DIACC Digital ID Design Challenge Paper

October 31st, 2017

Written by:

Yori Ding
Stephen Thompson
Jagriti Sona Sharma
Calvin Chu
Joshua Matettore

Introduction

This paper presents and evaluates a blockchain and a non-blockchain design solution to the Accessing and Distributing Electronically Delivered State of the Title Certificates Challenge. The design solution aims to improve the current system's efficiency for accessing, sharing, verifying, and trusting Electronic State of Title Certificates (eSTC) for customers and third-party participants of the Land Title and Survey Authority of British Columbia (LTSA).

This paper begins by explaining the current system that British Columbia follows and the challenge it presents. It further explores the opportunity to develop solutions on blockchain to address the issue, by looking at the benefits and drawbacks of the same. Later, it elaborates on how a non-blockchain solution can be quicker and cheaper to implement and provides an in depth reasoning and detailed arguments as to why our team would recommend a non-blockchain solution over a blockchain solution in this context.

Brief Description of the Challenge Problem

Original case - In situations where a customer loses or misplaces the original PDF of their eSTC, it creates a problem for both the customer and LTSA. The certificate number and access code can only be found on the original PDF. And LTSA has no ability of retrieving the certificate number and access code after it has been issued. The customer who can't access their eSTC must submit (or pay for) a new eSTC.This, however, creates dual inefficiency for LTSA: 1. It is impossible to recover eSTC without access to the original PDF 2. Lost certificates consume hard-drive space because they will remain in storage for the remainder 12 months period for which they are valid, even if the LTSA Certification Access Service is not being used.

Third parties such as banks and law firms, due to security reasons, are unable to rely on previous trust points of LTSA mail and uniquely colored paper that are delivered electronically. Also, third parties feel they have no mechanism of authenticating the eSTC PDF. The current problem with sharing and verifying of eSTC is that some third parties do not accept a printed copy of the certificate, or an email with the hyperlink or PDF.

Possible Blockchain Solutions and its Limitations

Blockchain represents a list of records/transactions that have been verified by decentralised nodes that participate in the network. Any centralised *application* can be built on blockchain or on a centralized server. We now explore various possible solutions that could replace the current system and why a centralized server would be better choice.

When initially working on this challenge, our team discussed various methods that a certificate could be shared on a decentralised platform after being added on the platform by the government. As the government is the only authority that can verify and distribute the certificates, the government must broadcast a hash value representing the certificate on the blockchain to state the validity of the document. Firstly, however, all transactions on blockchain are transparent and anything stored on Inter-Planetary File System (IPFS) is completely public. This can be overcome through a Hyperledger blockchain model and writing additional controls on top of IPFS.

Our team developed a solution using an open-source framework and toolset: Hyperledger Composer. Its key concepts are defining the eSTCs as assets, participants as individuals or companies, transactions as the exchange of eSTCs, digital identities and IDs are given to participants, events as the exchange of certificates and queries as the request for the eSTC. (Hyperledger Composer)

An issue presented is that if an individual requests an Electronic State of Title Certificate, regardless of the number of nodes on the blockchain to verify the request, it remains unverified until the government endorses the claim. Since the government has the authority to call the final vote, the trust in the system is centralised. Blockchain distributes trust among the network instead, wherein no central entity can outright influence the transaction claim or control the blockchain, unless an entity controls more than 50% of the system. If the government needs to be sole key source of trust, it may not be effective to use a blockchain application for a simple system.

One possible solution to overcome the transparency issue and centralisation issue would be to create a blockchain using Hyperledger, in which an individual could be digitally identified by the government and request for an eSTC. When the government issues it, only the individual can keep a copy of the certificate and it gets deleted from the government side. In this situation, if the third party wants to view the certificate they will have to view it through the individual's computer, which will be hosting it and that will require him/her to be online. A central server would be required constantly remain online, which is one of the reasons we would not recommend this model for such a system.

Although blockchain solution does have many advantages and uses in improving the effectiveness of the LTSA, the drawbacks and incompatibility with the current issues of the situation outweigh the decision to implement. If the issues or goal of the solution were different, there may be a variety of blockchain solutions that be much more appropriate. Thus, rather than implementing a complete blockchain solution for the LTSA, other methods could prove to be more effective.

As land can either be owned by a corporation, individual or separate entity, this requires the centralized role and authority of the government to be embedded into the system. Thus, when blockchain applied to the current system, there may be flaws that cannot be fully addressed and cause inefficiencies. Overall, blockchain as a solution would be expensive and unnecessary in this situation where centralisation and transparency are not the key issues that needs to be addressed, rather it is cost-effectiveness and digital identity verification are.

Proposed Solution: LTSA implements a Repository and a PKI

This solution can be governed by trusted authorities by two platforms: a repository at LTSA that stores the eSTCs to which authorized stakeholders can access, and a public key infrastructure (PKI), run by DIACC, that identifies each individual eSTC to the owner of the title. This solution is decentralised as there is no single authority that runs both platforms but, also, does not require a blockchain.

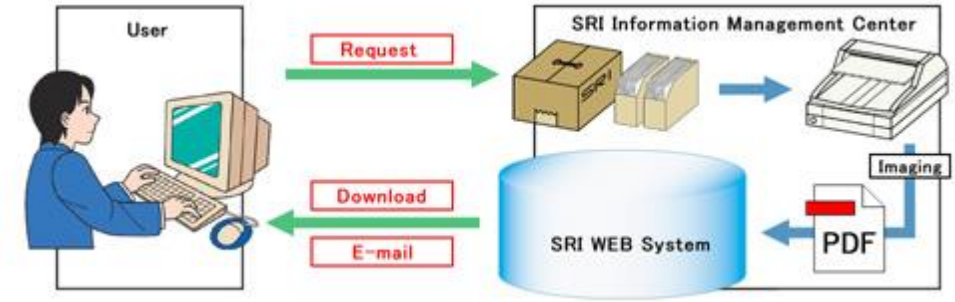
Repository

Repositories operate as a bridge between the data and the stakeholders who will be consulting the system from different locations i.e. the title owners who will be consulting the LTSA's repository of eSTCs. The repository will be part of the LTSA Certifications Access Service that runs a data storage facility that holds eSTCs at the back end for the title owners.

The repository would run as the facility's front end, acting as a clearinghouse for requested eSTCs.

The diagram, below, is taken from a third party but it depicts the way in which title owners can retrieve their documents.

1. The user (in our solution, the title owner) sends a request for the retrieval of his eSTC to the LTSA Certifications Access Service;
2. The SRI Information Management Center (in our solution, the LTSA Certifications Access Service) processes the request and checks its data storage facility to see whether the eSTC being requested will match the identity of the user;
3. If the request matches the document in question in the LTSA's facility, the LTSA Certifications Access Service will retrieve the PDF and send it to the eSTC repository (represented in this diagram as the SRI Web System). From that location, the PDF can be pulled by the user's mail server;
4. The user's mail server downloads the PDF and the user retrieves it from his machine.



From https://www.sri-net.co.jp/storage_eng.htm

PKI

The public key infrastructure "is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption." (Opinions)

THIS SECTION IS ADAPTED FROM STEPHEN THOMPSON'S REPORT "BLOCKCHAIN HELP OR HYPE"

PKIs can come in the form of key management servers or centralized directories. They combine software with a management process that, according to the CGI's 2004 White Paper (2004, p. 10-11) on public key encryption, covers the following operations:

- the creation of the key pair – the key pairing resemble a set of keys that unlock a safe. The private key unlocks the safe while the public key locks the safe. In order for the user to decrypt his eSTC from the LTSA's repository, the user creates a private-public key pair by running a key generation algorithm from the DIACC's PKI.
- Creation of digital certificates – certificates verify the digital signature by displaying the link between the user and his public key. In those systems that issue certificates, the signature is known as a "qualified digital signature". They produce the validity period, the signature algorithm, a serial number and the name of the certification authority. These validity periods can be of a long duration and they also rely on the sustained readability and integrity of the signatures. Alternatively, the validity period can be tied to that of the OTP (one-time password).

- Private key protection – in key pairings, the private key is encrypted (will be stored with DIACC) while mathematically linked to the public key which is unencrypted (on DIACC and displayed on the eSTC PDF). Despite being linked, it is computationally infeasible to deduce the value of the private key from the value of the public key.
- Certificate revocation in the event of a compromised private key – once a user's certificate has been revoked, the PKI will preserve the certificate on a database accessible to all users in the network so that it cannot be re-used. This attempts to deal with a problem that Kohnfelder (1978, p. 16) identified: a public file encryption function has a single point of failure. Once breached, the attacker can pass encryption functions that are bogus. He also stated that updating such a large system would be expensive and inefficient.
- private key backup and recovery – if the user loses his private key, any eSTCs encrypted with that key will be lost. So, the PKI needs a backup and recovery mechanism for lost private keys,
- key and certificate update – this is a mechanism for the renewal of expiring digital certificates. DIACC's PKI can achieve this by carrying out the renewal automatically or notifying the user himself to carry out an operation that updates the certificate. The idea behind fixed expiry dates is to mitigate against incremental damage to the network's integrity due to corrupted public keys.
- Key history management – following a key update that generates new key pairs, history management makes it easier for the user and the LTSA alike to determine which private key to use for decrypting files.

For our solution, the PKI can be run from DIACC as a plug-in to the LTSA Certification Access Service. It will most likely be a closed PKI so that it will be compatible with the proprietary software the LTSA will be using to run its Certifications Access Service.
In the diagram, the user would be the land title owner who holds an eSTC along with the private key that will decrypt it. An independent Certification Authority (CA) is a key feature of PKIs. The PKIs themselves are a unit of organization that does not, of itself, validate keys. The validation is a process carried out by the CA as the trusted third party. So, in our scheme, the CA issues the public key certificate to the DIACC PKI. The DIACC PKI relays the certificate to the LTSA who can then verify it against their record of eSTCs in order to ascertain the user's ownership of the eSTC.

In order to promote efficiency, the DIACC can generate an identifier for the public key certificate, possibly as a QR code or some other machine-readable format. The QR code embeds the user's public key while DIACC's PKI can hold the user's public key and private key. Either the DIACC or the LTSA can impress this QR code onto the eSTC PDF so that, should the PDF ever be printed, the certificate itself will remain readable when scanned. The CA would hold the digital original until the validity period of the key lapses.

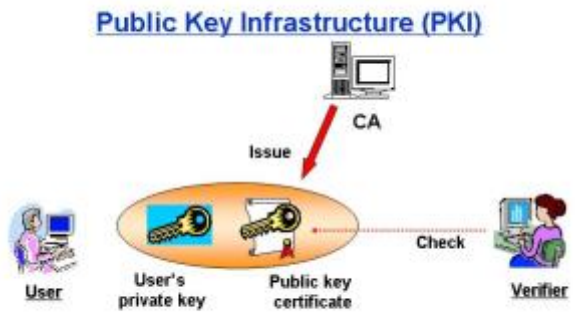


Figure from http://www.writeopinions.com/public-key-infrastructure

The legal ramifications of this solution concerns primarily the management of handling sensitive data on the government's proprietary systems, as well as cooperating with various government agencies efficiently. Governments often reinforce strict controls over its data, which may cause friction with the practical implementation of the PKI system as there may be security concerns or time lags due to lengthy approval times. Additionally, government procedures and bureaucracy could undermine the effectiveness of the PKI system if security concerns are not properly addressed, for example incorporating two-factor authentication would alleviate some of security concerns about user access. Another example is developing a closed PKI rather than an open PKI, which may be more resource consuming but significantly reduces risk.

Benefits of our solutions:

A major advantage of a closed PKI is the secrecy of its code. This is significant in a state-run repository with the DIACC public key infrastructure plugged in. (Hiavaty) The code is not readily available to the public. As a result, it is safe to assume that a closed PKI is more secured, although it is difficult to be completely secured because of electronic transaction.

Another major advantage is risk management. For instance, LTSA can issues eSTCs to whomever that are verified by the government. This gives LTSA the advantage of predicting (or in some cases, control) the losses (if any) to their database.

The advantages of having a repository is that it will provide a clean platform on the current existing one (LTSA) without worrying about the details of where the data is going and how it's coming back. A repository is both cost effective and less time consuming. When a user sends a request for his/her eSTC from the LTSA Certification Access Service, the repository minimizes and reduces the costs by imaging requested certificates. This reduces the financial burden for the LTSA. Orders are easily accessible through the LTSA website. Cost is further reduced because data is stored electronically without the need for office space. Data integrity is extremely important; therefore, sensitive data are kept securely within the LTSA Certification Access Services. With this in mind, downloadable PDF versions of eSTC can be quickly accessible online. This saves time for both the user and LTSA especially as it reduces time-consuming labor work to retrieve the eSTCs.

The general trend of making physical copies into digital has definitely revised the way we manage data. This can influence multiple sectors, from large IT sectors to government to the cost of human labor. The economic benefits can be limitless with this new adoption of storing secure data electronically. To just name a few, generation of innovative ideas, less time-consuming labor-intensive work, facilitate better data flow and deeper policies, etc. Beyond just economic benefits, by going digital, it opens up a wide variety of social implications.

Limitations of our solution:

Although secrecy of its code is a major advantage for a closed PKI, the code is not put under public eye, therefore it is difficult to know whether or not the code and the components behind PKI are truly safe. This could mean be possible disconnections between the government and DIACC PKI. According to the current guidelines on the management of PKI in Canada: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=20008

The PKI policy was established by “which the Governance of Canada (GC) would electronically authenticate the identity of entities or persons and enhance the integrity and confidentiality of documents”. This might remove the disconnections between PKI and the government.

LTSA could be liable for the software installation, problem, troubleshooting, and the cost of maintaining and updating the software. Maintenance can be an issue. If the software on the internal machines needs to be upgraded, the external machines probably need to receive the same upgrades or else there could be compatibility issues. If any system failure occurs, you as the user is relying heavily on the government’s ability to keep the repository model alive. And when all eSTCs are stored in a single storage area, this can be a major risk factor.

In terms of accessibility, if a customer’s private key is stolen, the thief could use that key to generate numerous fraudulent eSTCs and issue them to unwitting customers. However, in order to protect the customer's’ private key, it is important for customers to store it elsewhere and protect it with a password. LTSA should resort to the use of 2 factor authentication by seeking the username, password, and OTP to verify the users. OTPs are used by means of text message or hard tokens as a second factors of authentication.

Conclusion

The LTSA’s current eSTC system can be considered effective to an extent, however as this paper discussed, there are many other solutions that can improve the efficiency for accessing, sharing, and verifying eSTCs. As presented, a blockchain solution could possibly increase the effectiveness of the current eSTC system, optimally using IBM’s Hyperledger frameworks and toolsets. The blockchain solution, as a novel form of addressing network security, is not however the most compatible nor effective solution, primarily due to the nature of the issues and the infrastructural design of the eSTC system. Even for blockchain frameworks built for business applications, such as Hyperledger, the design of issuing and verifying digital certificates have different flaws and issues that blockchain itself does not effectively address.

As proposed in this paper, a more effective solution would be to implement a repository to authorize access and a closed PKI for user identification. This solution address this issues at hand in a more direct manner, while retaining a few key elements of a blockchain solution, including decentralization, encryption using public/private keys, digital certificates, and hashing algorithms. Thus, this solution focuses on addressing the four network security issues of data integrity, data authentication, confidentiality, and non-repudiation in a procedure that suits the nature of managing eSTCs. Overall, the key implications and drawbacks of a closed PKI and managed depository solution may be deemed highly suitable and practical, though not completely perfect, for the LTSA to implement.

References:

"Key Concepts in Hyperledger Composer." Key Concepts | Hyperledger Composer, Github, 2017, www.hyperledger.github.io/composer/introduction/key-concepts.html

"Opinions on Public key infrastructure." WriteOpinions, WriteOpinions, www.writeopinions.com/public-key-infrastructure.

Hiavaty, Philip. The Risks Involved With Open and Closed Public Key Infrastructure. SANS Institute, The Risks Involved With Open and Closed Public Key Infrastructure, www.sans.org/reading-room/whitepapers/vpns/risks-involved-open-closed-public-key-infrastructure-882.