Freshness Tokens without Absolute Time

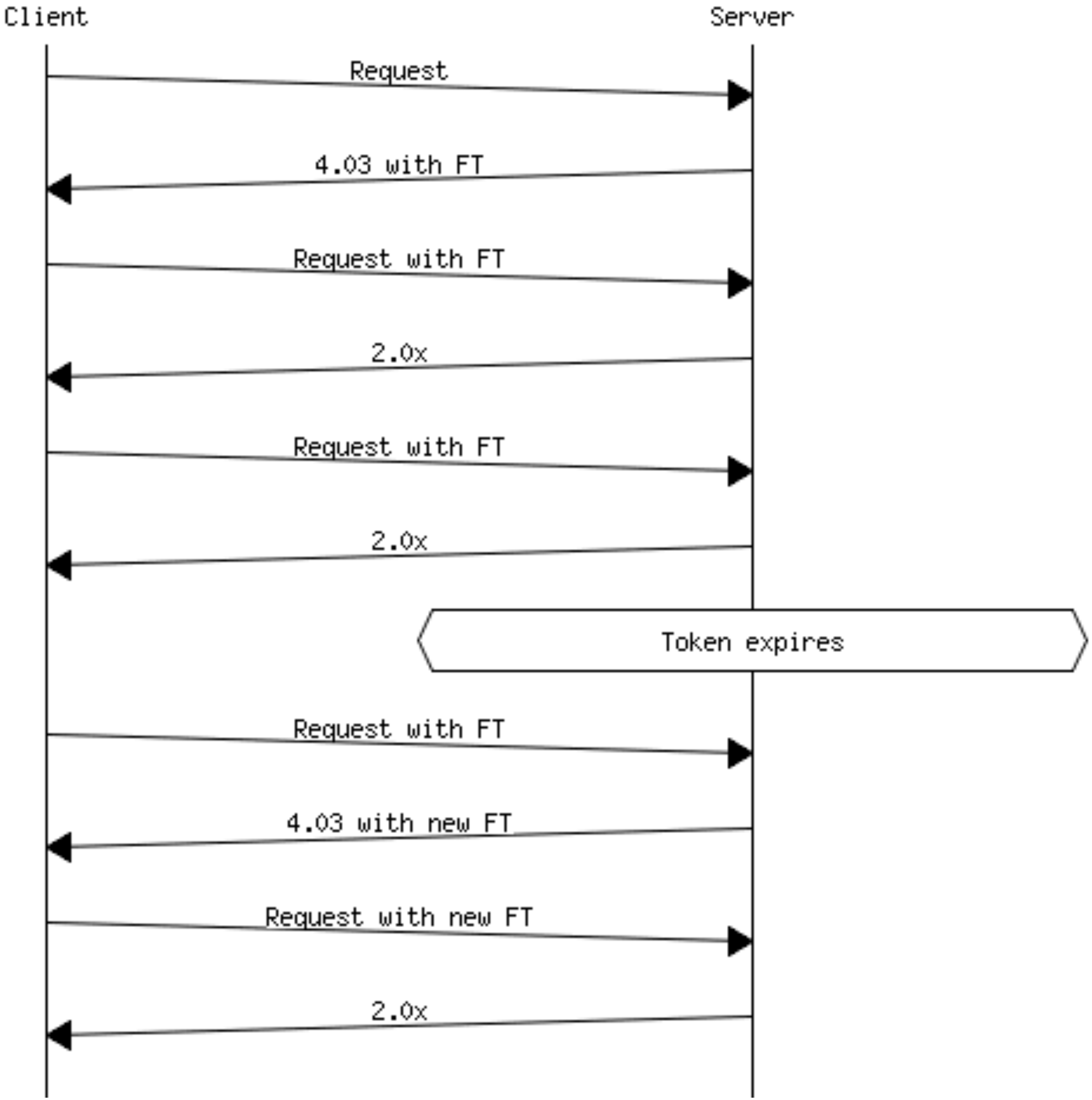
Carsten Bormann 2016-05-30

Using local relative time

- Local: Not synchronized with others;
  not necessarily precise

- Relative: Relative to an event
  (but can be based on absolute)

- Generating Freshness Token:
  Start timer T on local relative time
  (can stop timer T when Freshness Token elapses or is handed back)


Client
Server
Request
4.03 with FT
Request with FT
2.0x
Request with FT
2.0x
Token expires
Request with FT
4.03 with new FT
Request with new FT
2.0x

Freshness Token request

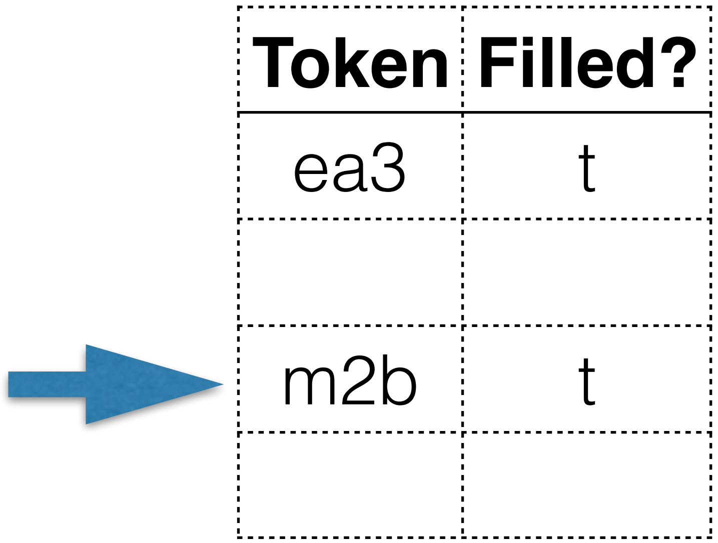
- FT request can be
  - explicit request
  - implicit in 4.03 response
  - implicit in any action on token (“renewal”)
- Potential hand-back with last action on token
  - Server then can stop timer (unless token shared)

Token metadata

- scope?
- lifetime?
  (may be quite inexact, but that is not a problem, if re-request implicit in 4.03)

Multiple clients

- If server has space for N active FTs:
  - keep an array of N FTs
- Hand out used token while $t < t_0 + T/N$
  - advance proportionally in array and fill it in with a new token, otherwise
- Expire one entry (if filled) every T/N, advance
- Note: State sharing ➔ some information disclosure



Token	Filled?
ea3	t
m2b	t

Using event-based time

- Instead of counting timer ticks, count relevant external events
- May not be related to relative time much, but can still be good enough for freshness
- Scale event counter for multi-client case