Roughtime & RFC 8032

- **Roughenough follows RFC 8032 when generating private keys**
  - SHA-512(secret)[:32]
  - Clears highest bit and lowest three bits, sets second highest bit
- **Unclear exactly what other implementations do**
- **An implementation issue, but should probably be included as a MUST in security considerations**

Version downgrade attacks

- **No way to detect tampering with VER in request**
- **No signing of VER in response**
- **Suggested fix**
  - Replace hash of NONC in Merkle tree with hash of entire request
  - Include VER in SREP in server response
  - Include tag in SREP specifying server’s supported versions

Other issues

- **Lack of client checks highlights need for grease**
- **Regression between draft-07 and draft-08**
  - (draft-06) "RoughTime v1 delegation signature--"
  - (draft-07) "RoughTime v1 delegation signature"
  - (draft-08) "RoughTime v1 delegation signature--"
- **Max Merkle tree height should be explicitly specified**
- **Multiple version numbers allowed in requests**
- **Several editorial issues**

Next draft version

- **Multiple changes already up on Github**
  - https://github.com/ietf-wg-ntp/draft-roughtime
- **Issues mentioned are tracked on Github**