What is Claimed is:

1. A computer-implemented method for anonymously evidencing the existence of a digital document comprising the steps of:

A. obtaining metadata of a digital document in a user's system;

B. obtaining a cryptographic hash of the digital document;

C. sending the metadata and the cryptographic hash to a remote device;

D. receiving the metadata and the cryptographic hash at the remote device,

E. requesting the user's identity data from an identity source;

F. obtaining a cryptographic hash of the user's identity data to form an identity hash;

G. receiving the identity hash at the remote device;

H. combining the metadata, the cryptographic hash, and the identity hash at the remote device in an evidence key generator to generate an evidence key;

I. storing the evidence key to provide a stored evidence key;

J. generating a reference code for the stored evidence key; or wherein the reference code is a QR code, and

K. sending the reference code to the user, a third party and a combination thereof,

wherein the digital document never leaves the user's system, wherein the identity data never leaves the identity source, and wherein the reference code allows a third party to access the evidence key; or allows a third party limited access to the evidence key, optionally wherein the digital document comprises information selected from the group consisting of biometric information, corporate information, financial information, health information, historical information, identity information, legal information, personal information, and a combination thereof.

2. The method according to Claim 1, further comprising the steps of:

requesting a time stamp by the remote device from a time source;

receiving the time stamp at the remote device from the time source, and wherein the remote device does not comprise the time source.

3. The computer-implemented method of Claim 1, wherein the identity source is selected from the group consisting of an identity document, an identity database, and a combination thereof.

4. The computer-implemented method of Claim 3, wherein the identity document is selected from the group consisting of a government identification, a private identification, and a combination thereof.

5. The computer-implemented method of Claim 4, wherein the government identification is selected from the group consisting of a driver's license, a passport, a tax identification, a citizenship identification, a legal status identification, a residency identification, a voter registration identification, a biometric identification, and a combination thereof.

6. The computer-implemented method of Claim 4, wherein the private identification is selected from the group consisting of a membership identification, a group identification, an institutional identification, an affiliation identification, a company identification, and a combination thereof.

7. The computer-implemented method according to Claim 3, wherein the identity document is a surrogate identification.

8. The computer-implemented method according to Claim 3, wherein the identity database is selected from the group consisting of a public identity database, a private identity database, a government identity database, a voter registration database, a medical database, a credit database, a financial database, and a combination thereof.

9. The computer-implemented method according to Claim 1, wherein the digital document is selected from the group consisting of a voting ballot and the identity document is a voter registration document.

10. A computer-implemented method for evidencing the existence of a digital document comprising the steps of:

A. obtaining metadata of a digital document on a user's system;

B. obtaining a cryptographic hash of the digital document;

C. sending the metadata and the cryptographic hash from the user's system to a remote device; or sending the metadata and the cryptographic hash to the remote device over the internet;

D. receiving the metadata and the cryptographic hash at the remote device;

E. requesting a time stamp from a time source;

F. receiving the time stamp at the remote device from the time source, wherein the remote device does not comprise the time source, and wherein the time stamp is based upon the time that the remote device receives the metadata and the cryptographic hash;

G. combining the metadata, the cryptographic hash, and the time stamp at the remote device in an evidence key generator to generate an evidence key;

H. combining a plurality of evidence keys to form a compound evidence key; optionally wherein the plurality of evidence keys comprises from about 2 to about 1000 evidence keys; or from about 5 to about 100 evidence keys;

I. storing the compound evidence key to provide a stored compound evidence key;

J. generating a further cryptographic hash of the compound evidence key to form a further evidence key; and

K. storing the further evidence key to form a stored further evidence key,

wherein the digital document never leaves the user's system.

11. The method according to claim 10, further comprising the step of storing compound metadata with the plurality of evidence keys to form the compound evidence key, optionally wherein a predetermined period of time determines which evidence keys in the plurality of evidence keys are combined into the compound evidence key.