## AUTHENTICATION
B Verifies something about A

---

CHOICE (?)

~~CONFIDENTIALITY~~

2 KINDS OF CRED.
  USABLE BY ANYONE
  TIED TO RP

WHITELISTING (WL)
CLAIM MINIMALITY (CM)
~~MUTUAL AUTHE~~
MUTUAL PROOF PARTIC. (MPP)

| ATTRIBUTE (FPI) | | ANTI Phishing | |
|---|---|---|---|
| ATTRIB | 3RD PARTY | FIX AUTH | FIX PHISH |

NON-BROWSING
HTTP SUPPORT

SUPPORT FOR
EXIST. INFRA.

X-APP
CREDENT.
(XAC)

EKR1: Fix ~~Web~~ HTTP Auth
   ~~– Non insane Digest repl.~~
   - Anti-phishing: GUI, Mut. Auth
   - Passwords <u>AND</u> other

EKR2: Cross-site Identity
        Eliot's Dad's Prob

EKR3: Claim & Attribute Transferral

EKR1: Fix HTTP Auth
- Anti-phishing: GUI, Mutual Auth
  → Liase w/ W3C on GUI
    HTML & Links to HTTP
- Passwords <u>AND</u> other
- Layer/Arch. TBD
- Can stand <u>alone</u>
  Would need to coord. w/ EKR2 &
  EKR3
- ~~This requires EKR~~

EKR2: Cross-site identities identifiers
- Eliot's Dad's Problem
    → Too many passwords / use same
- "Raw assertions of identity are easier
  to trust than attrs." – roughly
  Name subordination
- Probably existing tech
    → Maybe Glue work
    → More analysis
- Requires work/sol'n EKR1
    → May require shared mechs.
    → Definitely requires co-ord

# EKR3: Claim & Attribute Transferral

- Existing Claim/Attr. Syntaxes can be used, maybe glue work
- Binds Attr assertions to underlying communic'n
- Not just limited to HTTP