

[illegible]

- a. Immigration lawyer (IL) is provided with the Vault Access canister (VA) canister URL
- b. IL logs into the VA and following authentication via her II makes a request to access the Evidence Vault (EV) to download files (e.g. all/part of the timeline)
- c. The VA sends a request to the Relationship for the master key, and a secure connection (three pass protocol) is established
- d. The Partners' apps collaborate using the Vetkeys service to recreate the master key using the threshold algorithm and securely transmits it to VA
- e. The VA uses the master key along with the algorithm for the deterministic encryption keys to access and decrypt the requested parts of the EV, to create a viewer package
- f. VA creates a temporary encryption key (temp-key) by hashing the concatenation of the master key and the IL's II. The temp-key is used to re-encrypt the viewer package, which is stored in a temporary canister (set to 'expire' after a set period, using techniques such as expiry-duration and heartbeat)
- g. VA uses the same secure connection from step c to transmit the temp-key to IL, along with the TV URL
- h. IL, again using the secure connection, connects to TV and uses the temp-key to decrypt the viewer package. The contents of the viewer package are now displayed on IL's terminal. Ideally, the file download and screen-print facilities will be blocked for security reasons (depending on the access agreements we have with the authorised entities: e.g. perhaps we will be forced to allow immigration officials the ability to download content)