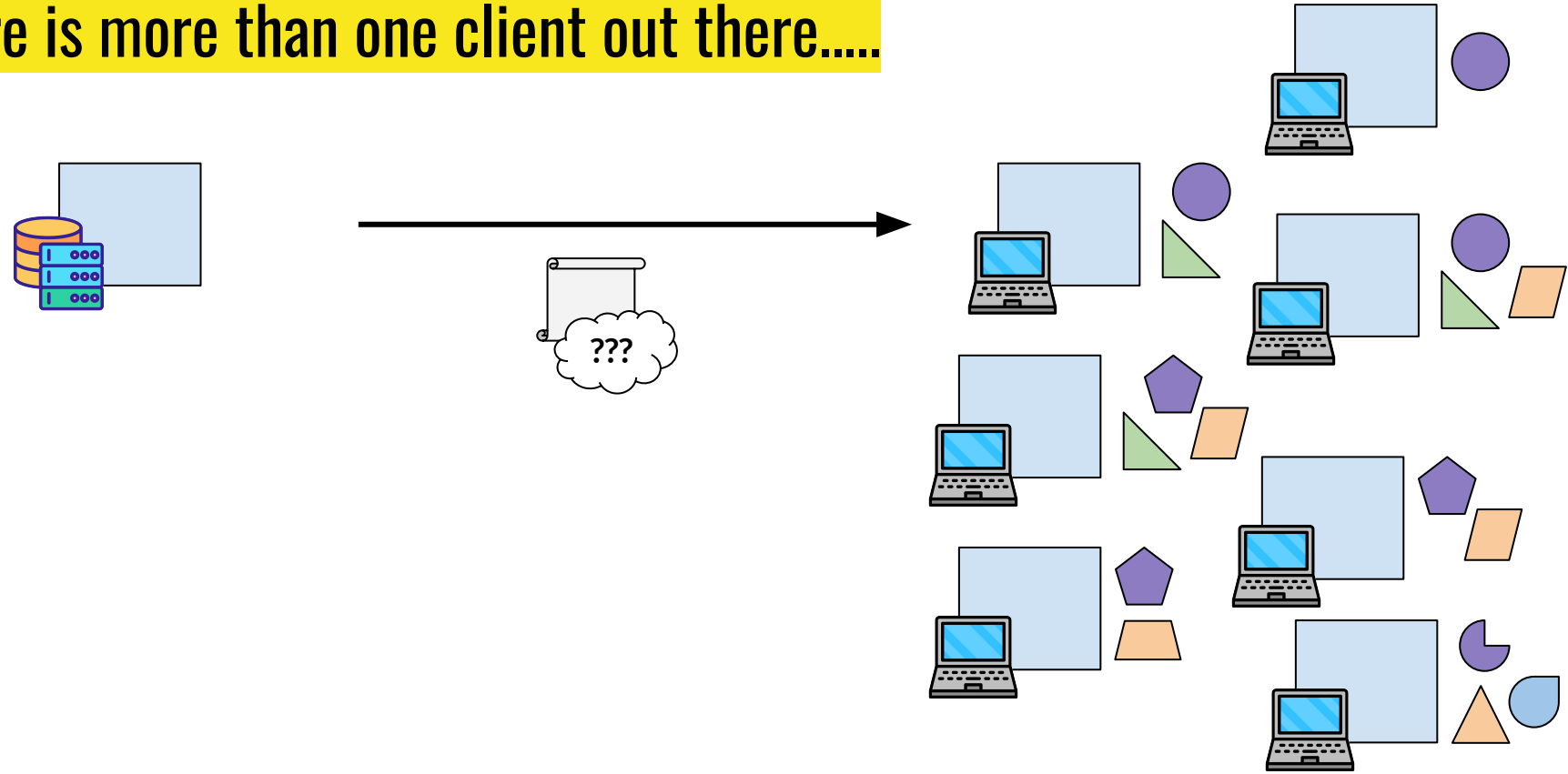

That key's getting kinda old, let's rotate it...

# There is more than one client out there....



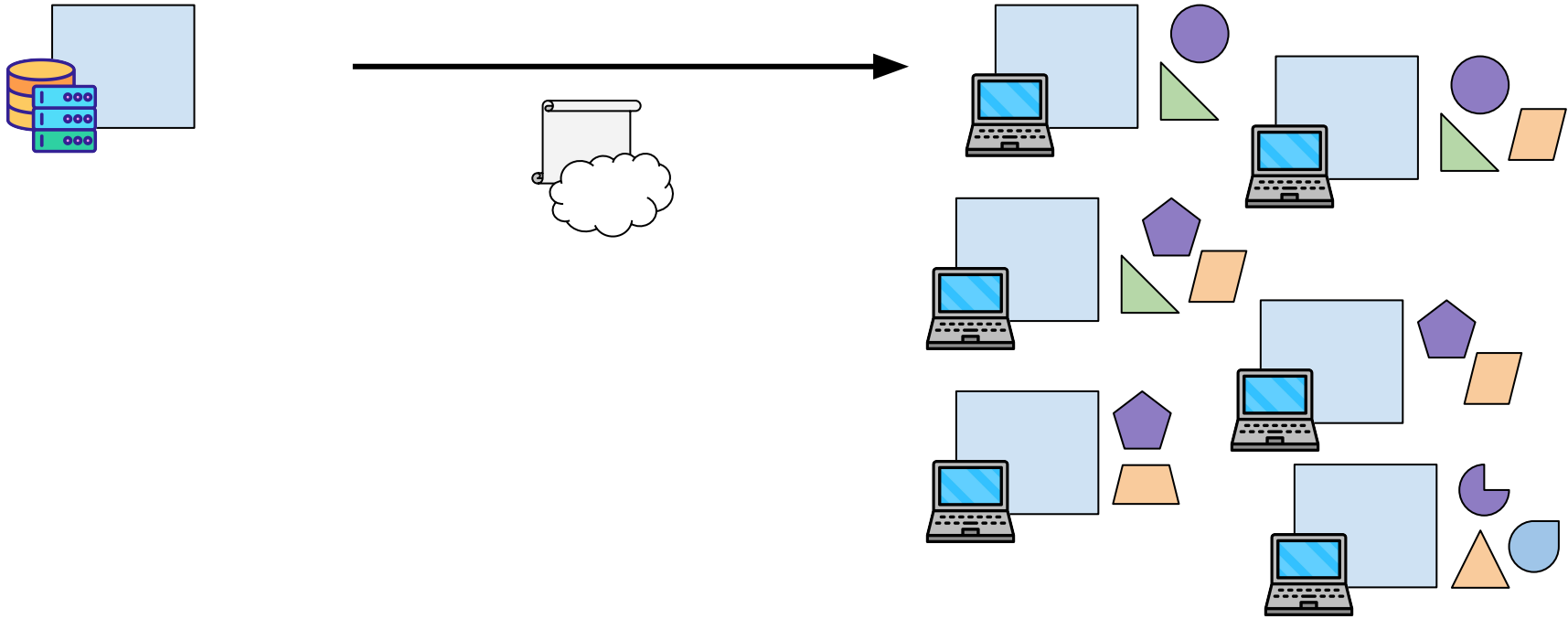

Wait, we need to replace it all with post-quantum...

# There is more than one client out there.....

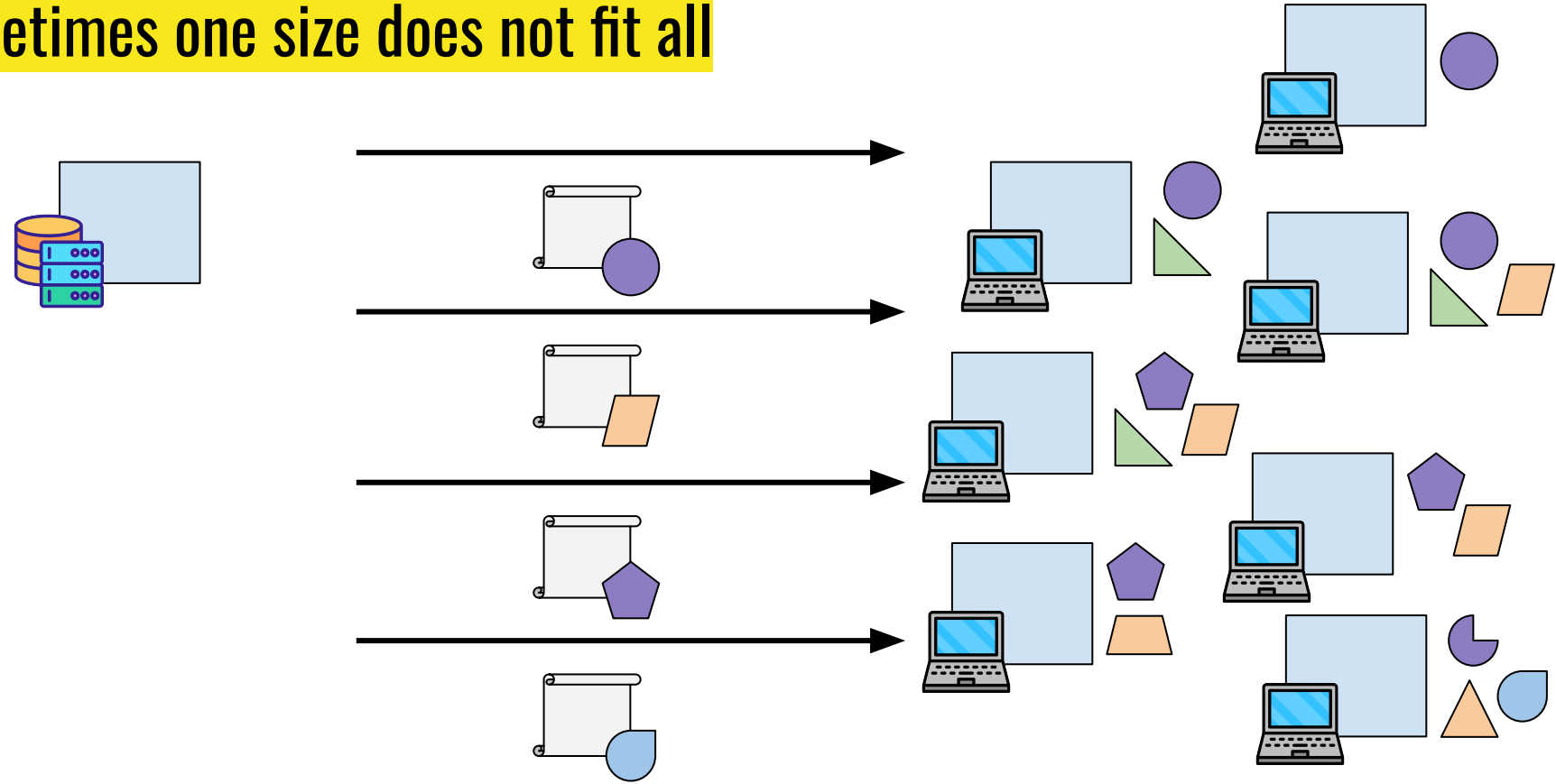



That un-updatable TV only shipped one CA to save on size??!?

# In the limit, old clients last forever



# Sometimes one size does not fit all



# Let the ACME server help

Extend ACME profiles with “profile sets”

Lists of related profiles, defined by the ACME server

May be updated over time as relying parties evolve

ACME clients make orders from individual profiles

Renew as certificates expire or set changes

```
...
"profiles": {
  "profile1":
    "https://example.com/docs/profiles#profile1",
},
"profileSets": {
  "profile1Ext": {
    "description":
      "https://example.com/docs/profiles#profile1Ext",
    "profiles": ["profile1", "profileExt"]
  },
  "profile2": {
    "description":
      "https://example.com/docs/profiles#profile2",
    "profiles": ["profile2a", "profile2b",
                 "profileExt"]
  }
}
...
```

# Why the ACME server?

Many, many more TLS server operators than ACME server operators

ACME server operators are close to the PKI

Closer to how PKI changes

Can help automate PKI transitions

- Help transitions complete more quickly
- Get security benefits more quickly

# Next steps

Other designs?

- Multiple results in one order instead?
- This design avoids changing ACME state machine
- <your favorite JSON spelling here>

Separate draft?

Fold into draft-ietf-acme-profiles?

Thoughts?