Work in Progress

- Posted -00 version in december based in the ECDSA design team work
- I have newer -01 version ready, but not posted
  - Some changes based on the comments from the list
    - Comment about the RSA-PSS and RFC4055
    - Some references
- Need to decide what to do with RSASSA-PSS before continuing
Open issues

- RSASSA-PSS issue
  - Current version cannot really support it
  - One possible change is to include full SubjectPublicKeyInfo object from PKIX, including parameters in front of the signature instead of just OID.
Next Steps?

- Are people interested in this?
- Should this be made WG item?
  - I.e. charter change or not?
  - Or just continue with individual standard track draft?