SafeCurves

Yoav Nir

IETF 95

Status

- Version -01 submitted in February
  - Updated reference to RFC 7748
  - Textual Changes
- Seems about done.

Signatures?

- draft-irtf-cfrg-eddsa is in its final stages.
- draft-ietf-curdle-pkix-newcurves recently adopted.
    - Assigns OIDs.
- With RFC 7427, that is all we need.
    - We can at most provide one bit of information: pre-hashed or non-pre-hashed version of the algorithm.
    - The answer is, of course, the non-pre-hashed version.
- Should we wait?