walked through a draft of the new simplified version of SFA
- clarify wording: passwords are chosen by the user and not generated for them
- add complexity rules as a requirement for passwords with 72 character set
  - leave exact definition of the rules open
- look-up secrets are often unlimited in time so there needs to be some extra protection against brute-force attacks
  - if a short non-time-based OTP is exposed to a brute-force attack for an unlimited time it is like cracking a poor password
- TAN and TOTP is not defined in 800-63B, find proper reference
- what is an authentication secret?
  - if authentication is done by sending a challenge that the user needs to encrypt with their key and then return, which one (the
    key or challenge) is the authentication secret?
  - enough to say needs to be cryptographically protected, without defining how
    - otherwise we find ourself defining algorithms which last time led to troubles
- can Table 1 be applied to backup keys and OTPs that are provided to the user in advance?

next call: 23 April 15:30 CEST/8:30 CDT