Digital Content

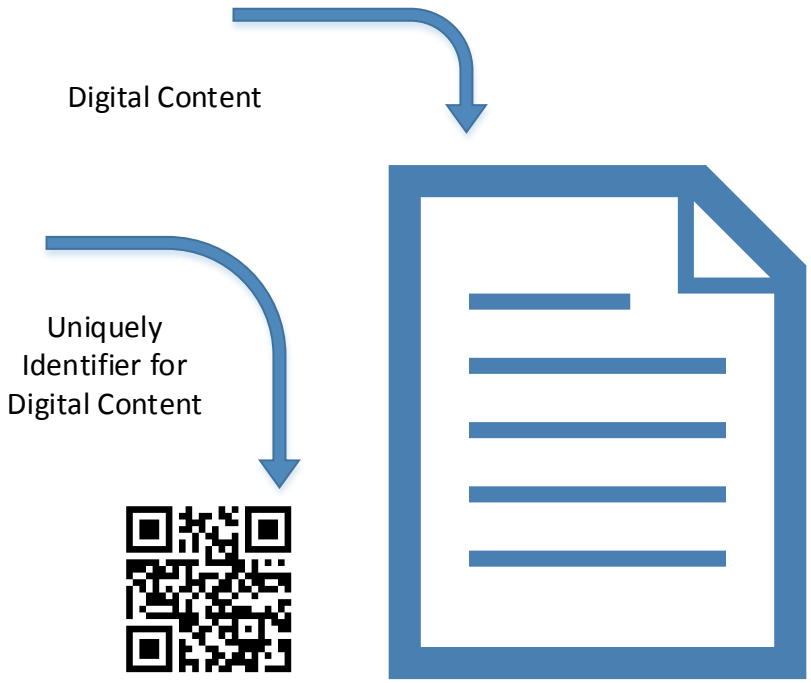
Digital Content includes any data that you can store on a computer or mobile device. This includes text files, pictures, videos, sound clips, spreadsheets, …

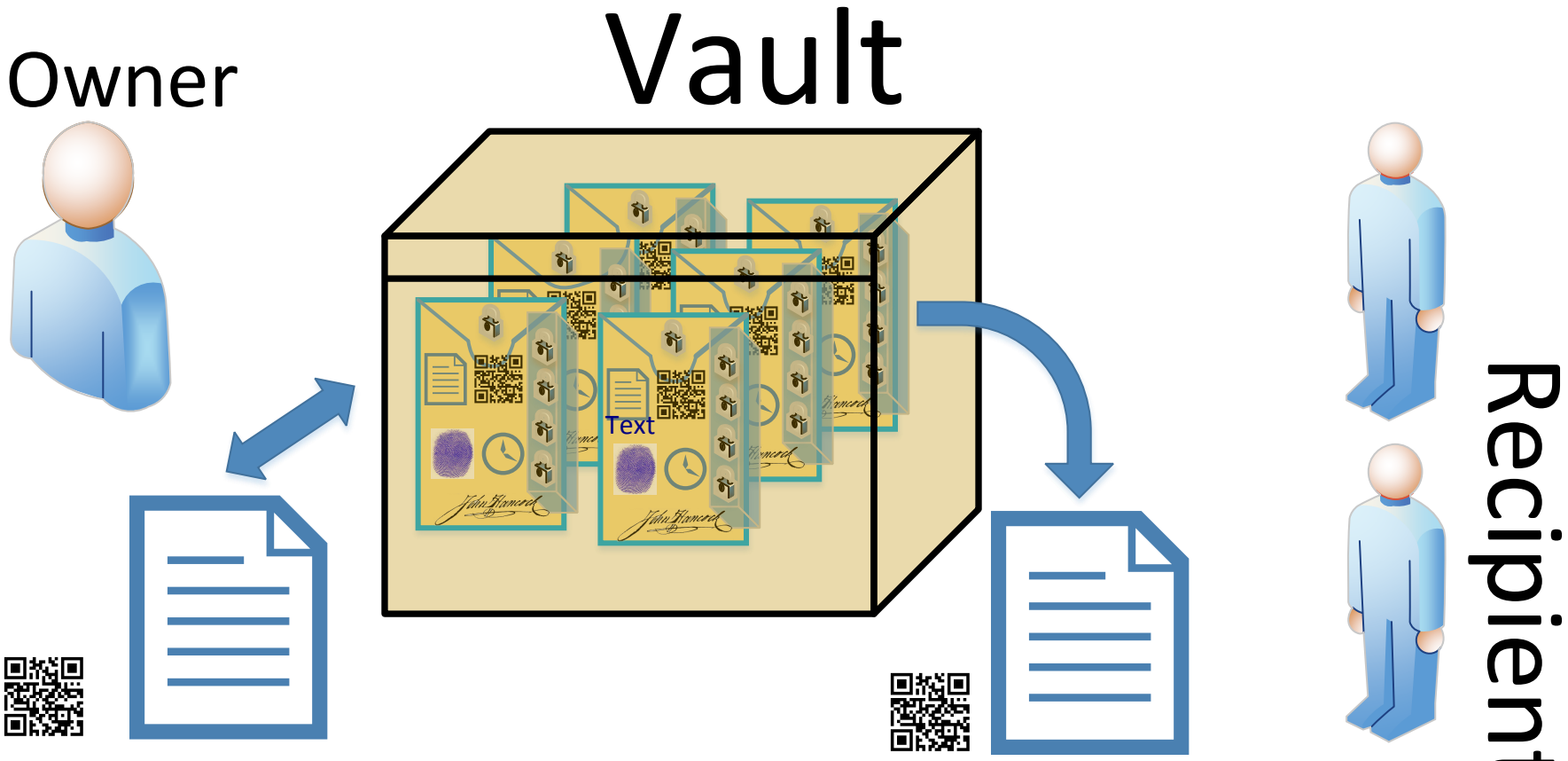
When you share some Digital Content, you want to make sure that the recipients receive an exact copy of the Digital Content that you provided.

We use standard computer practices to generate a “Cryptographic Hash” which is a unique identifier for some Digital Content.

Even the smallest change to the Digital Content will generate a completely different “Hash”.

If the generated Hash for two instances of Digital Content are the same then the Digital Content is guaranteed to be exact copies of each other.





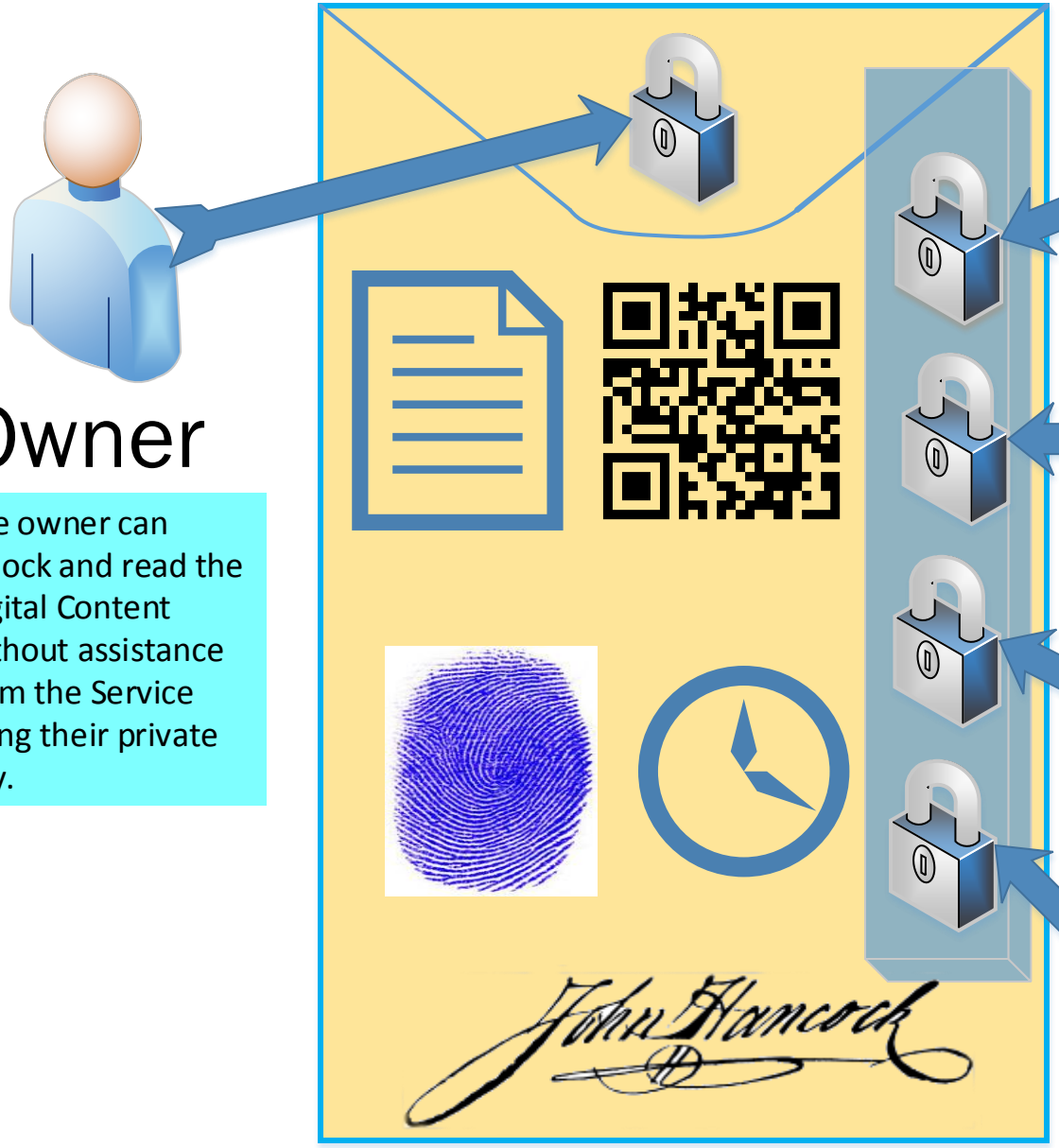
A Vault has an Owner. The Owner indicates the Recipients they wish to share their data with. It has a mode which indicates the Owners “Intent to Share” with the Recipients. This mode can be “Safe Deposit Box” where sharing does not happen until something happens to the Owner. The Recipients demonstrate their Legal claim to the Administrator to facilitate their access. The mode can be a Time Capsule where sharing happens at a future Owner Specified time. An immediate mode is also possible and can be used for secure sharing of Digital Content In The Cloud. The “Escrow” mode can be used when there is some legal arrangement between the Owner and Recipients that specifies the Digital Content to placed into the Vault, and when the sharing of the Digital Content happens.

The Owner determines the Digital Content that is contained in the Vault. A side effect of adding Digital Content to the Vault is that the content is encrypted and Digitally/Cryptographically Signed and Time Stamped.

When an Owner adds a Recipient to a Vault. The Recipient will be made aware of the Vault. The Recipients will minimally be able to know the “Intent to Share” or mode of the Vault, the number of Vault Files, the number of recipients, and the most recent date where content was added or modified. The Owner can also specify that the Recipients are able to see the Names and the Creation or Modification date of ALL of the Vault Files. And lastly, as specified by the Owners “Intent to Share”, the Recipients can have full access to the unencrypted Digital Content.

Each Vault has a Unique Vault ID (VID) defined by the Service.

Vault File



Owner

The owner can unlock and read the Digital Content without assistance from the Service using their private key.

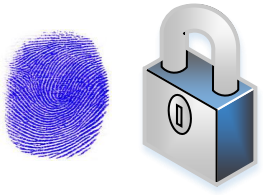
The Master Lock is unlocked by the Service (using the App) if the Owner has indicated that the Vault files can be read by the Recipients.

Recipients

In order for a recipient to be able to unlock their lock with their private key, the Master Lock must be unlocked by the service (using the App).

A Vault File is an Envelope (Zip File) that contains the original Digital Content in an encrypted format as well as additional Meta Data. This additional Meta Data includes a Cryptographic Hash that uniquely identifies the Digital Content, the Owners Digital Thumbprint, a Digital Signature of the document by the Owner, and a Cryptographic Time Stamp of the time the Digital Content was Signed. It also contains Meta Data that enables Recipients to access the Digital Content if enabled by the Service (Complying with the Owner's defined Intent to Share).

Signing Certificate

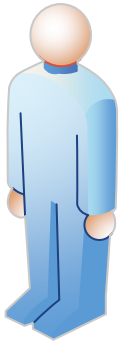


The Signing Certificate is critical to providing security and validation of the Digital Content and it's Meta Data for a Vault File. It contains some information that is public, such as your Name and Address, and your Digital Thumbprint. This public information is only shared with your Recipients via the Service.

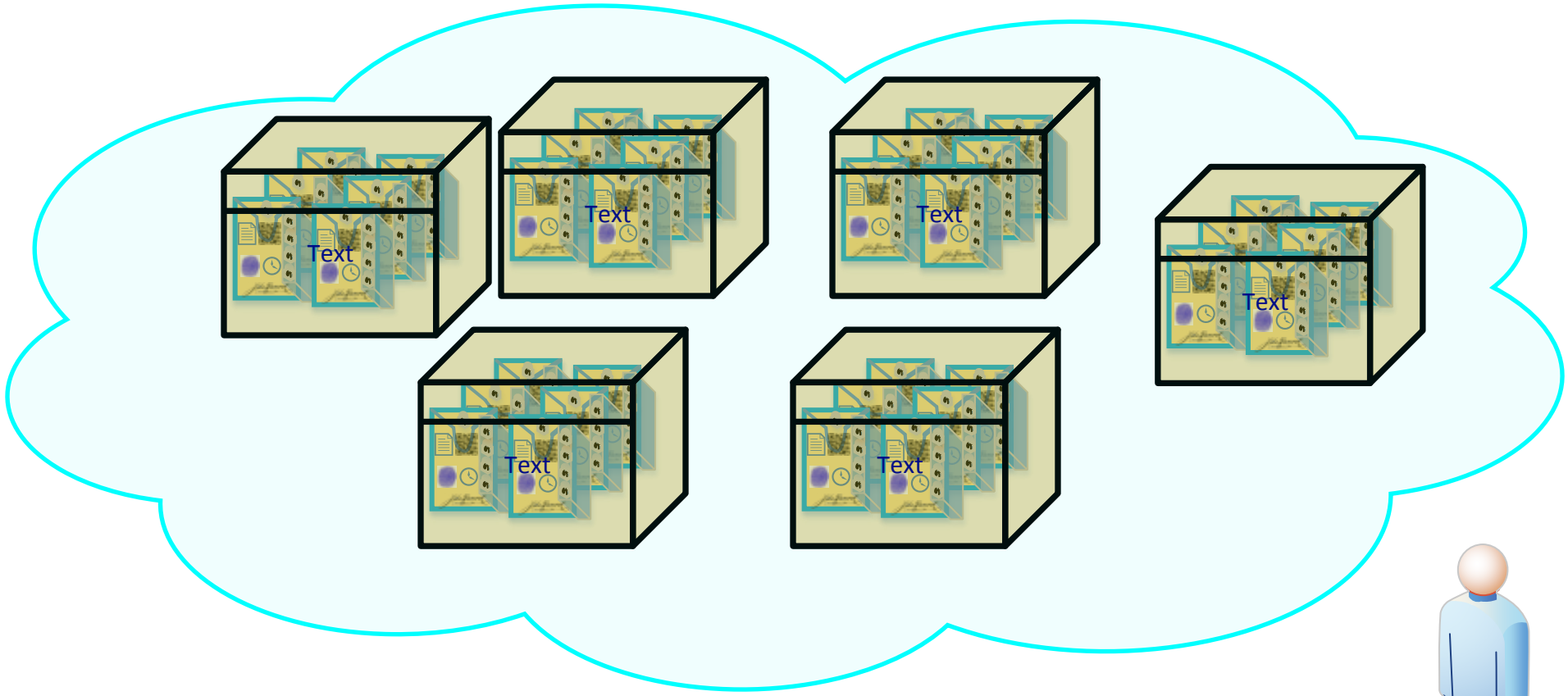
The Signing Certificate also contains a Key that is used for encryption and digital signing. You should protect your access to the key by adding a separate password to the your account with the Service. Do not share this password with ANYONE. Access to the Key enable the modification of Digital Content in the Vault, and Digital Signing in your name!

When an Owner creates a Vault File, it obtains the publicly accessible Signing Certificate for each Recipient. It uses this to create a Lock, identified by the Recipients Digital Thumbprint, that only that Recipients Private Key can unlock. This lock secures the information needed to decrypt the associated Digital Content.

In the Vault File, the various locks are identified by the Digital Thumbprint. To unencrypt the Digital Content, the App will find the lock that matches the Digital Thumbprint of the Users Signing Certificate. The key associated with the certificate can be used to access the information secured by the lock. In the case of a Recipient Lock, this information is also encrypted by the Service to ensure that the user can only access the Digital Content in a manner that is consistent with the Owner's "Intent to Share".



In The Cloud



A user can be an Owner of many Vaults, and a Recipient of many other Vaults. Security of the Vault contents as well as complete assurance that the contents are conveyed from the Owner to the Recipients, at the designated time, in an unaltered form is the primary focus of the Service.

Vaults are stored in the Internet Cloud. The commercial Cloud Storage Services provide security for communicating between the Cloud Service Storage Servers and the Users. Unauthorized access of the data has been demonstrated by internal/external "Hackers" of those Services.

In this type of security breach only the Meta Data for a Vault File would be accessible. The Digital Content is encrypted in such a manner that the only people that can ever access the actual unencrypted Digital Content are the Owner, and when Authorized by the Owner based on their "Intent to Share", the Recipients (Brute force attacks are possible but not practical with current encryption standards).

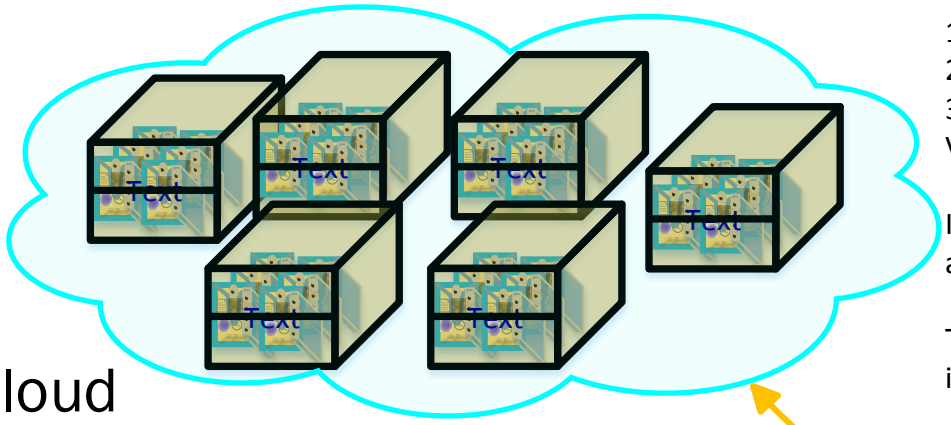
When a Recipient does access the Vault File, the Meta Data is used to Validate that the Digital Content is an unmodified copy of the original Digital Content, that was placed into the Vault, by the Owner, at the specified Time Stamp. The Techniques used are Legally Binding in most parts of the world. Any attempt to modify the Digital Content and/or the Time Stamp would be detected during validation.

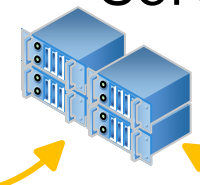
Service

The Service provides a Database of:
1) Users
2) Users Signing Certificates (Public Information)
3) Vault definitions including the Vaults Owner, “Intent to Share” Vault mode, Recipients, and Links to Cloud Storage

It also provides a Cryptographic Time Service to timestamp files added to a Vault.

The Administrator of the Service can release a Vault to Recipients if the Recipients can prove they have legal access to the Vault.






Last Will and Testament (Verified)


Financial Status & Inventory (Verified)


Last Will and Testament (Original)


Financial Status & Inventory (Original)

6/7/2014
Owner Places Digital Content into the Vault and Identifies Recipients and Intent to Share as a Safe Deposit Vault.

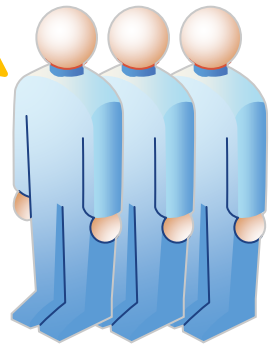
7/14/2020
Recipients Provide Copy of Death Certificate To the Administrator

7/16/2020
Administrator verifies “Intent to Share” with All Recipients and releases the Digital Content if no objections from the parties.

7/4/2020
Owner Dies

7/16/2020
Recipients receive a copy of the Digital Content and Verifies it is An unmodified version of the Digital Content Placed into the Vault by the Vault Owner on the Specified Date and Time (June 7, 2014)

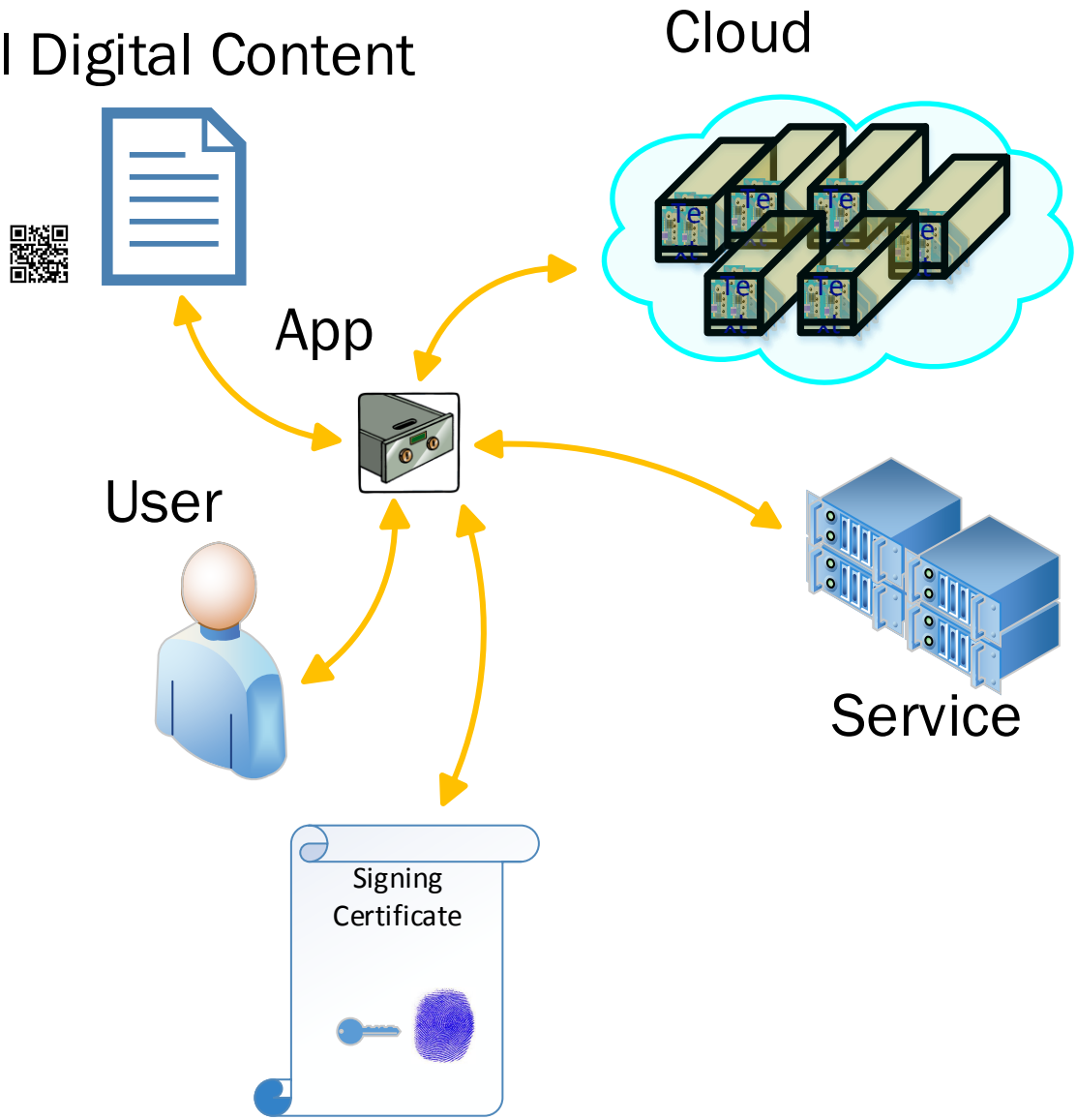
Time



App

The App allows the User to interact with the Cloud Storage and the Service to deposit and extract Digital Content from Vaults. It allows the user to do the following:

1) Specify the Cloud Storage Account (Different, but linked to the Service Account).
2) Create and Mange the Signing Certificate that is used to securely encrypt and decrypt Digital content and sign/verify the Digital Content has not been modified. Provides protected storage for your private key.
3) Create Vaults, Specify the Vault Mode witch defines your “Intent to Share”, and specify the Recipients for a Vault.
4) Move local Digital Content to/from your Vaults. When you save data to the vault it is Digitally Signed and gets a Cryptographic time stamp that can be verified before/when/after you extract a file from a vault.
5) Extract Digital Content that you are a recipient of from another user’s Vaults. The Digital Signature, and Cryptographic time stamp can be verified which assures you the Digital content is an exact copy of the Digital content that the owner signed and saved in the Vault at the specified time.



Current Cryptographic Standards

- Hash Function - SHA-512
  Used to Hash of the Digital Content to uniquely Identify the Digital Content.

  Used to Hash of the Signing Certificate to provide a Digital Thumbprint for the Certificate Owner.

- Block Encryption – RSA/ECB/PKCS1Padding – 2048 bit key
  Used for the Locks in the Vault Files, the locks secure the AES Key for the file, uses the Recipients Certificate.

  Used for Digital Signature of the Digital Content, uses the Owners Certificate.

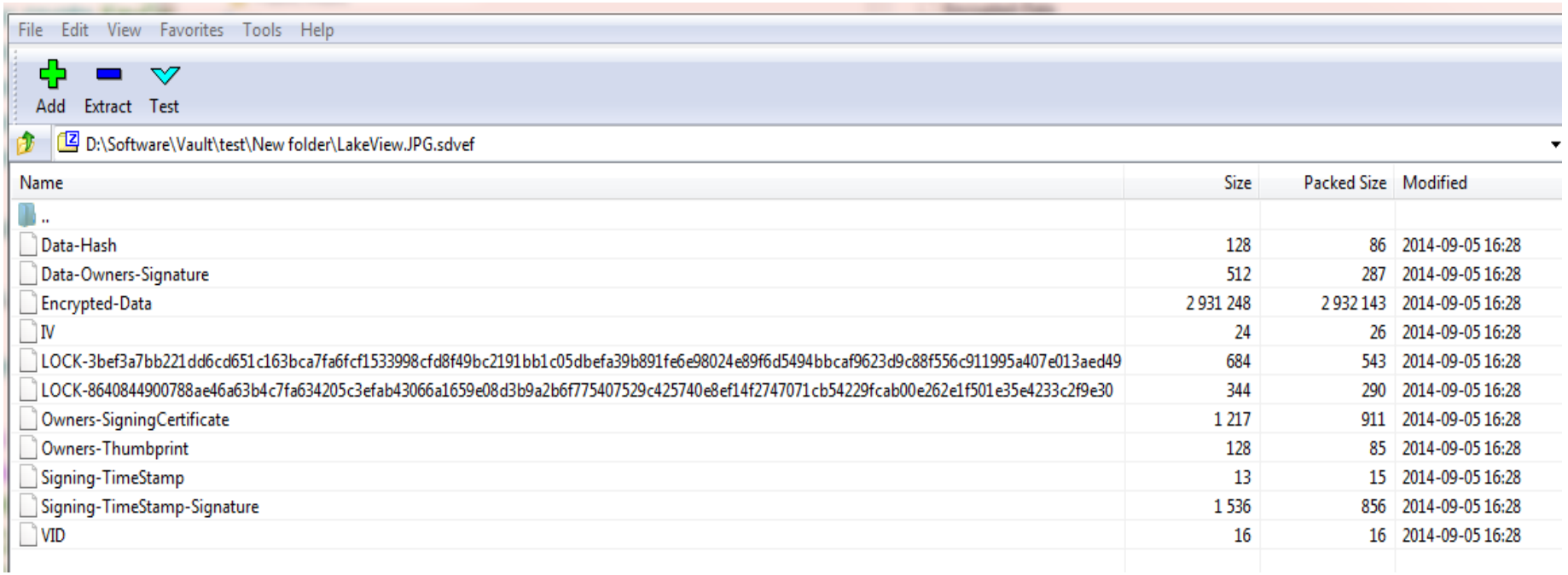
  Used for Digital Signature of Time Stamp, uses the Services Certificate.

.

- Stream Encryption - AES/CBC/PKCS5Padding – 256 bit key
  Used to Encrypt/Decrypt the Digital Content.

Zip File View of Vault File

A file stored in a Vault on the Cloud is actually a simple ZIP file that contains an encrypted copy of the original Digital Content as well as Meta Data used to Cryptographically sign and time stamp when the Digital Content was placed into the Vault.



Name	Size	Packed Size	Modified
..			
Data-Hash	128	86	2014-09-05 16:28
Data-Owners-Signature	512	287	2014-09-05 16:28
Encrypted-Data	2 931 248	2 932 143	2014-09-05 16:28
IV	24	26	2014-09-05 16:28
LOCK-3bef3a7bb221dd6cd651c163bca7fa6fcf1533998cfd8f49bc2191bb1c05dbefa39b891fe6e98024e89f6d5494bbcaf9623d9c88f556c911995a407e013aed49	684	543	2014-09-05 16:28
LOCK-86408449007 88ae46a63b4c7fa634205c3efab43066a1659e08d3b9a2b6f775407529c425740e8ef14f2747071cb54229fcab00e262e1f501e35e4233c2f9e30	344	290	2014-09-05 16:28
Owners-SigningCertificate	1 217	911	2014-09-05 16:28
Owners-Thumbprint	128	85	2014-09-05 16:28
Signing-TimeStamp	13	15	2014-09-05 16:28
Signing-TimeStamp-Signature	1 536	856	2014-09-05 16:28
VID	16	16	2014-09-05 16:28