1. To verify that no one modifies the file or the containers contents.

2. It is used to generate a random starting seed for the encryption.

3. The files themselves aren’t encrypted so you technically can’t provide the keys for them. I think that these laws are not okay, based on some idea of right to privacy.

4. It is legally barred by the 5th amendment, but there are specific cases where it has been overruled. They can take your device, but they can’t *force* you to give passwords, however they can make life inconvenient for you if you don’t.

5. By physical transfer, preferably several napkins containing parts of the passwords.

6. It is apparently safe to use, even though it lost the support of its original creators.