CLAIMS

1. A method for deploying a trusted identity for a user issued by an issuer,

wherein the user has a user device configured to send a request for signature to an issuer device handled by the issuer, said request comprising a user public key allocated to the user,

wherein the issuer device is configured to compute an issuer signature by signing both the user's trusted identity and the user public key using an issuer private key allocated to the issuer,

wherein a block chain transaction containing the issuer signature is created and submitted to a Block Chain for transaction verification and storage,

wherein said request comprises a block chain address, wherein the issuer device generates an encrypted identity by encrypting the trusted identity with a secret key generated in the issuer device,

wherein the issuer device generates an encrypted key by encrypting the secret key using the user public key, and

wherein the issuer device creates a block chain transaction containing a digital asset including both the issuer signature, the encrypted identity and the encrypted key and submits the block chain transaction to the Block Chain for transaction verification and storage to the block chain address.

2. The method according to claim 1, wherein said issuer device sends the issuer signature in response to

the request and wherein the block chain transaction is created by the user device and contains the user's trusted identity.

3. The method according to claim 2, wherein the user device generates an encrypted identity by encrypting the user's trusted identity with a secret key generated in the user device,

wherein the user device generates an encrypted key by encrypting the secret key using a key encryption key, and

wherein the block chain transaction created by the user device contains the encrypted key and the encrypted identity.

4. The method according to claim 3, wherein the key encryption key is a public key belonging to a key pair generated by the user device.

5. The method according to claim 1, wherein said request comprises a block chain address, wherein the issuer device computes a hash of the trusted identity and sends the trusted identity to the user device,

wherein the issuer device creates the block chain transaction containing the hash and submits said block chain transaction to the block chain for transaction verification and storage to the block chain address, and

wherein the user device receives the block chain transaction from the block chain.

6. A method for authenticating a user trusted identity by a verifier device, said user trusted identity being issued by an issuer,

wherein the user has a user device which sends a message to the verifier device, said message comprising a transaction identifier, and a user public key allocated to the user,

wherein the verifier device retrieves a block chain transaction comprising an issuer signature from a block chain using the transaction identifier and verifies the transaction,

in case of successful verification, the verifier device sends a challenge to the user device which computes a response by signing the challenge using the user's private key and sends the response to the verifier device, the verifier device checks the user signature using the user public key,

in case of successful checking, the verifier device verifies the issuer signature using both the user trusted identity, the user public key and the issuer public key,

wherein the block chain transaction contains an encrypted key and an encrypted identity,

wherein, in case of successful checking of the user signature, the verifier device sends the encrypted key and a verifier public key to the user device,

the user device derives a key encryption key and retrieves a secret key by decrypting the encrypted key using the key encryption key, then the user device encrypts the secret key using the verifier public key

and sends the resulting new encrypted key to the verifier device, and

the verifier device retrieves the secret key by decrypting the new encrypted key using a verifier private key, then the verifier device retrieves the user trusted identity by decrypting the encrypted identity using the secret key.

7. The method according to claim 6, wherein the verifier device retrieves the user trusted identity from a block chain transaction or receives the user trusted identity from the user device.

8. An issuer device configured to send a trusted identity for a user issued by an issuer,

wherein the issuer device is configured to receive a request for signature from a user device, said request comprising both a block chain address and a user public key allocated to the user of the user device,

wherein the issuer device is configured to compute an issuer signature by signing both the user's trusted identity and the user public key using an issuer private key allocated to the issuer,

wherein the issuer device is configured to generate an encrypted identity by encrypting the trusted identity with a secret key generated in the issuer device,

wherein the issuer device is configured to generate an encrypted key by encrypting the secret key using the user public key, and

wherein the issuer device is configured to create a block chain transaction containing a digital asset including both the issuer signature, the encrypted identity and the encrypted key and to submit the block chain transaction to a Block Chain for transaction verification and storage to the block chain address.