GDCA's solution to the Digital ID Design Challenge

By

Team GDCA

30 October 2017

Table of Contents

1. Introduction

Introduction

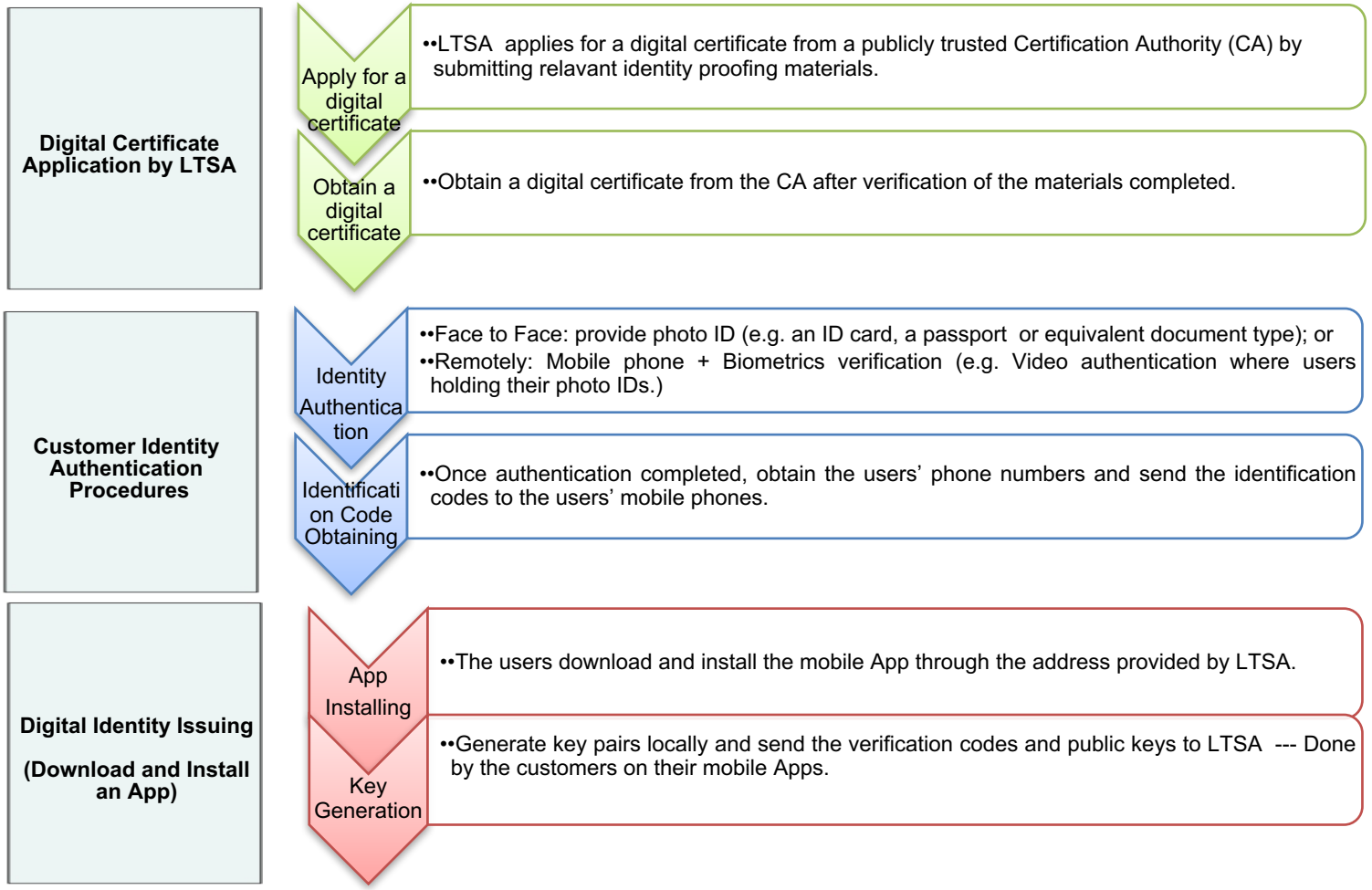
About GDCA: Global Digital Cybersecurity Authority Co., Ltd ("GDCA") is a Certification Authority (CA) based in China and founded in March 2003. Being a WebTrust certified CA, GDCA has its root CA included in multiple trust programs. GDCA has been committed itself in providing publicly-trusted electronic certification services, and it is becoming a first-class information security services provider in China and internationally.

By joining like-minded organizations including CA/Browser Forum, FIDO Alliance, IFAA Alliance etc., GDCA is well informed of the state of the art technologies, security and privacy best practices, and the latest policies and standards in the community, and also contributes its part in moving the industry forward, both in China and internationally.

Current Problems: Inefficiencies caused to LTSA and inconvenience and extra cost to customers due to possible loss or misplacement of the original PDF of the eSTC. Additionally, third parties have trust issues with an electronically delivered eSTC.

An overview of our proposed solution: Authentication on the customers identities, customers download and install a mobile App, LTSA issues eSTCs on blockchain, and third parties, after being authorized by the customers, access and verify the issued eSTCs within a specified period of time.

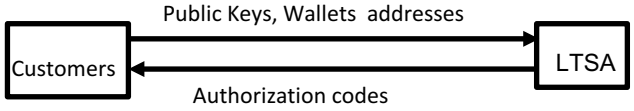
2. Identity Proofing and Digital Identity Issuing



3. Issuing an eSTC

Step 1

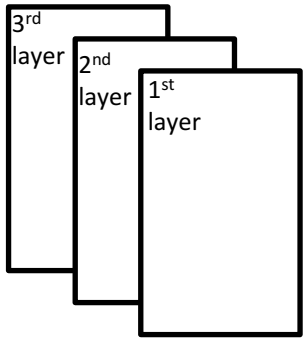
LTSA receives the public keys and wallets addresses of the customers, and bind them to the authorization codes.



Step 2

An eSTC issued by LTSA consists of the following three layers:

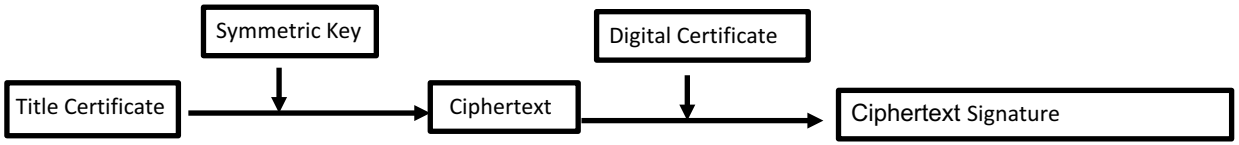
The first layer is the physical appearance of a Title Certificates;
The second layer stores customers' public keys and codes related to the links in the 1st layer;
The third layer stores the digest value of the Title Certificate and codes related to the links in the 2nd layer.



(Source: http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017)

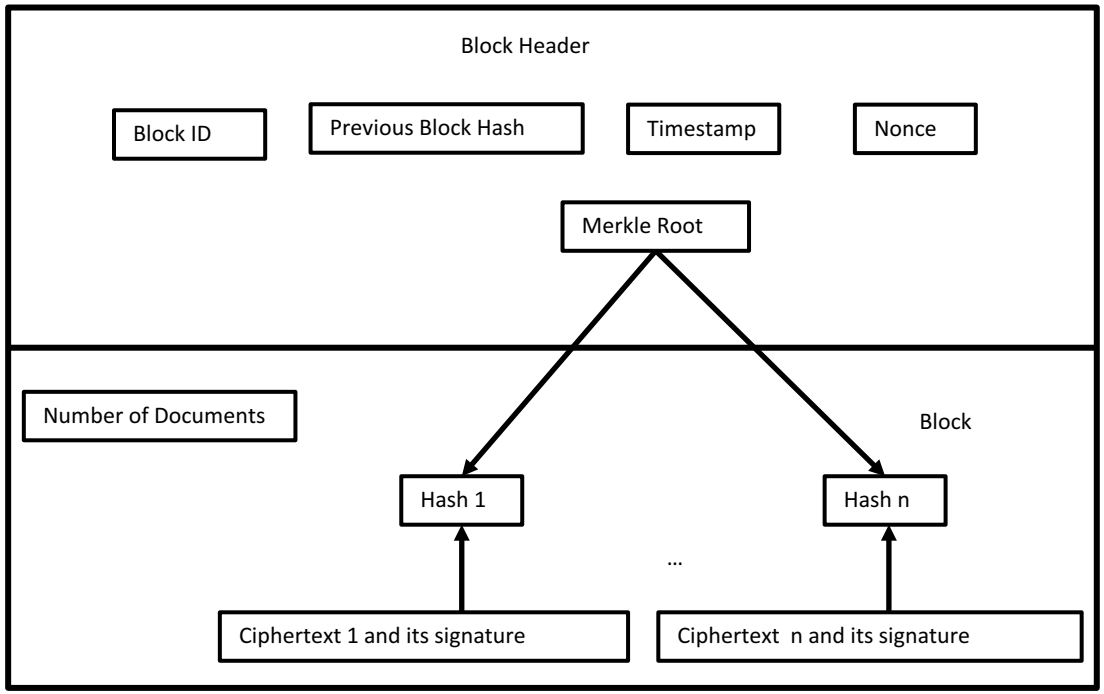
Step 3

LTSA generates a 256-bit symmetric key and encrypts the Title Certificate using the AES-CBC algorithm to get the Ciphertext, And LTSA uses the digital certificate from the CA to digitally sign the Ciphertext.



Step 4

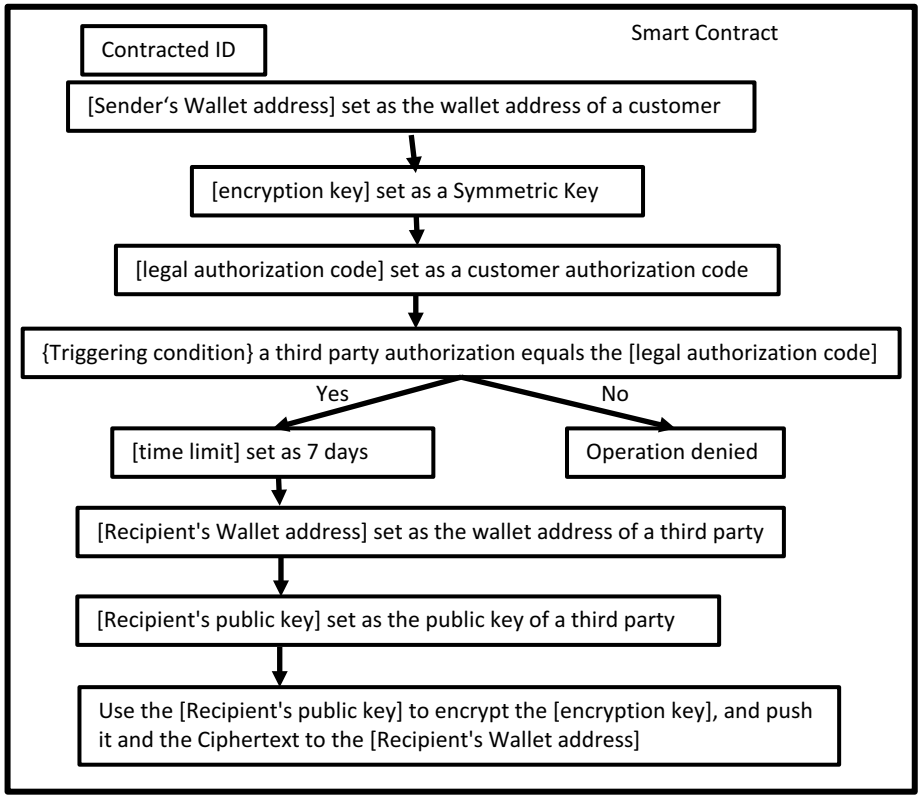
LTSA uploads the Ciphertext and its signature to the blockchain, we may conclude from the following figure that whenever a Ciphertext has been tampered, its corresponding Hash value will be inevitably affected, thus further affects the Merkle root value, as a result, miners who maintain the chains will identify such a problem and will reject the block's inclusion into the chains, such a procedure ensures that a Ciphertext will be tamper-proofing.



Step 5

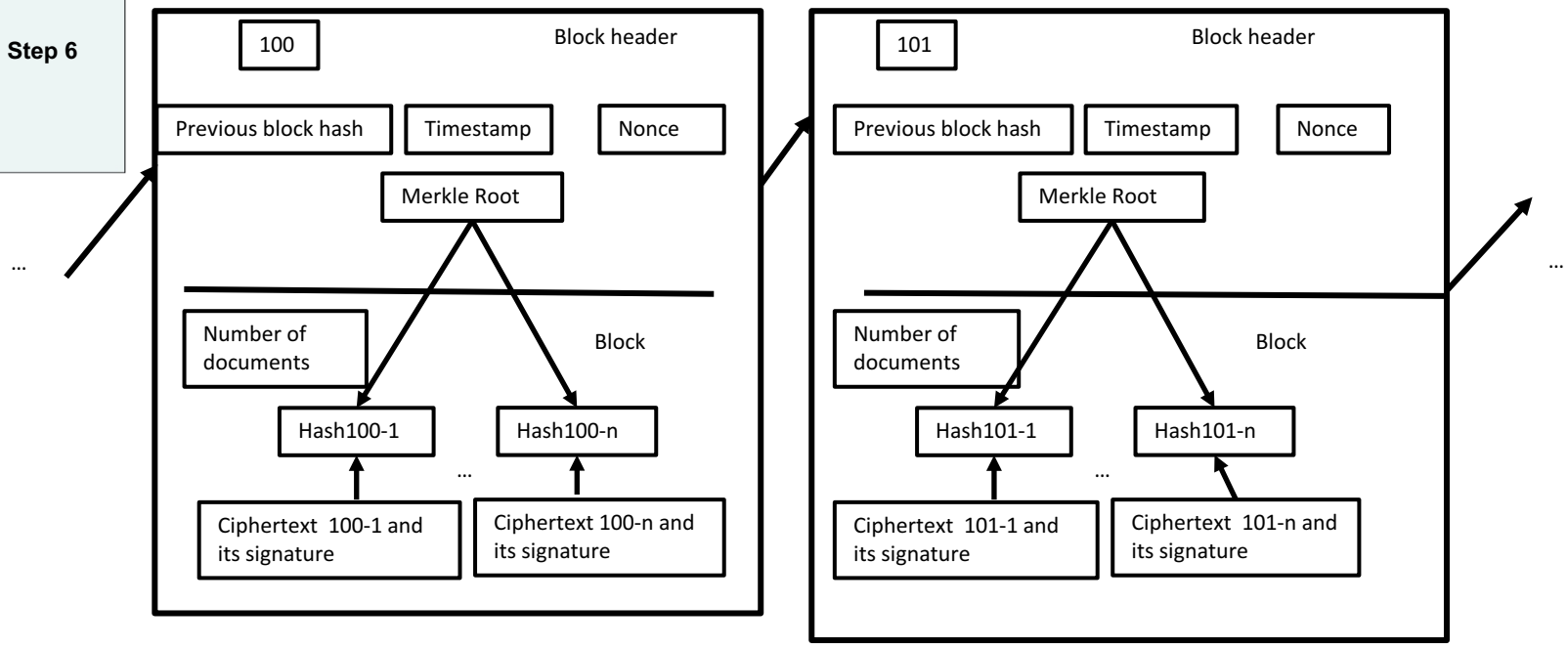
The blockchain platform automatically generates smart contracts according to the customers' document and data, and sets the basic parameters (as shown in the following figure). A smart contract is a piece of codes in essence, and it operates as follows:

When the authorization codes received by the LTSA equal the authorization codes of the customers, LTSA automatically sets a time limit, and sets the wallet address that receives data as the wallet address of the corresponding third party, and encrypts the symmetric key using the public keys of such third party and pushes such digital envelope and Ciphertext automatically to such third party.



Step 6

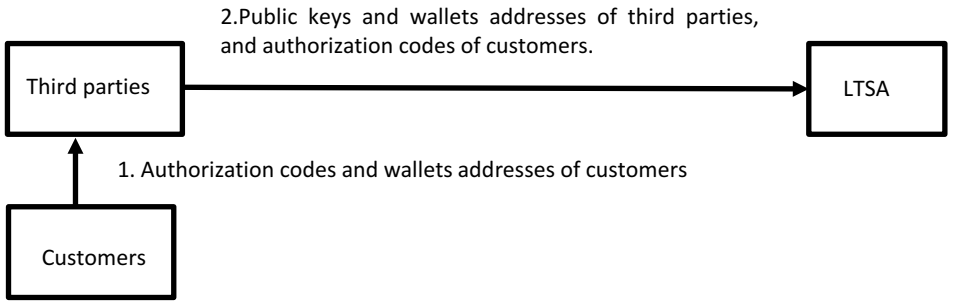
The chains maintained by the LTSA system are as follows, each of the blocks in the following Figure stores multiple Ciphertexts and corresponding signatures of different customers.



4. Verification by Third-Parties

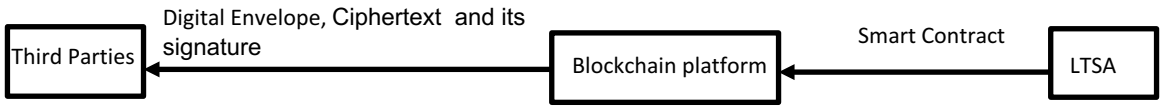
Step 1

A third party obtains the authorization code and the wallet address of a customer, and sends its own public key and wallet address, together with the authorization code obtained to LTSA, and LTSA automatically accesses the blockchain and executes the smart contract based on the wallet address of the corresponding customer.



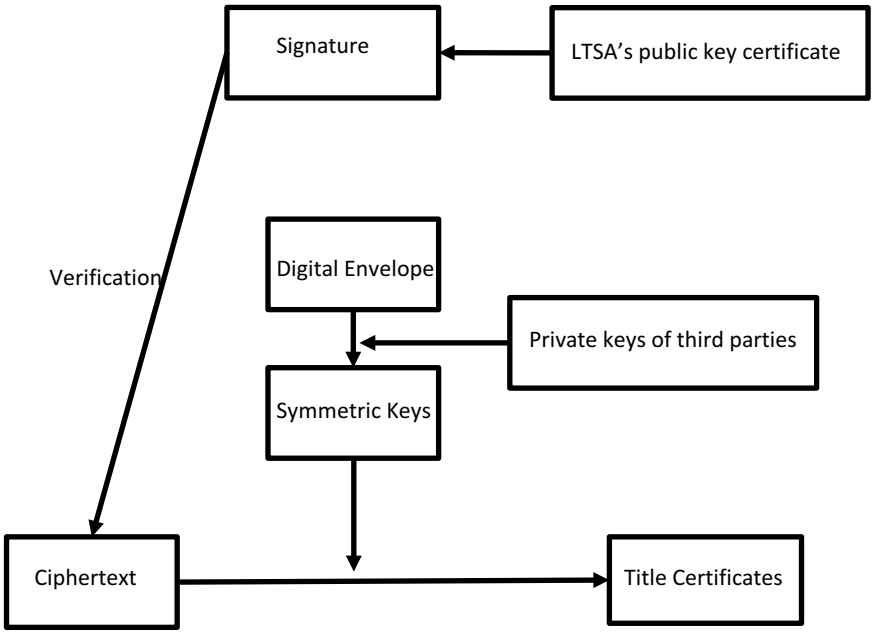
Step 2

During the execution of a smart contract, data sent over by a third party will be entirely filled into the contract automatically, triggering the contract conditions and executing corresponding sub-processes. Verification by a third party ends when failed to trigger the contact conditions, otherwise, the blockchain platform automatically pushes the digital envelope, the Ciphertext and its signature to a third party.



Step 3

Third parties verify the signature through LTSA's public key certificate and the Ciphertext to confirm the signer is LTSA indeed, and obtain the symmetric keys by the use of their private keys to decrypt digital envelopes within a specific time period, thereafter, third parties use the symmetric keys obtained to decrypt the Ciphertext, and at this point, third parties run a calculation on the digest value of the 1st layer of an eSTC, the eSTC will be acceptable if the calculation result equals the digest value in the 3rd layer.



5. Exception Handling

Loss of Mobile Phones and Software Compromise

Repeat the procedures under Customer Identity Authentication and Issuing an eSTC.

Forget the App logging password

Reset password through mobile phone SMS verification.

Title Certificate revoked by LTSA

Add a field for the Ciphertext to label the revocation status of the Title Certificates.

Changes in the registration of the Title Certificates

Re-issue the Title Certificate, even if the certificate cannot be revoked, the most updated certificate can still be obtained by tracing the blockchains.

6. Security Mechanism

- LTSA strictly implements identity authentication on customers;
- Binding customer identifications to digital identities;
- LTSA issues encrypted data and publish on the blockchain to ensure security and non-repudiation;
- Only authorized third parties may access the encrypted data by using the authorization codes;
- An eSTC is verified by LTSA and its authenticity guaranteed by LTSA.

7. Key Strengths

- Tamper-proofing by leveraging the blockchain technology;
- Adopting the digital identity authentication technology with high LOA.
- Enhanced privacy protection: Customers may authorize anyone to access the eSTCs anytime and anywhere without the involvement of LTSA.
- Cost-effective

Thank you!

Contact us:

Mr. Xiu
E-mail: jxstones8@gmail.com / xiulei@gdca.com.cn
Tel: (+86) 13580594895 / (+8620)-83487228
Website: https://www.gdca.com.cn/