Locally Decrypting URLs

For Dispatch at IETF114

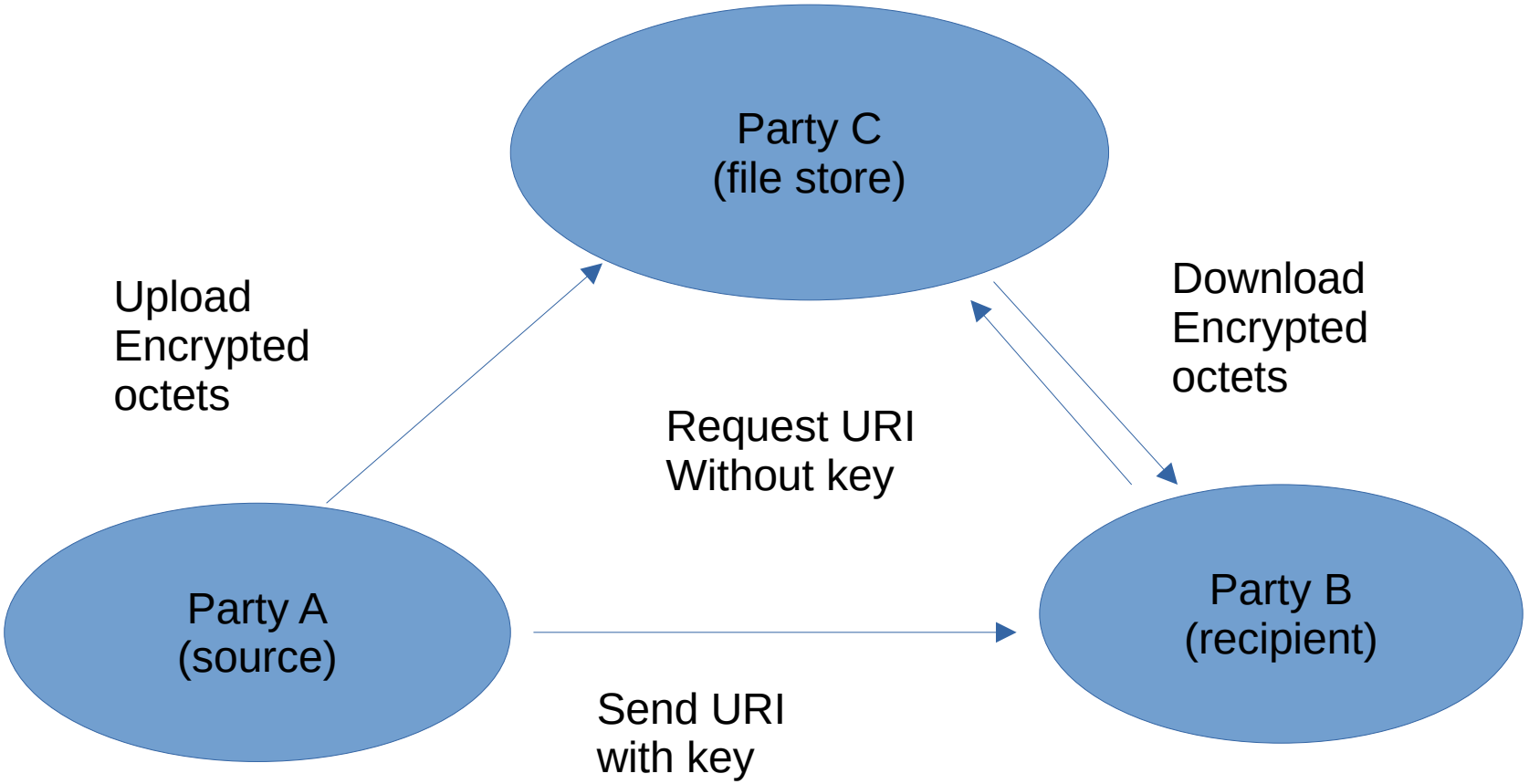
Bron Gondwana
<brong@fastmailteam.com>

Problem statement

- I came to this via the “large file email” problem
- Party A wants to send data to party B
  - Both aren’t online at the same time, or not 24/7
  - So data gets stored with an intermediate 3rd party
- Right now: either third party gets an unencrypted blob; or need special tooling.

Transparent Decryption

- In my dream world:
  - Party A creates and encrypts the blob
  - Party C stores the encrypted blob, and never sees the decryption key
  - Party B receives a URI in some standard form, which transparently decrypts the blob while downloading
- Party A and Party C need some relationship (contract) since party C is storing data on behalf of Party A
- Party B need know nothing of this
  - so long as their software handles the format, they can transparently get a regular https: download URI, or one of these things, and it works the same
  - Any software on Party B's machine gets the plaintext octets when asking the standard library / operating system to fetch the URI, regardless of whether it's in this format.


Party C
(file store)
Upload
Encrypted
octets
Download
Encrypted
octets
Request URI
Without key
Party A
(source)
Party B
(recipient)
Send URI
with key

Bootstrapping

- It will take time, but the goal is to limit the number of places this needs to be implemented.
- Data transfer formats and messaging formats need no changes; it’s just another URI
- Decryption key is in a URI fragment or other part of the URI structure such that the server (party C) never sees the key material.

Design

- Option – new scheme
  - https+xcrypto://example.com/download/foo#<key>
- Option – fragment magic
  - https://example.com/download/foo#xcrypto_key=<key>
- Option – something else?
  - I’d love suggestions, this isn’t my area of expertise

Usage

BEGIN:VCARD
VERSION:3.0
N:Gump;Forrest;;Mr.;
FN:Forrest Gump
ORG:Bubba Gump Shrimp Co.
TITLE:Shrimp Man
PHOTO;TYPE=JPEG;VALUE=URI:https://upload.wikimedia.org/wikipedia/commons/8/87/My_Dog_%2861220578%29.jpeg
TEL;TYPE=WORK,VOICE:(111) 555-1212
TEL;TYPE=HOME,VOICE:(404) 555-1212
ADR;TYPE=WORK,PREF:;;100 Waters Edge;Baytown;LA;30314;United States of America
...
EMAIL:forrestgump@example.com
REV:2008-04-24T19:52:43Z
END:VCARD

BEGIN:VCARD
VERSION:3.0
N:Gump;Forrest;;Mr.;
FN:Forrest Gump
ORG:Bubba Gump Shrimp Co.
TITLE:Shrimp Man
PHOTO;TYPE=JPEG;VALUE=URI:https://files.example.com/c3e72b46-a93b-4068-a5b5-f862d9f0a7c2/data.jpeg#xcrypto_key=<alg>:<key>
TEL;TYPE=WORK,VOICE:(111) 555-1212
TEL;TYPE=HOME,VOICE:(404) 555-1212
ADR;TYPE=WORK,PREF:;;100 Waters Edge;Baytown;LA;30314;United States of America
...
EMAIL:forrestgump@example.com
REV:2008-04-24T19:52:43Z
END:VCARD

Dispatch Questions

- Is something like this even within the IETF’s remit/interest?
- If so, where should the work be done?
- Volunteers to help?