

Web Push + HTTP/2

IETF 91

Proposal overview

Architecture

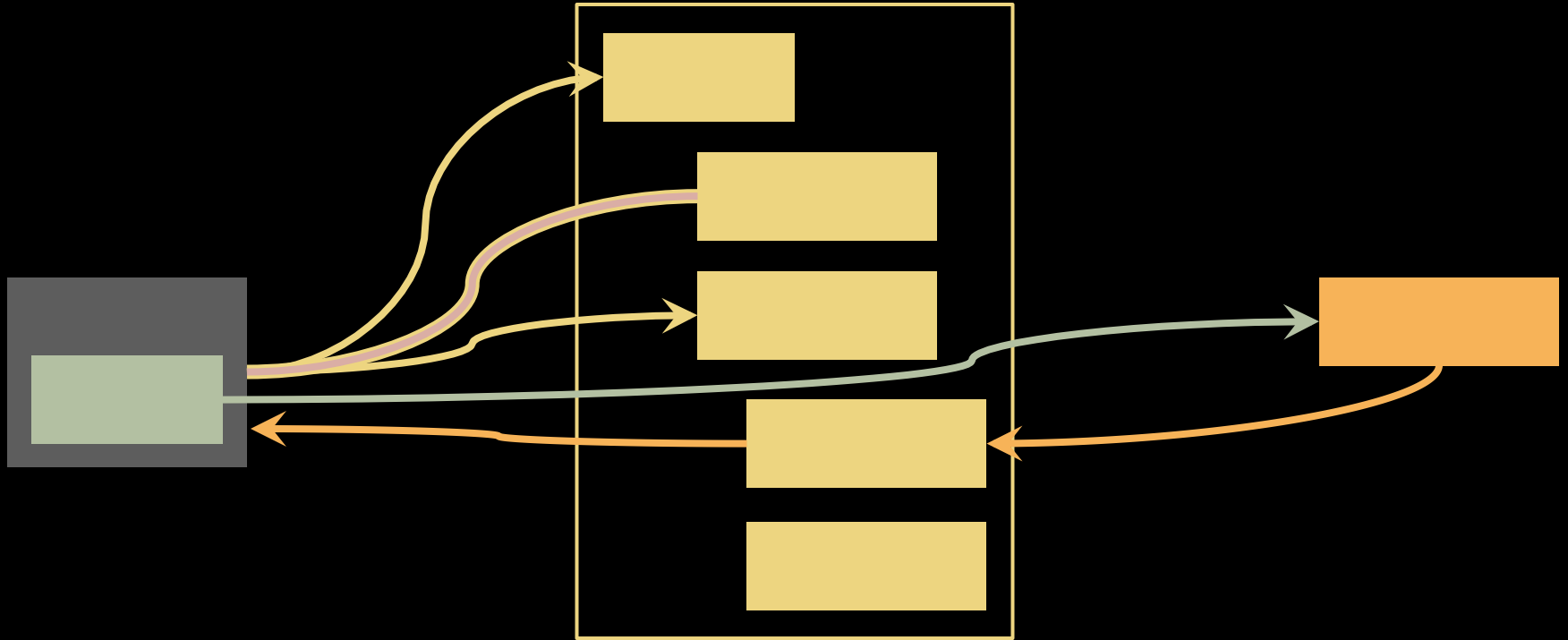
Names

Protocol Pieces

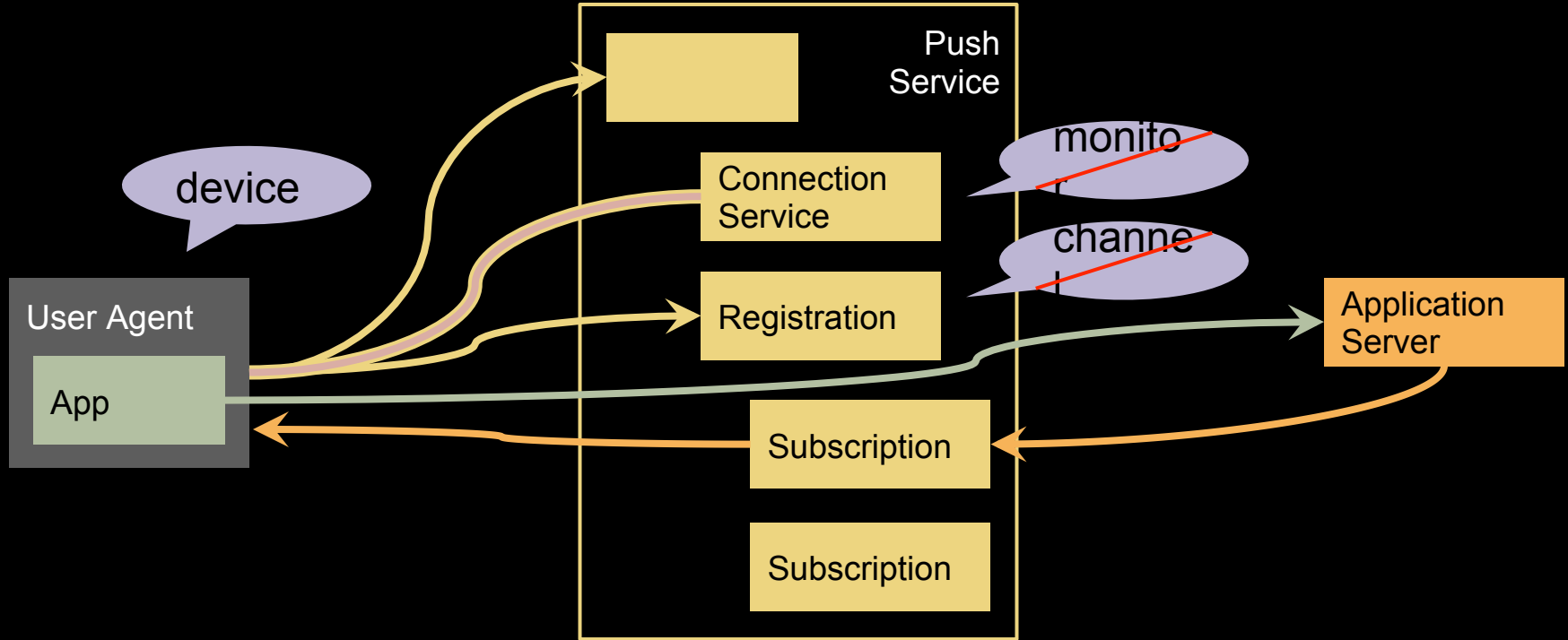
Forcing end-to-end

Authentication

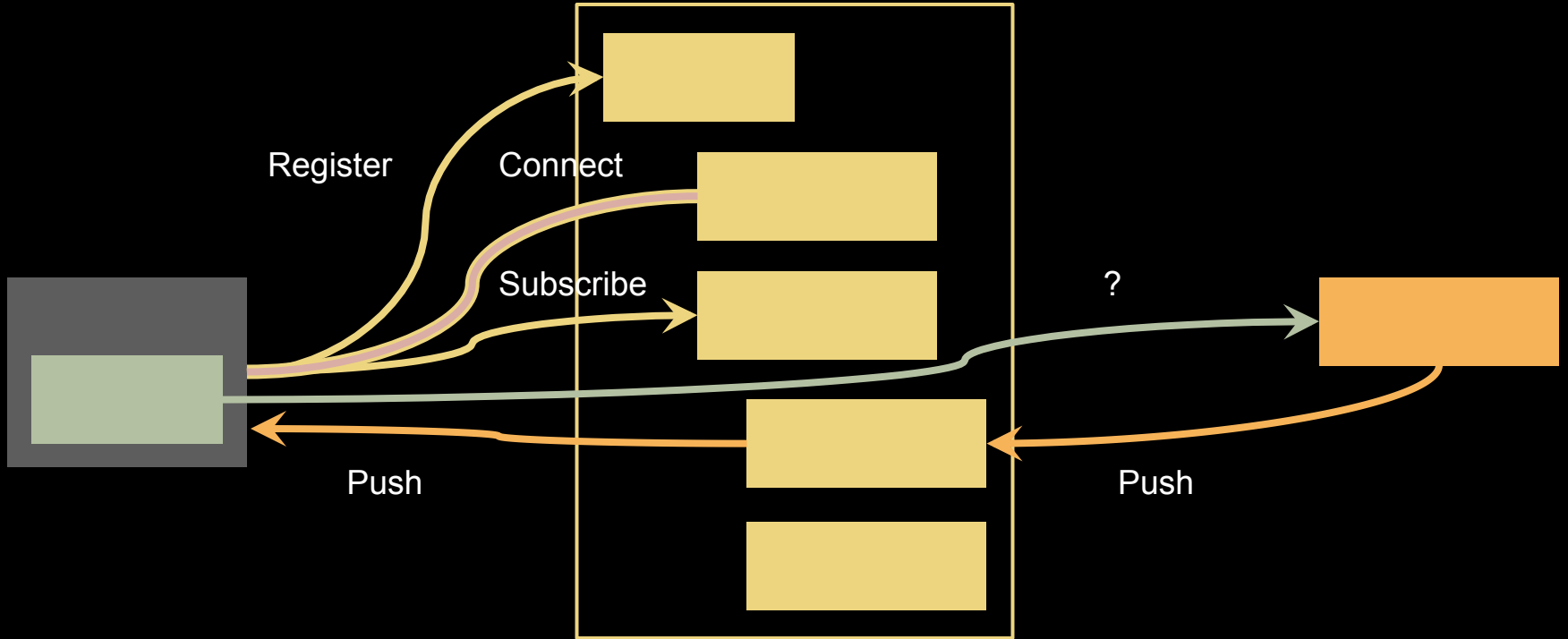
Architecture



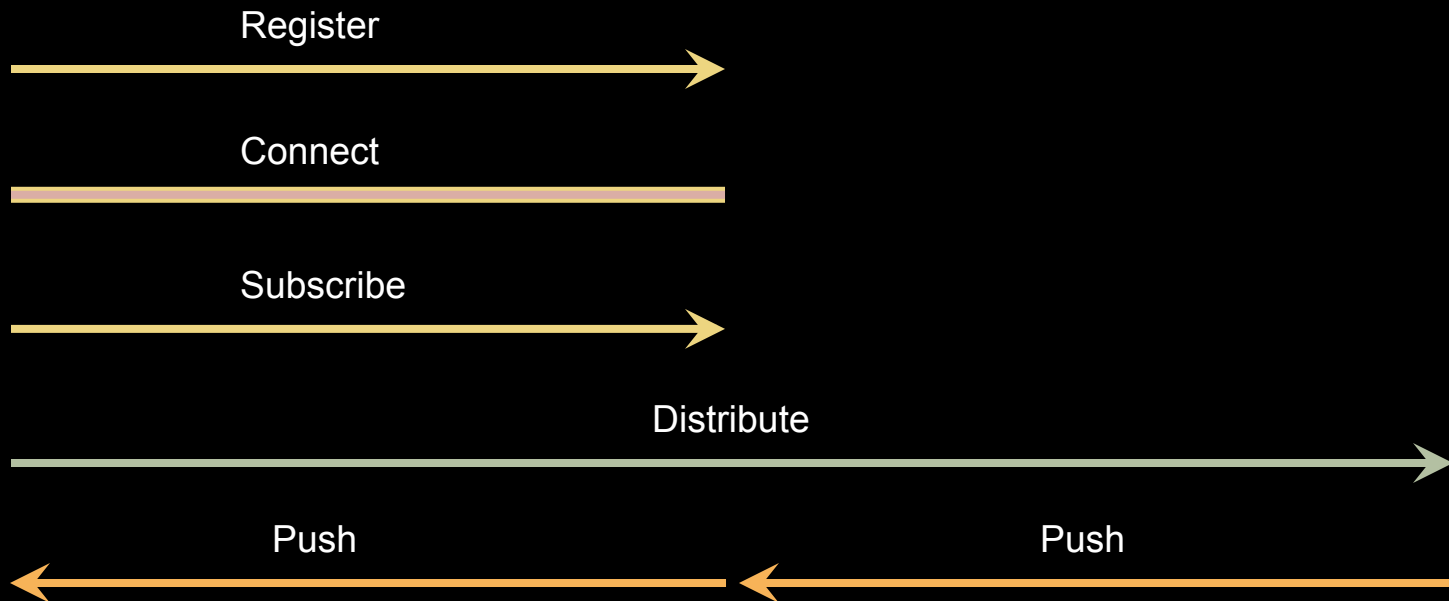
Names



Things we do



Pong



Register

POST <push service URI> HTTP/2

Host: <push service host>

201 Created

Location: <connection URI>

Link: <<connection URI>>; rel=...:monitor

Link: <<subscription URL>>; rel=...:subscribe

Connect

GET <connection URI> HTTP/2

Host: <connection host>

... { no response }

... long polling is back!

Subscribe

POST <connection URI> HTTP/2

Host: <connection host>

201 Created

Location: <subscription URI>

Distribute subscription info

Don't care how this happens

Application-specific

Push

PUT <subscription URI> HTTP/2

Host: <subscription host>

{ arbitrary content }*

Turns into server push toward the UA

Securing web push

using skullduggery

End-to-end protection

Push service sees push messages

Applications can apply end-to-end confidentiality and integrity protection

...but they probably won't

...or at least not everyone will

Forcing end-to-end integrity

The W3C API will surface a key

a new key is attached to each subscription

Messages that aren't encrypted and authenticated by that key will be dropped

The bike shed

The W3C seem likely to delegate choice of protection container to the IETF

Obviously we should build a new format

Authentication

Authenticate the application server

But to whom

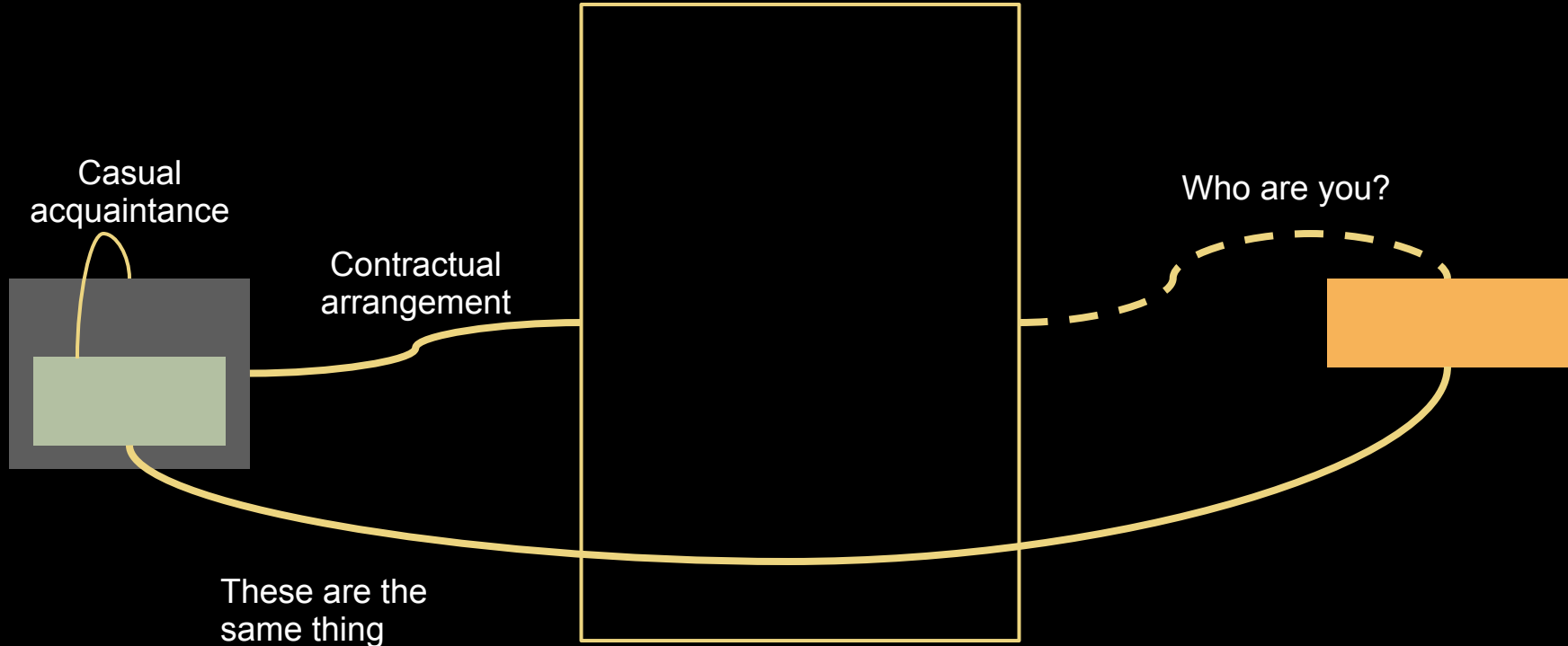
- The application?

- The user agent?

- The push service?

Current systems authenticate application servers at the push service

Established Relationships



Authentication

Current proposal uses capability URLs

My belief is that this is adequate

Time limitations are possible (and a good idea)

New protections can be added

Applications might request that the push service apply additional guards to stop unwanted pushes

The long tail

Open Issues

Need a way to signal the end of a registration or subscription

This is currently only expiration driven

More work

Delivery of the same message to many

<https://tools.ietf.org/html/draft-thomson-webpush-aggregate-00>

Prioritization

<https://tools.ietf.org/html/draft-thomson-http-nice-02>