DIACC Design Challenge Submission

Submission Overview

Submitted by: Noah Bouma, OnePair Technologies
Email: noah.bouma@gmail.com **Web:** onepair.ca **GitHub:** boumba100

Solution Abstract

The proposed solution architecture for the LTSA eSTC is a decentralized electronic certificate issuance, registration, presentation, and verification scheme using verifiable claims model and the blockchain as a registry. The architecture allows for independent apps for electronic State of Title certificate: issuance/registration (LTSA app), storage/presentation(customer app), and verification (third party verification app). A prototype of the customer app has been developed (Android) using the BlockCerts standard. The app proves out the functionality and viability of the primary components of the solution architecture and demonstrates usability and convenience. The architecture has also been designed using standards to fit into a larger ecosystem of digital identity, while ensuring privacy and security. Finally, the implementation uses open source and standards, which enables LTSA to explore numerous opportunities to enhance its existing services, or consider alternative and innovative approaches.

List of Deliverables

The following table lists the deliverables that comprise the submission, as part of DIACC Digital ID Design Challenge ("DIDC). In accordance with guidance, this document (No. 1) shall be considered for evaluation, the primary submission deliverable, to page 15 (as per submission instructions of 15 pages PDF). A slides presentation has been included (No.2) that summarizes the submission content for presentation and discussion purposes. Other supporting deliverables, videos and sample certificates have been included for the benefit of evaluation.

No.	Title of Deliverable	Deliverable Type
1	DIACC Design Challenge Submission (this document)	Primary
2	DIACC Design Challenge Presentation	Supporting
3	DIACC Design Technical Overview Video	Supporting
4	Design Challenge Solution Overview Video	Supporting
5	Example of State of Title Certificate with QR Code	Supporting
6	A working version of demonstration prototype is available upon request.	Supporting

Understanding the Problem

The Land Title and Survey Authority of British Columbia (LTSA) is responsible for operating the land title and survey systems of BC. These systems provide the foundation for all real property business

and ownership in the province. In accordance with legislation, the LTSA system registers land title interests and survey records. Using this land registry, the LTSA provides services that are an essential underpinning to BC's private property market, civil justice system, civic governance, taxation and, Crown land management frameworks.

The LTSA service relevant to the DIACC Digital ID Challenge (DIDC) is the land title registration service along with the associated services of accessing and distributing electronic State of Title Certificates (eSTC) that are issued to authorized customers and third-party participants. An eSTC provides documentary evidence of the right of ownership of real property and is used by title insurance companies to ensure good title and to list encumbrances such a liens or easements before approving mortgage loans.

Currently, there is an online eSTC service where organizations can apply for and receive certificates (https://ltsa.ca/). There is also a certificate access service (https://apps.ltsa.ca/srs/public#/cert) where electronic copies of certificates can be access for verification purposes.

The design challenge identifies high-level "pain points" that can be use to map back key considerations and design objectives. These pain points are summarized below.

Pain Point 1: If an authorized user loses the original PDF certificate (along with the certificate number and access code) they cannot validate. The valid copy on the system becomes 'orphaned' taking up space on the system, and the user must request another copy, taking time and process resulting in a duplicate on the system.

Pain Point 2: Electronically sharing of the certificates makes it difficult to verify the authenticity of the certificate. While there is a verification hyperlink in the PDF (a phishing security risk), many institutions will not accept the electronic and still require a paper copy.

Proposed Solution

This section discusses the key challenges and opportunities for LTSA, which then are used to generate design objective and the solution architecture for LTSA, leveraging blockchain technology and digital identities. (Note: It is assumed that the reader is familiar with these concepts to understand their potential application.)

Key Challenges and Designing for Opportunity

This section highlights key challenges identified in use case and discusses how technical, business and ecosystem opportunities can be realized in adopting blockchain-based/digital identity technologies and services.

Reducing Friction

Challenge: Participants that interact with LTSA must register for an account or use an online service. Participants, such as third parties, may find this problematic because they require infrequent, but

essential access to verify state of title certificates.

Opportunity: Reducing friction for the users of the LTSA system and for the third parties that must verify the state of title certificates to conduct business (insurance, mortgages, etc.)

'Friction' is simply the barriers and/or costs associated with using a system for the first time or subsequent time. In reviewing the LTSA, this 'friction' comes from two sources:

1. **Digital Identity Friction** - this relates to issue of identifying the business applicant and the individual acting on behalf of the business. Once the application process is completed, the identified business/individual is authorized to request eSTCs and to provide these eSTC to third parties, such as banks, and land title insurance companies.

2. **Claims Verification Friction** - this relates to the issue of verifying and relying on claims that are broader than digital identity. In this use cases, this is the verification of a state of title (including encumbrances) as registered by LTSA.

Digital identity friction is significant for LTSA, but for the purpose of this submission, the friction is best reduced by taking advantage of using the emerging standard-based digital identity and authentication process being put in place by the provinces, such as the BC Services Card and My Alberta Digital Identity. Since the LTSA exists in a larger ecosystem services, its focus should be on providing and verifying state of title certificates, and the existing LTSA services and apps should be evolved to adopt standardized digital identity and authentication services as they become available.

The primary benefit for LTSA is to improve the certificate issuance, distribution and verification process. Thus, the emphasis of the solution design is aimed toward reducing claims verification friction, or in other words, making it easier to issue, distribute and verify state of title certificates. By focusing on improving the central function and mandate of LTSA using blockchain technologies, there are significant benefits of streamlining and enhancing the integrity of eSTC services.

Reducing Administrative and User Burden

Challenge: The current LTSA system requires account registration and requested certificates must be generated and stored as copies on a centralized service. This requires time, resources and costs.

Opportunity: Reducing burden for administration of the LTSA system and users of the system.

As discussed earlier, the eSTC services should leverage standardized digital identity services. Regarding the eSTC services, a decentralized approach using blockchain is proposed, which will reduce (eliminate) the requirement to have a centralized service that stores copies of, and validates certificates. Instead, the proof of issuance of the certificate can be registered on the blockchain, and an app can be developed to manage the secure storage and recovery of certificates.

Increasing Security and Privacy

Challenge: The current system has a validation service, that if someone gains access to the certificate number and access code, they can view the entire contents of the certificate. This is a significant security and privacy risk.

Opportunity: Reducing to near zero (for LTSA) privacy and security risks by creating a decentralized validation service that uses zero-PII (personally identifying information) cryptographic proofs instead of a centralized service using that requires the transmission of PII.

There are several privacy and security concerns with the existing eSTC service. The embedded link in the PDF certificate provides an opportunity for hackers to produce bogus certificates with malware links that can be clicked on by an unsuspecting user. Even a legitimate PDF certificate provides opportunities for hackers: the link provides an opportunity to gain access to a legitimate certificate that could be used in a fraudulent transaction. The additional information gained from the certificate could be used to support other attacked.

To address these security and privacy issues, is to remove any and all personal information from the verification service. Further, the verification service can be mediated through a cryptographic proof (with zero-PII) registered on a blockchain. The distributed nature of the blockchain (i.e., many duplicate copies) enables multiple endpoints. As well, the app, through a peer-to-peer protocol, can carry out the verification function with no dependencies. Finally, by ensuring that any personal information, is delivered, only to the authorized user (no copies stored elsewhere) and providing a secure storage management and certificate presentation and verification function greatly increase privacy and security that is under the direct control of the user.
In developing the services and application, the code will be open source to ensure defects and security vulnerabilities rectified as soon as possible. The application and code will also be subject to the relevant security and IM/IT policies and frameworks such as the BC IM/IT Standards.

Finally, the principles of Privacy By Design (PbD) are employed. PbD's seven foundational principles enable service without data control transfer from the citizen to the system, the citizen is in the centre of all transactions, all personal information is mediated through the user, and no personal information is leaked through other processes.

Ensuring Authenticity of Certificates

Challenge: The current system, while electronic, still relies on human interaction to visually verify the certificate and contents. This is a potential for human error and/or fraud.

Opportunity: Ensuring digital authenticity of the the state of title information contained in the certificate.

The current eSTC scheme relies on humans to visually carry out the verification process. The PDF provided to the user, must be visually compared with the copy stored on the server. This requires human attention, sustained due diligence (especially if several certificates must be verified for a transaction) and therefore subject to error and potential fraud.

The approach used in the solution design uses the Blockcerts standard to cryptographically guarantee the integrity of the certificate (i.e., nothing has changed or been tampered with), and the verification process is fully electronic. If so required, the verification process could be added to an audit log to indicate when a certificate was verified.

Preventing Improper or Inconsistent Use

Challenge: The current system does not have in place, robust controls to ensure that recipient of the certificate is the only party that can present to another party for verification. Once presented to another party, there is no way to prevent improper or inconsistent downstream use by unauthorized parties.

Opportunity: Preventing improper use of the state of title certificates.

The current process is fairly weak and relies on the relative secrecy of the certificate number and corresponding access code. Several options can be considered to strengthen the process, including developing an app that manages the transmission and verification processes; including a public key of the recipient that is used by third party to challenge ownership before verifying the certificate. Finally, if required, the contents of the certificate can be encrypted, and only decrypted before verification.

Eliminating Downstream Dependencies

Challenge: The current system requires a centralized online service and copies of the certificate to be available for parties to validate the certificate. This availability poses an additional cost to maintain a high level of service for infrequent users of the system.

Opportunity: Eliminating dependencies for the downstream business processes that rely on the state of title certificate. Instead, Instead, use standards-based protocols and eliminate requirement for centralized services.

Downstream dependencies can be considered along two dimensions: time and other parties. In terms of time, there may be a requirement for the certificate to be verified years (or decades) after its issuance. The current scheme, allows only for a year (before the certified copy is removed from the system). A blockchain-based approach can assume that the underlying blockchain (as in Bitcoin blockchain) will alway exist, even decades into the future, thus a verification scheme, will also exist into future. In terms of other parties, the verification function may be required by an expanding set of participants, the blockchain approach and distributed ledger allow for the verification of the certificate by separate and independent systems.

Solution Building Blocks

Blockchain (including Cryptographic Techniques)

The term ‘blockchain’ generally refers to scheme of related methods: i) a cryptographically linked list of ‘blocks’ or data structures, which are ‘sealed’ using a cryptographic techniques of one-way hashing and proofs (SHA256, and merkle trees) , ii) a distributed consensus method of maintaining the list, such as proof of work (PoW), and iii) a distributed ledger that can securely maintain a unit of account

(e.g., cryptocurrency) or state (smart contracts) over many instances. In a public permissionless blockchain, the "miners" would be incentivized to maintain the blockchain using a competitive PoW scheme with cryptocurrency rewards.

Verifiable Claims

A *verifiable claim* is a qualification, achievement, title, or any piece of information about an entity (individual, organization or property) that can be verified or vouched for by any recognized authority. For example, a person's name, as vouched for by the vital statistics registrar, or a state of title, as vouched for a land registrar (this is the case of the LTSA)

Blockcerts

BlockCerts (www.blockcerts.org) is an open standard developed by MIT Media Labs for creating and issuing certificates that can be verified using the blockchain. BlockCerts standard is designed to give control of a tamper-proof electronic certificate to a recipient, who then can present this certificate to any third party, who in turn can perform a verification that is independent of the recipient and the issuer. This is achieved by registering a cryptographic proof on a blockchain, in such a manner that this proof does not contain any personal or identifying information). The initial use case for the BlockCerts standard in for the independent verification of academic credentials, however, the standards-based approach applies equally well to the LTSA use case.

Digital Identification and Authentication Ecosystem

A key requirement of systems of record and transactions is that the identity of the user must be confirmed and established (identification) before granting any rights or privilege. When the user accesses the system must confirm that is the same person (authentication) Traditionally, these capabilities have been developed on a system-by-system basis (as is the case with LTSA), but are now evolving to federated and more recently, decentralized architectures. The goal is to integrate into the larger digital identity ecosystem enabled by the DIACC Pan-Canadian Trust Framework. Recently, cryptographic techniques now standardized by the FIDO Alliance are enabling the self-registration of authentication tokens and the ability to authenticate these tokens using a decentralized cryptographic challenge and response protocol.

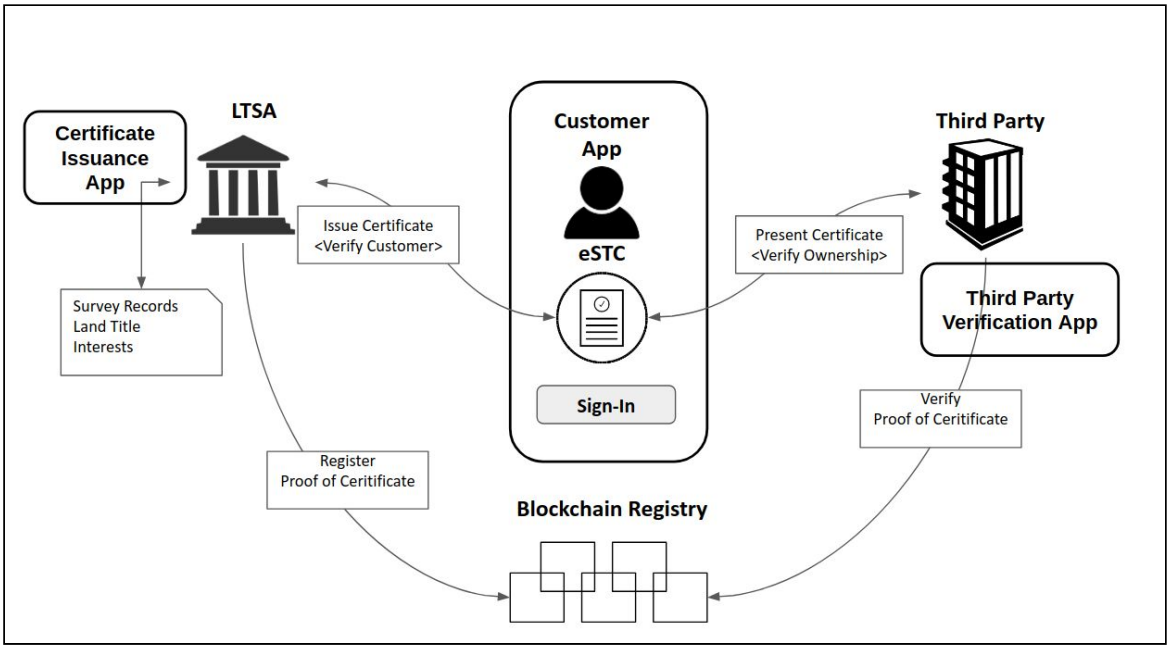
Open Source and Standards-Based Approach

Open source is software for which the original source code is made freely available and may be redistributed and modified. Standards-based approach means the use of accepted standards in the building of solutions. Both open source and standards-based approach are crucial to ensure that any software and system can be freely inspected and modified to suit the needs of the business, fix errors, and address security issues. Further, these systems must must open, not proprietary, as over the longer, the goal is to operate in a larger ecosystem that provides a choice of capabilities (e.g. digital identity, etc.)

Solution Architecture

The solution architecture is based on a Twitter Thought Experiment using verified claims as proposed by Tim Bouma and Anil John in July 2017. This scheme, adapted for the LTSA use case is

illustrated below. The solution architecture uses the building blocks and patterns discussed in the previous section. The architecture also takes into account the Privacy by Design's root principle that enables service without data control transfer from the citizen to the system. In this architecture, the user is in the centre of the transaction, all personal information is mediated through the user, and no personal information is leaked during the issuance and verification processes.



Independent Actors

The architecture defines three independent actors, whose actions are eventually coordinated via the blockchain registry.

- **LTSA as Issuer.** The LTSA is the authority that issues state of title certificates based on the land register. Before issuing certificates, the LTSA must verify its customer.
- **Customer as Recipient.** The customer of LTSA, once registered and authorized, can request and receive state of title certificates. These certificates, under the control of the customer, are presented for verification.
- **Third Party as Verifier.** A financial institution or title insurance provide, verifies the state of title certificate when it is presented by an authorized customer.

Blockchain Registry

The blockchain, or distributed ledger is used as the register of certificates. The blockchain is cryptographically secure, distributed store of transactions that can be used as an open and independent registry where anyone can independently verify a certificate. When a certificate is issued and provided to a recipient, proof of its existence is registered on the blockchain. Aside from providing the certificate to the user, no personal information is disclosed or stored elsewhere once the issuance is completed, and no personal information is recorded on the blockchain - only one-way hashes and cryptographic proofs. For broadest access, a public, permissionless blockchain can be used (e.g., Bitcoin blockchain). Other blockchain platforms (private and public) can be considered, such as Ethereum and Hyperledger.

Blockcerts Standard

The Blockcerts standard provides the cryptographic mechanics of creating, issuing, registering and verifying a certificate using the blockchain. The eSTC would be implemented using this standard. When a Blockcerts certificate is issued, its data is compressed into a hash and logged on the blockchain generating a “receipt” that can be used to independently verify the certificate at a later date.

Independent, Open Source, and Standards-Based Apps

The solution architecture uses the blockchain, and the Blockcerts standard. Thus, the implementation of the solution architecture can be broken into separate and independently maintained apps using open source and standards . This openness and independence allows the solution architecture to evolve into an adaptive ecosystem to support eSTC certificates, but can expand into other sectors depending on demand. Since the standards and implementation are open source, the apps can support a variety of platforms: Android, iOS, web services. Finally these apps can be white-labeled as components into industry-specific apps or services.

The app architecture consists of three independent apps:

- The **Certificate Issuance App** is used by the LTSA to generate certificates using registered land title interests and survey records. This app can be developed by the LTSA using the Blockcerts Standard and open source software.

- The **Customer App** is used by the authorized LTSA customer. This app (also open source) can be used to enforce the conditions of the customer agreement, such as signing in, before requesting a certificate.

- The **Third Party Verification App** is used by third parties such as financial institutions or title insurance providers. Like the other apps (open source) it can be independently developed and tailored to the requirements of the third parties. This app validates the signature of the issuer and the certificate data and also ensures that the certificate status has not expired or been revoked. The verification app can have additional controls in place to ensure that the presenting party of the certificate is the same as to whom it was issues.

Generic Service Patterns

The solution architecture specifies the generic service patterns that need to be implemented within the apps or services.

- **Issue Certificate** - the certificate issuance app retrieves the necessary information from the land registry, generates a Blockcerts standards compliant certificate that cryptographically seals the information within the certificate and signs it with the issuer public key. The certificate includes the eSTC information, and optionally, a public key of the authorized customer so that they can be challenged during the verification process.

- **Register Proof of Certificate** - When a certificate is issued, its data is compressed into a hash and logged on the blockchain. This generates a "receipt" that can be checked at a later date.

- **Present Certificate** - the customer app can present the certificate through a variety of electronic, option and physical means. Mechanisms can be a simple as an email attachment, upload to a secure endpoint, near field communication (NFC) or QR code. The QR code can also be printed to paper or PDF, mailed or emailed in, and electronically verified. This process can also have a challenge-response protocol using the customer's public key included in the certificate. The challenge would need to be met using the corresponding private key of the user (in hardware or software)

- **Verify Proof of Certificate** - the verification service validates the signature of the issuer, the certificate data and ensures that the certificate status has not expired or been revoked

- **Wallet Functionality (optional)** - the popular paradigm that is emerging for mobile applications is the notion of a wallet. Not dissimilar to the traditional leather wallet, the mobile wallet model was popularized by Bitcoin wallet providers. In addition to cryptocurrency, the wallet model can be extended to include storage of personal information, and certificates such as eSTC. A wallet app can also provide enhanced functions such as secure store.

- **Secure Storage and Recovery of Certificates and Keys (optional)** - this service is dependent on the requirements of customer app (likely a wallet app) and on factors in addition to what is provide in the use case. A key requirement is the restoration of the certificates and key recovery if the device or information is compromised. There are numerous Bitcoin wallet implementations that have online backup (Google Drive, Dropbox, et.c) and recovery strategies.

Demonstration Prototype

This section describes the demonstration prototype that has been developed to demonstrate implementation of key concepts and the end-to-end functional validity of the solution architecture, and applicability to the design challenge use case.

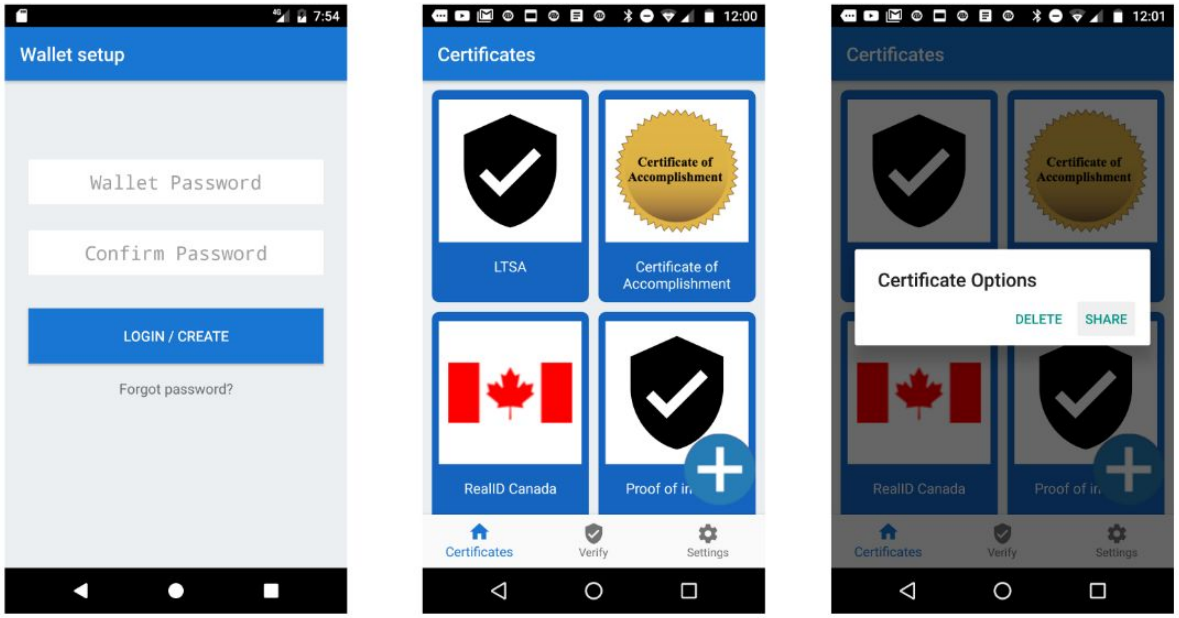
Customer App Prototype

The demonstration prototype is an implementation of the **Customer App** for the Android mobile operating. The prototype uses the Blockcerts standard and associated open source libraries. To develop the Android app, the open source libraries that were implemented in Python, have been re-implemented in Java. Once these libraries are finalized and tested they will be contributed to an Blockcerts open source SDK.

Wallet App Functions

The Customer App prototype is a wallet app that implements a Blockcerts version of the **State of Title** certificate provided in the use case example. A sample certificate has been generated, issued and registered on the blockchain. This resulting certificate has been imported into the wallet app, which includes the verification functions that are also necessary for the **Third Party Verification App**.

The figure below illustrates the general functions of the Android Customer App.



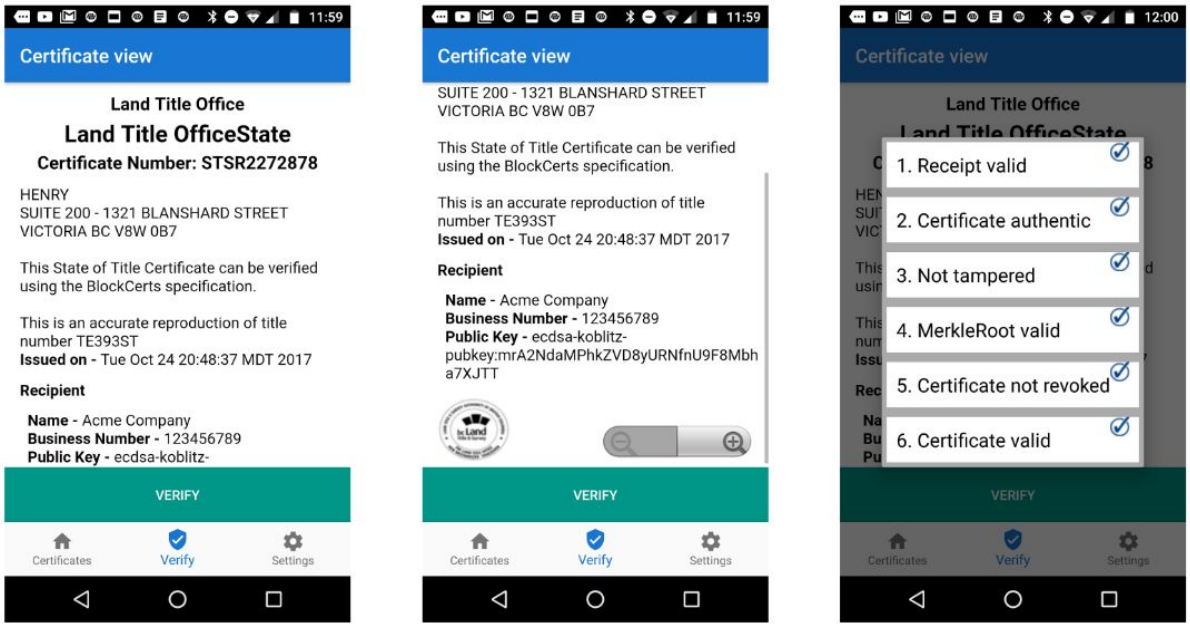
The leftmost screenshot illustrated the login and recovery functions. As discussed earlier, it is anticipated that the wallet application would be integrated into a larger ecosystem provided by the LTSA or the province (for trusted digital identity).

The centre screenshot shows the certificate held within a secure wallet application. The Blockcerts standard and verification scheme can address a wide variety of use cases, so other certificate examples are also shown.

The rightmost screen shows the sharing options of a selected certificate (**Present Certificate,** as described in previous section). Depending on the circumstances, numerous sharing option may be required for the customer to present the certificate for verification, such as email, secure file transfer, NFC, or QR code.

Certificate Verification Functions

The figure below illustrates the certificate verification functions of the Customer app (**Verify Proof of Certificate,** as described in previous section). As noted earlier, these verification functions can also be implemented in a **Third Party Verification App** that is separate from the Customer App.



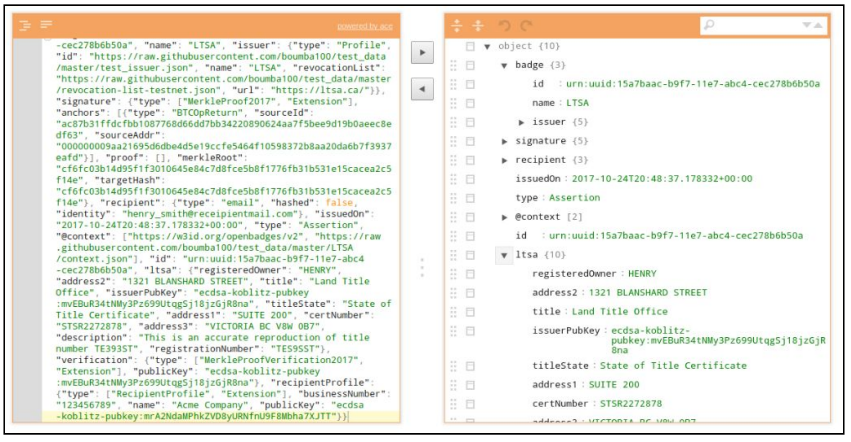
The leftmost and centre screenshots show the certificate (scrolling is required). The certificate is stored in the Blockcerts standardized format and the app, using a template provides the information visually to the user. As required by the use case, the state of title information is shown, also with information of the recipient who is the authorized user of the certificate. In addition to the Name, and Business Number, a public key was added to the certificate format. The corresponding key would be provided to the recipient (authorized user) and can be used by the Third Party verification app to additionally challenge the presenting user, if required.

Additional Technical and Implementation Detail

This section provides additional technical and implementation detail on various aspects of the demonstration prototype.

eSTC in Blockcerts Standard JSON Format

The following figure illustrates the eSTC certificate generated and used in the demonstration prototype as a raw JSON file (left) and as structured tree (using a JSON editor).



Paper-based/PDF Format (QR Code) that is Electronically Verifiable

The following figure shows an alternative format of the eSTC certificate as a printed document (paper or PDF). While the LTSA seal on the right provides a visual affirmation of authentication, the QR code on the left can be electronically read with a standard QR reader (incorporated in the demonstration prototype) and electronically verified. This option is particularly attractive for third parties that wish to remain in the paper world, but have a means to electronically verify the information on the paper certificate. While human intervention may still be required, this verification method is superior than the current method and obviates the need for secure paper stock.


LAND TITLE OFFICE
STATE OF TITLE CERTIFICATE
Certificate Number: STDR2272878

HENRY
SUITE 200 - 1321 BLANSHARD STREET
VICTORIA BC V8W 0B7

This is an accurate reproduction of title number TE393ST
Issued on - 24/10/2017

Bitcoin Blockchain as a Registry.

In Bitcoin Blockchain implementation, cryptographic proof data is embedded in the Bitcoin blockchain using the OP_RETURN code. In the case of the Blockcerts standard, the issuer (LTSA) creates a transaction that includes a Merkle Proof related to the certificate and a digital signature that can be used prove that the issuer created the certificate and that the information contained within the certificate has not been tampered with.

User Challenge and Response Methods.

To ensure that the individual presenting the certificate is the same person to whom the certificate was issued can be achieved in different ways. One method is to ensure that certificate remains under the control of a secure managed context. Another method is to include in the certificate the public key of the recipient, that can used by the verifier to challenge the presenter.

Decentralized Identifiers (DIDS) and Pairwise Identifiers.

Currently, the issuer has a public key or Bitcoin address that is part of the certificate body. These keys or addresses are difficult for humans to differentiate and impossible to remember. Further, if the public key or address is required to change, for ongoing verification purposes, it is necessary to maintain a historical list of keys/address associated with the issuer. There are efforts underway to abstract these concepts to DIDs or pairwise identifiers having human-friendly identifier (easy to remember) that are embedded in the certificate, thus abstracting away cryptographically generated

identifiers and allowing these to change (key rotation) while keeping the human-friendly identifiers constant.

Peer-to-Peer Verification.

Despite their claims, many decentralized solutions are still dependant on centralized endpoints which then mediate access to blockchain nodes (e.g. blockchain.info for blockchain services). An alternative approach is to download the block headers, including the merkle roots for each block. When required to verify a transaction, the verification can request the block from a full node and reconstruct the merkle branch to required for a merkle proof. For the Bitcoin blockchain, this is the Simplified Payment Verification (SPV) protocol.

Certificate Revocation.

The current Blockcerts revocation scheme still relies on a certificate revocation list (CRL) hosted by the issuers. This also introduces a dependency that requires the issuer to provide an endpoint to the CRL. Approaches are being considered to enable a certificate revocation state to be recorded on the blockchain. For example, each certificate may have an unspent transaction output (UTXO) balance, that if spent (UTX=0), indicates that the certificate is revoked.

Mapping Back to Pain Points

The following table illustrates the Design Challenge pain points are fully addressed.

Pain Points	**Addressed by Solution Architecture and Demonstration Prototype**
Pain Point 1: If a customer loses or misplaces the original PDF of the eSTC that was issued to them, the eSTC becomes inaccessible for the remaining time period during which it is valid. This is because the Certificate Number and Access Code can only be found on the PDF. Further, the LTSA has no mechanism that enables retrieval of the Certificate Number and Access Code after the eSTC is issued. This is problematic for both customers and the LTSA. Customers who can't access their eSTCs would have to submit (and pay for) a new eSTC. This creates dual inefficiencies for the LTSA: 1) LTSA staff receive related enquiries on how to recover their eSTC (which is not possible without access to the original PDF of the eSTC). 2) Lost certificates consume hard-drive space of the LTSA certificates Access Service, because lost certificates will remain in storage for the remainder of the 12 months period for which they are valid, even if the service isn't being used.	● For security and privacy reasons, the LTSA should not be able to retrieve the certificate and access code, however if the eSTC is issued as a Blockcerts standard, securely stored in the Customer App and backed up, it should be easy for the Customer to recover. This would reduce the number resubmissions. ● Using the Blockcerts standard, there is no longer a need retain a duplicate PDF in central storage because the certificate can be verified against the Blockchain. This frees up storage, and there is no longer to limit the validity period of the certificate because a copy no longer needs to be stored. ● If, for any reason, a lost certificate needs to be re-issued (as stated in the previous points) a newly issued certificate no longer needs to be centrally stored. **PAIN POINT 1 IS FULLY ADDRESSED**
Pain Point 2: Before STCs were delivered electronically, they were originally delivered by mail. Third-parties such as banks and law firms identified the mail as coming from LTSA and	● The QR code method proposed can be used to replace paper-based security method such as coloured papers. This allows third parties to keep a paper-based method but providing them with the added benefit of electronically verifying the certificate (by reading the

trusted it to be authentic by the colour of paper the certificate was printed on. With the move to eSTCs, customers have to access the eSTC and then email the hyperlink or the PDF to the third party. Or they can print out the PDF and deliver it in person or by mail. However, third-parties are unable to rely on previous trust points of LTSA mail and uniquely coloured paper and feel they have no mechanism of authenticating the PDF. For security reasons (e.g., authentication of individuals' identities), some third parties (e.g. law firms, banks) will not accept a printed-PDF copy of the certificate, or an email with the hyperlink or PDF..	QR code off the paper). ● The QR Code becomes a paper-based trust point that makes other security features redundant. A paper certificate can be verified as authentic against the blockchain using the mobile app, or a component integrated into existing applications. ● By providing the public key of the authorized individual in the certificate (which can be read into the QR code), the individual can be authenticate using a variety of methods employing a standardized cryptographic challenge-response protocol (FIDO Alliance) **PAIN POINT 2 IS FULLY ADDRESSED**

Conclusion

I believe I have met the requirements of the DIACC Digital ID Design Challenge and have proposed and proven, end-to-end, a design idea, solution architecture and demonstration prototype that leverages blockchain technology and digital identities as appropriate. I also believe that I have demonstrated how to improve the overall efficiency for accessing, sharing, verifying, and trusting Electronic State of Title Certificates for customers and third-party participants of the Land Title and Survey Authority of British Columbia (LTSA).

Annex A: Evaluation Grid Criteria Cross Reference

The following table cross-references this material within the document to the criteria categories and can be used to assist in the evaluation of the submission.

Category	Wt	Evaluated Criteria Cross-Referenced to
Context and Relevance	25%	*Are relevant to the context of the cases provided.* ● Context and relevance: CR1 CR2 CR3 ● why blockchain technology are necessary CR4 CR5 ● why Digital ID is necessary: CR6 ● clear that blockchain & Digital IDs together will solve a problem where other technologies will not.
Security and Privacy	25%	*Demonstrate security and privacy principles by design.* ● Solution clearly and effectively incorporates security & privacy considerations to a very high standard, including demonstrating adherence to BC Government IMIT standards and principles SP1 SP2 of privacy by design SP3
Economic and Social Benefit	15%	*Clearly demonstrate economic and social benefit.* ● Proposed solution elegantly addresses economic and social benefits, making a very strong case for the solution design in relation to these benefits. EC1 EC2 EC3 EC4
Feasibility	15%	*May be developed with the right resources and support.* ● The solution is feasible in along all dimensions FE1
Usability and Convenience	10%	*Are convenient and easy to use.* ● The solution demonstrates careful and sophisticated attention to usability & convenience, and references authoritative supporting or background documents such as BC Government design standards UC1 UC2
Creativity and Presentation	10%	*Presentation is creative and presented with high quality.* ● The design solution is very innovative and demonstrates a high degree of creativity. CP1 ● The team presentation clearly and effectively tells the story about how their solution will solve pain points. The presentation is very professionally presented. CP2 CP3 CP4

Note: This table is provided for evaluation assistance only.