

После разработки формата - P2P модель

- Первоначальное - без сервиса
- Или же клиент-сервис
- Запрос на подписку например, по email
- Получение контента с Google Drive
- Публикатор / Синхронизатор "постов" на Google Drive
- Локальные сервисы
 - получатель фидов, сервер / локальный дешифратор /
 - сервис - расшифровка / презентатор контента. шифратор

Рассмотрим, как
пойдут
(Клиент-сервис или
P2P)

Fidd key, metadata: 1) url 2) FlatBuf

Как получить свой fidd.key не привлекая атакующего?

- известны UserId (secret) ← collisions?
- известны MessageId
- тогда $\text{SHA256}(\text{UserId} + \text{MessageId}) \rightarrow \text{fidd.key filename}$

Можно ли без UserId?

- не думаю, т.к. без секретов не можно восстановить

Самое безопасное:

- вообще без looker, Synchronizer не fidd.key
- Сервис дает только твой ключ, через mTLS

Шифрование fidd.key

- либо при помощи User Public Key (sender unverified)
- либо при помощи User Public Key + Server Signature (standard)
- либо при помощи Service Private Key
 - + сверху при помощи User Public Key (non-standard, Public Keys secret)

Offline-flow с Offline-мобилой

ceph FS

Android app (Stream-only)

Сервис на FS-директории

Сервис на Google Drive - директории

Сервис на Сервисе

CTpuM npora v1 - npocTo cnycoK u cTpuM qpauJloB

CTopoHHuu ingest - qpopyM nocTbl, comments

- gocTyn Ha qpopyMe - o6paTHaR ppyHnoBaR nogrucb

(npobepReTcR npyBaTHblM KJII04oM, 4To6bl BblRcHyTb ecTb JIy y Bac gocTyn) mb He HywHa?

- caM qpopyM He MoweT 4yTaTb

- gocTyn gaeT ywe uMel0wuu gocTyn

ABTop (public key)

Signature embedded in fidd - sign content only

Aggregator - group chat

Enumerate subscribers and their fids

Author's signature in fidd file signs content and fidd,
publisher's signature signs fidd file with author's signature

Blog/Rep



Chat



Forum



Network



Federation

Fidd Metadata- special object or special message?

FiddHub B T.4. perucTpaTop qpuggoB? u xocTep qpuggoB

Fidd Metadata - Tuna xegepa Ha rpyne, 4To, 3a4eM,
no4eMy, onucaHue u np.