DIACC Design Challenge

Noah Bouma
OnePair Technologies

ONEPAIR
SECURITY. TRUST. INTEGRITY. .ca

Understanding the Problem - Context

- **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.
- LTSA provides **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.
    - **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.

OnePair DIACC Submission Full Report is available here.

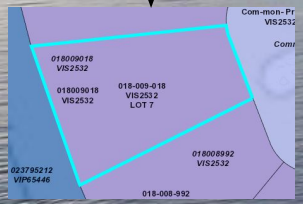
Existing System

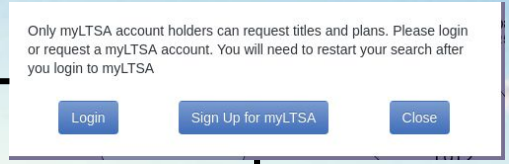
LTSA

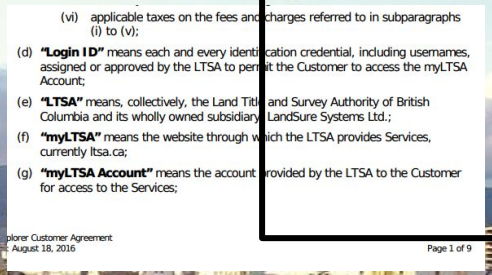
myLTSA (web)

Survey Records
Land Title
Interests

PDF
Cert DB







(vi) applicable taxes on the fees and charges referred to in subparagraphs (i) to (v);

(d) **"Login ID"** means each and every identification credential, including usernames, assigned or approved by the LTSA to permit the Customer to access the myLTSA Account;

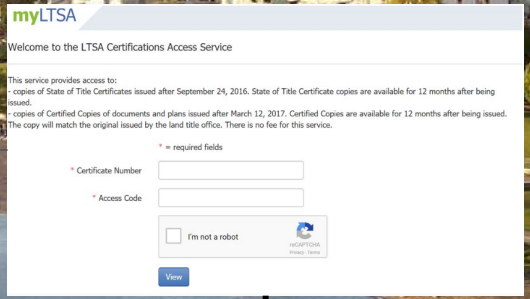
(e) **"LTSA"** means, collectively, the Land Title and Survey Authority of British Columbia and its wholly owned subsidiary, LandSure Systems Ltd.;

(f) **"myLTSA"** means the website through which the LTSA provides Services, currently ltsa.ca;

(g) **"myLTSA Account"** means the account provided by the LTSA to the Customer for access to the Services;

plorer Customer Agreement
- August 18, 2016

Page 1 of 9



Designing for Opportunity (1 of 3)

Challenge	Opportunity
Reducing Friction. 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.	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.) ● **Digital Identity Friction:** Leverage standards-based services (e.g. BC Services Card) ● **Claims Verification Friction** verifying and relying on issued digital claims (eSTc) using standards-based blockchain certificates.
Reducing Administrative and User Burden 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.	Reducing burden for administration of the LTSA system and users of the system. ● **Eliminate centralized service** that stores copies of, and validates certificates. Instead, the proof of issuance of the certificate can be registered on the blockchain

Designing for Opportunity (2 of 3)

Challenge	Opportunity
Increasing Security and Privacy 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.	● **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. ● **Remove any and all personal information from the verification service**. The verification service can be mediated through a cryptographic proof (with zero-PII) registered on a blockchain. ● Use **Privacy By Design (PbD)** to ensure 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 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.	● **Ensuring digital authenticity** of the the state of title information contained in the certificate. ● **Uses 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.

Designing for Opportunity (3 of 3)

Challenge	Opportunity
Prevent Improper or Inconsistent Use 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.	● **Develop an app** that manages the transmission and verification processes ● **Include a public key** of the recipient that is used by third party to challenge ownership before verifying the certificate ● **Encrypt**, if required, the contents of the certificate and securely decrypt before verification
Eliminate Downstream Dependencies 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.	● **Eliminate technical and centralized service dependencies** for downstream business processes that rely on the state of title certificate. ● **Allow for an expanding set of participants (ecoystem)**, using standards-based, blockchain approach to enable for the verification of the certificate by separate and independent systems.

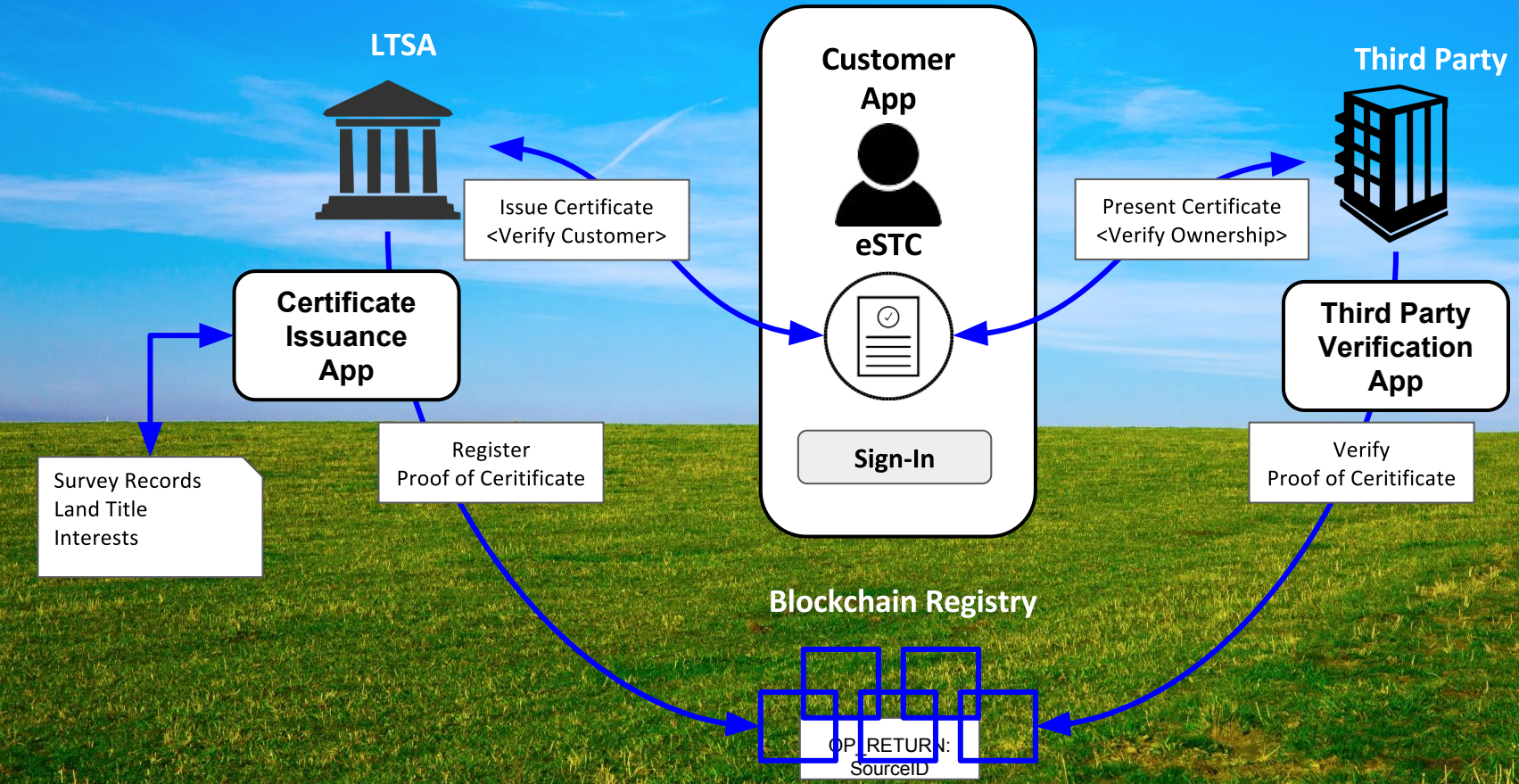
Solution Building Blocks (1 of 2)

Solution Building Block	What is it?
Blockchain (including Cryptographic Techniques)	• **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) • **Distributed consensus method** of maintaining the list, such as proof of work (PoW) • **Distributed ledger** that can securely maintain a unit of account (e.g., cryptocurrency) or state (smart contracts) over many instances • **Public permissionless blockchain**, the “miners” would be incentivized to maintain the blockchain using a competitive PoW scheme with cryptocurrency rewards.
Verifiable Claims	• **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 • **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)

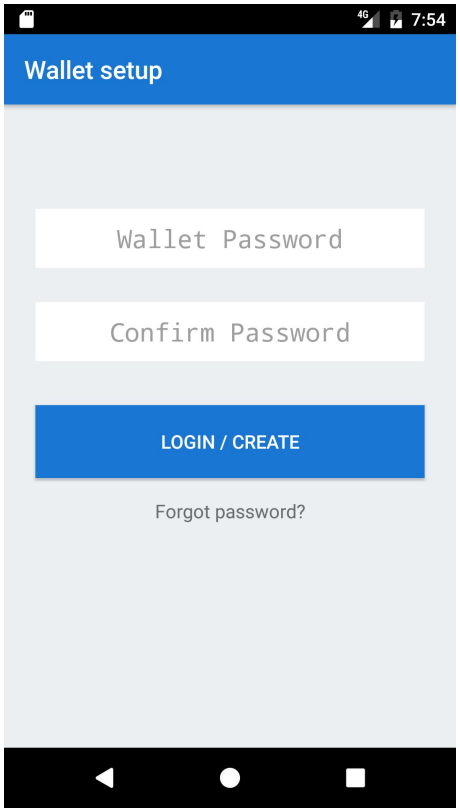
Solution Building Blocks (2 of 2)

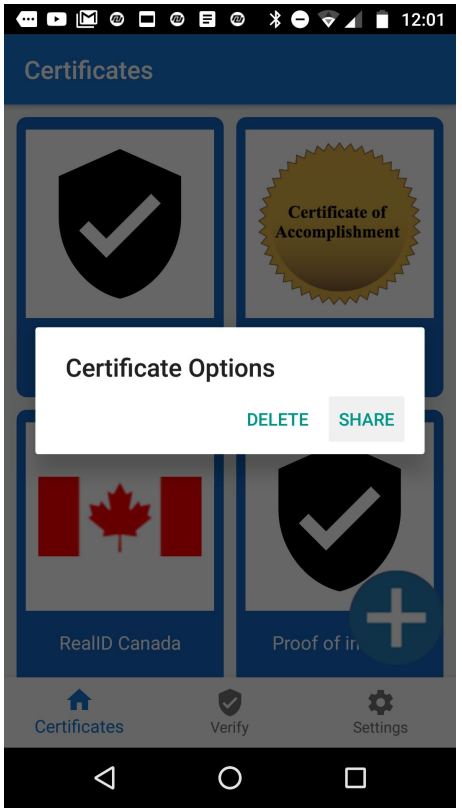
Solution Building Block	What is it?
Blockcerts Standard	• **BlockCerts** (www.blockcerts.org) is an open standard developed by MIT Media Labs for creating and issuing certificates that can be verified using the blockchain. • **Enables tamper-proof electronic certificates** to be presented by a recipient to any third party, who in turn can perform a verification that is independent of the recipient and the issuer.
Digital Identification and Authentication Ecosystem	• **Integrate solution into the larger digital identity ecosystem** enabled by the DIACC Pan-Canadian Trust Framework. • Use FIDO Alliance standard to 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	• **Use open source and standards-based approach** to ensure software and system can be freely inspected and modified to suit the needs of the business, fix errors, and address security issues.

Solution Architecture

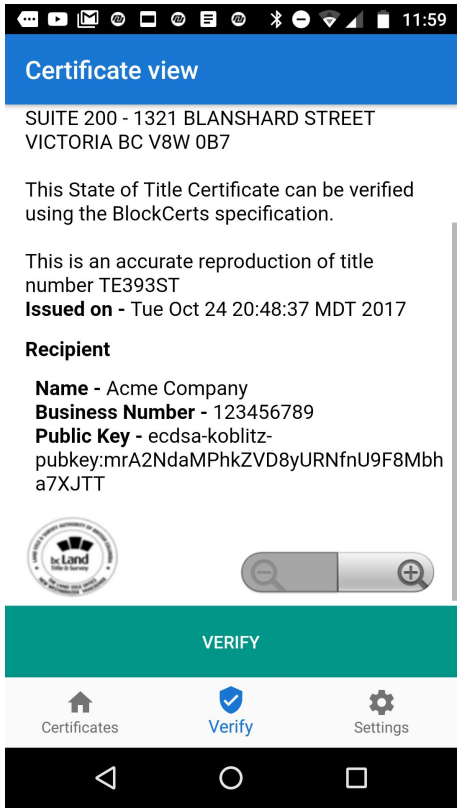


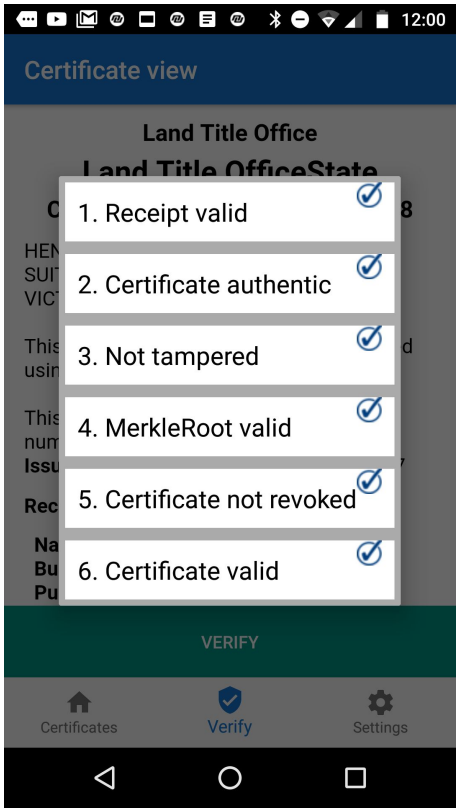
Android Customer App Demo (see demo video)





Android Customer App Demo (see demo video)





Key Processes

Issuing eSTC Blockchain Certificates

- Generate certificates with key values (receipt, badge, recipient info, issuer info, pubkey, revocation info)
- Hash the individual certificates
- Build a Merkle tree (Chainpoint V2-formatted Merkle receipt) with the hashes of the certificates
- Register the Merkle receipt in a bitcoin transaction on the blockchain

Sharing of eSTC Blockchain Certificates

- The blockchain is not used to broadcast or store claims
- The blockchain is only used to store the hash/signature of issued certificates
- The Blockcert specification does not determine how certificates should be shared.
- Certificates could be sent using email, NFC, qr-code, dedicated messaging protocol, etc...

Verifying of eSTC Blockchain Certificates

- Check certificate integrity (validate local hash and Merkle proof)
- Check certificate authenticity (valid pubkey, creation date - timestamp)
- Check certificate not revoked(CRL for now!)
- Check certificate not expired

eSTC Certificate formats

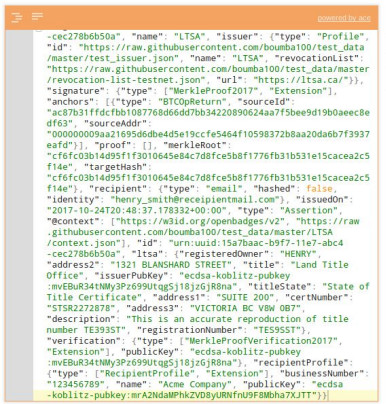
eSTC paper-based format with QR-Code….


LAND TITLE OFFICE
STATE OF TITLE CERTIFICATE
Certificate Number: STDR2272878

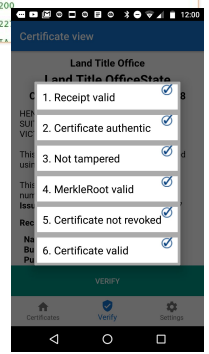
HENRY
SUITE 200 - 1321 BLANSHARD STREET
VICTORIA BC V8W 0B7

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

...can be read into eSTC Blockcerts format



...and verified electronically against the blockchain!!



Conclusion (read full report)

PAIN POINT 1 IS FULLY ADDRESSED	• 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 2 IS FULLY ADDRESSED	• 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 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).

- Proposed and proven, end-to-end, a design idea, solution architecture and demonstration prototype that leverages blockchain technology and digital identities as appropriate
- 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)