Uploading Media to Trusted Destination Server (old version)

When the user finishes creating an image or video in InformaCam, it automatically uploads to the chosen trusted destinations. This document explains that process.

Saving media

Upon saving an image or video, the device will generate a random public/private keypair that encrypts the metadata. This key can be used only by the device to access a source image's metadata. When the user is connected to the internet, the upload process begins.

Request for upload

For each selected trusted destination, the device must request an upload ticket. This transaction is carried out via the trusted destination's hidden service address (which is held in the device's encrypted database.)

For each upload, the Trusted Destination's server will generate an upload ticket containing a one-time-use password to encrypt the image/video. The device must then re-encrypt the metadata bundle with this password using AES encryption. Once the media is stored on the Trusted Destination's server, the media's metadata can only be decrypted with this password.
Upon request, the device must submit the following data:

1. the SHA-1 hash of the unredacted data to be uploaded
2. the SHA-1 hash of the redacted data to be uploaded
3. the number of bytes to be transmitted
4. the PGP key of the user's device (each device generates its own PGP key that is signed by the user upon initiation)

In response, (if approved) the server generates a [[one-time-use authentication token]] to the device to initiate upload. The server creates a unique, one-time-use user for this upload, and adds the user's unique ID to a queue of uploads to collect and then move to the main media repository upon successful upload. (This user ID is to be deactivated and removed upon successful upload.)

Uploading process

After receiving the authentication token, the user transmits the media via SSH over Tor via a background service on the app. Once the number of bytes declared in step 1 have been transmitted, the server must validate the hash of both the unredacted and redacted data to verify that the media received is the same as the media uploaded. Successful verification triggers a response to the user's device that the media has been accepted and stored by the trusted destination.

Upon successful transmission

Once the image or video has been successfully transmitted, the InformaCam-generated PGP key of the device is logged. If the administrator acting on behalf of the trusted destination desires to get in contact with the user, connection may be initiated via this key.