- 13 profiles – list the specific use cases for each of these (and why these use cases justify a profile for REFEDS RAF, IGTF, and G021/Assam)
- The IGTF profiles linked to research infrastructure risk profile, the RAF to feasibility (can enough IdPs do it, somewhat regardless of the need of the R/E-Infra's that rely on the IGTF profiles)
- RAF: feasible for the IdPs, split with authenticationContextClassReference because of limitations in single-valued SAML
- peer reviewed assessment in IGTF with relying parties that have done their own risk assessment for use of the assurance and bear the burden. External auditors are both too 'expensive' and add limited value (cost outweighs the risk)
- Kantara level 2 requires access to protected databases, and level 1 is too low for the risk at the RPs
- All use cases are global, so global credentials are needed and assurance must have 100% available coverage. Coverage is needed now (and having a notified natl eID scheme is not even required under eIDAS)
- The splitting off of AuthN could allow credential translation for AuthN
  - (through account linking with just the authenticator)
  - still will cover only part of the constituency
- In Kantara, eIDAS, NIST the mix of controls and vectors is specific to a set of use cases that have a different risk profile than the R/e-Infra use cases