What if...

Multiple users could retrieve the same content from a cache...

- without the cache being a man-in-the-middle
- without the cache being able to see
- ... or modify the content
- without the cache even knowing* what was acquired

Well

This might be possible

... without any complex models

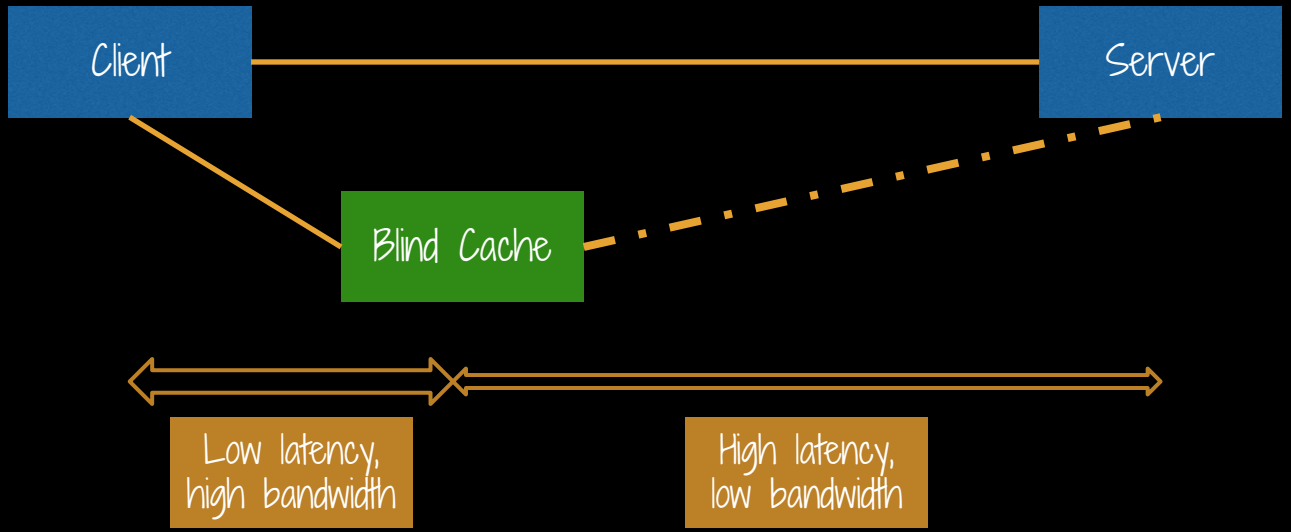
... without breaking TLS

... just simple HTTP (HTTPS really)

... without any fancy crypto

... maybe even without signatures

The blind-cache architecture



Principles/Goals

The cache is off-path

→ clients aren't exposed to issues with the cache

The server chooses what is cached

→ sensitive content isn't cached

Resources keep their origin

→ no impact on the web security model

How it works

The entity body is provided by the cache

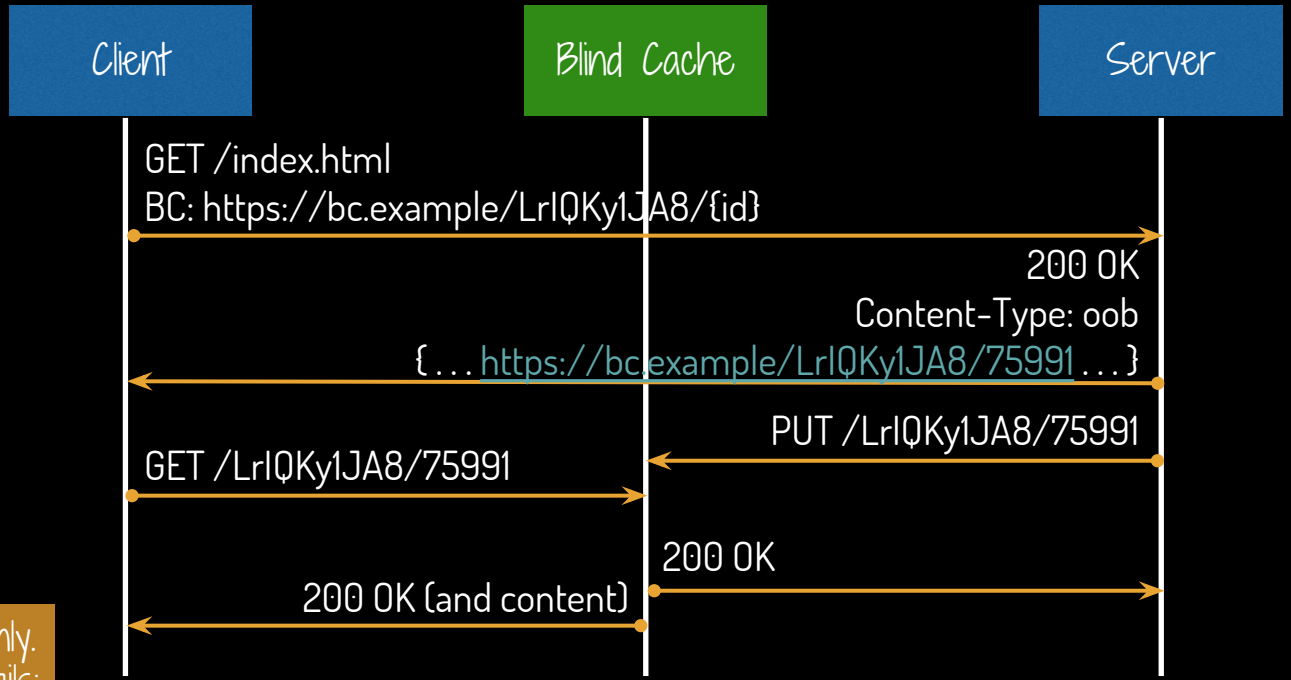
The entity body is encrypted and authenticated

- → MAC and encryption keys are provided by the origin
- → Metadata (entity headers) are provided by the origin

The client requests the entity body only from the cache

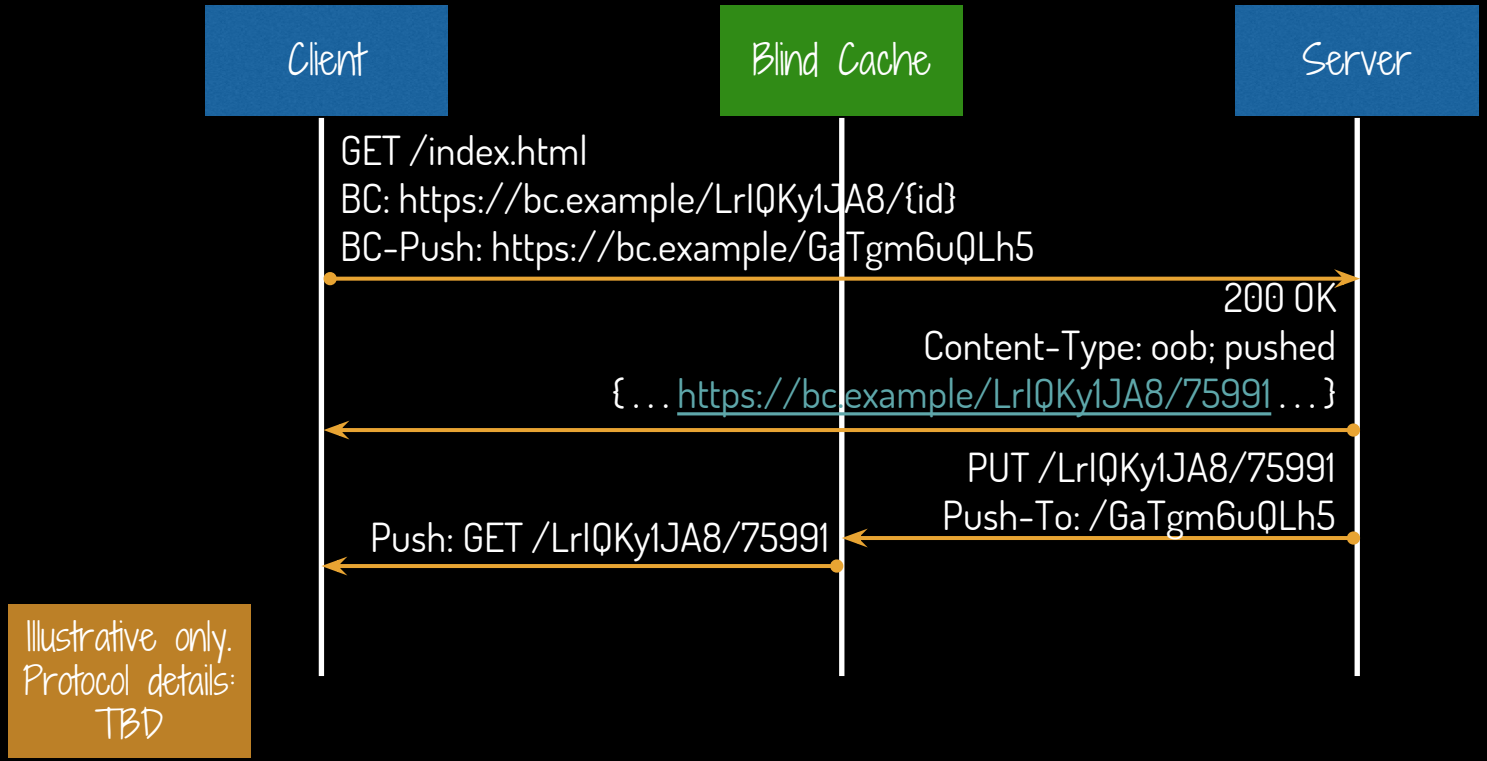
The entity body identity can be unlinked from the real content

Basic flow



Illustrative only. Protocol details: TBD

Using server push



Questions

Does it improve performance? … for whom?

The cache gains some information about resources…

… some resource linkage, sizes, sometimes content …

… shared caching doesn't work otherwise; is that OK?

How do we manage DoS mitigation?

How do we manage content integrity? SRI-like or signatures?

What are the implications for deployment?