VAPID

IETF 95, WEBPUSH

HOW IT WORKS

IN ONE SLIDE

Application servers have a signing key (ECDSA, P-256)

They sign a JWT that is bound to

- The push subscription URL (aud)
- A short interval of time (exp)
- Their contact details (sub), optionally

User agents can restrict a push subscription to a specific key

- Push service rejects pushes if a token with that key isn’t used

VOLUNTARY

MOSTLY

Will depend on push service

That’s OK

IDENTITY

SORT OF

The real identity here is a cryptographic one: the public key

The contact details aren't authenticated

They could be, maybe, but we're leaving that for another day