Push Crypto

Status, Questions

Changes

Base -encryption updated
> nonce matches recent TLS 1.3 change
Simplified record structure
> sender is required to use a single record
> receiver is required to check for truncation anyway
(i.e., Content-Length != rs + 16)

Curve choice

P-256	25519
better deployment	better

Application Server Authentication

We rely on confidentiality of URLs and DH shares

David Benjamin raised a concern that

> URLs leak

> Implementations don’t treat public keys with sufficient care

Should we add additional authentication?

> David suggests HMAC