Solution Overview

Version 1.4.8

TRUSTI

4 Corporate Blockchain Integration
5 Solving Blockchain Identification
7 Public Key Infrastructure
9 The Trusti Ecosystem
10 Trusti Certificate Content
11 Who Can Issue a Trusti Certiticate?
12 Trusti for Securities Trading
16 The Trusti Wallet
20 Compliance

Trusti enables the creation of accredited and identified cryptocurrency wallets, with specific attributes defined by the authority certifying them.

This not only helps secure blockchain transactions against fraudulent practice, but means government and corporate entities can certify addresses, only to be held by identified, accredited persons such as securities traders, people of a defined age range, or those holding a license to trade an asset class. A new blockchain reality in which parties can recognise the credentials of each other while performing a transaction, protecting each in terms of compliance and security.

The Perils of Corporate Blockchain Integration

While global enterprise has embraced blockchain technology, and its potential to revolutionise the way in which aspects of industry can function, the same advantages that make it appealing, expose new risks. While the birth of cryptocurrency was based on aspects that are advantageous to global enterprise (such as speeding up and scaling transactions), many attributes (such as anonymity at all cost), can harm enterprise and those they serve as clients.

While true anonymity is an extreme example of the drawbacks facing enterprise wishing to embrace blockchain, the lack of appropriate means to certify the identity of parties to a transaction is a widespread issue preventing advancement in multiple areas, such as securities trading.

Industries that are most reticent to adopt blockchain infrastructure are apprehensive because of a disconnect between expected and traditional transacting protocols and what currently exists on the blockchain. These industries express a strong willingness to harness blockchain's power but cannot do so because of, among others, integration issues.

A key example of an area of commerce struggling to adapt to blockchain technology is regulated securities. While the tokenization of security assets is seen as a core future direction of cryptocurrency, almost every global legal jurisdiction mandates that the persons exchanging securities be identified and accredited in some form. This can range from simply knowing their identity, to requiring specific, bespoke information.

Aside from these core examples, the use cases for volutary accreditation and identification of cryptocurrency wallets is endless. Whether it be the requirement to identify by age, residency, credit rating, memberships or more.

Trusti

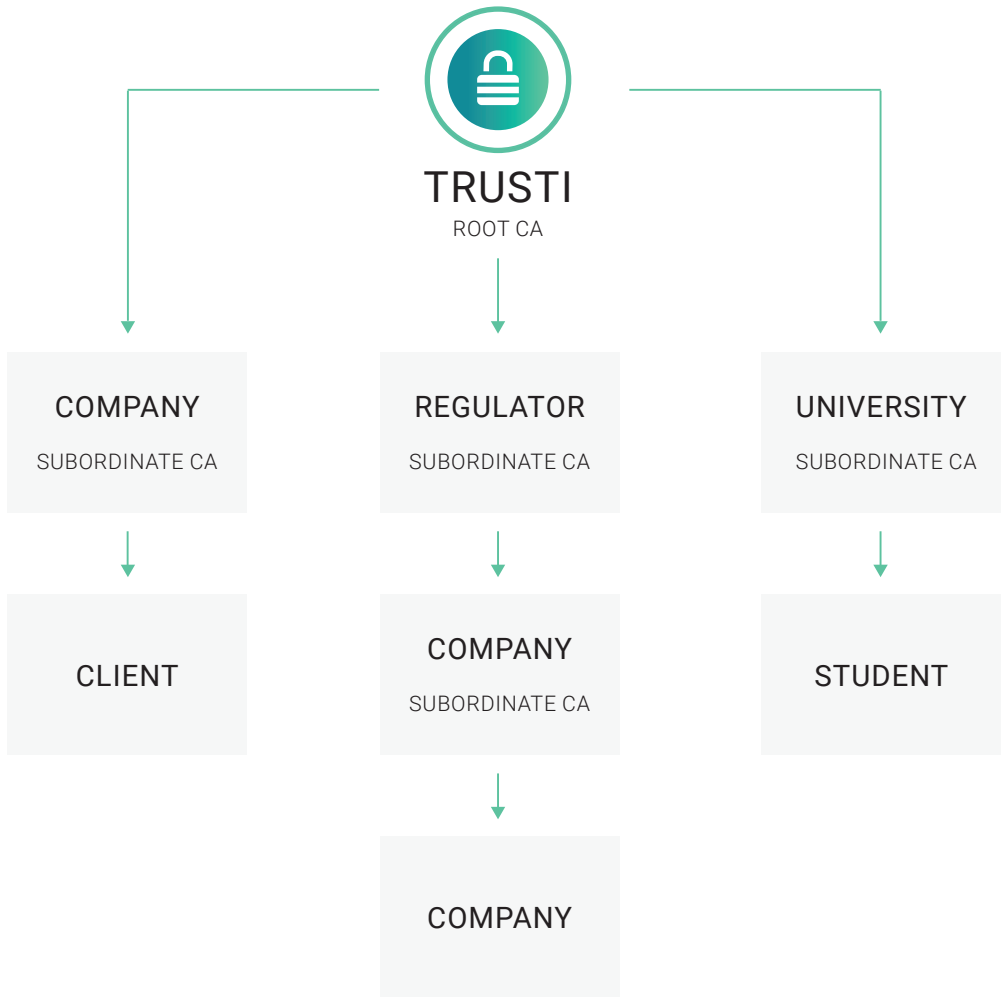
A singular solution to the certification of wallet users

Trusti is a comprehensive answer to fraud, impersonation, and the misuse of ostensibly regulated products on the blockchain. Trusti's technology and infrastructure bridges the gap between the expectations of enterprise and the anonymous reality of cryptocurrency by providing cross-chain certification of identity and attributes. The protocol enables enterprises –such as regulated exchanges– to provide certification of cryptocurrency addresses which can be used for anything from trading authorised securities, to issuing cryptocurrency loans.

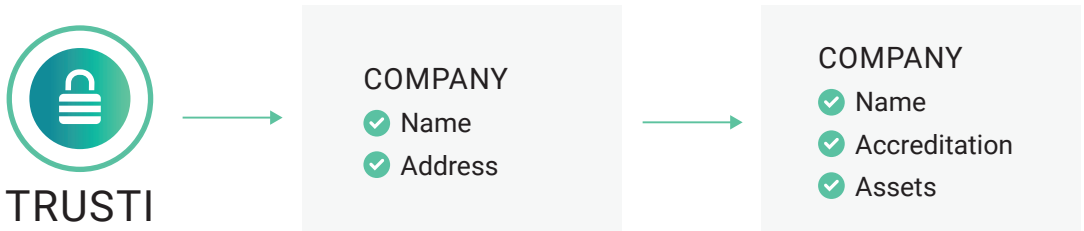
Trusti enables:

- A Certificate Authority (CA) which certifies an address (or certifies the ability to issue further certificates) is who they say they are.
- A Subordinate Certificate Authority to choose what attributes should be identified on the cryptocurrency addresses (such as age or accreditation), and certifies them under their own reputation.
- Those wallets to be proven as belonging to whom they are certified to, including the attributes selected, under the trust of the CA.

1 Typical Certificate Chain Linking to Root CA



2 Typical Chain of Attribute Certification



PKI Infrastructure

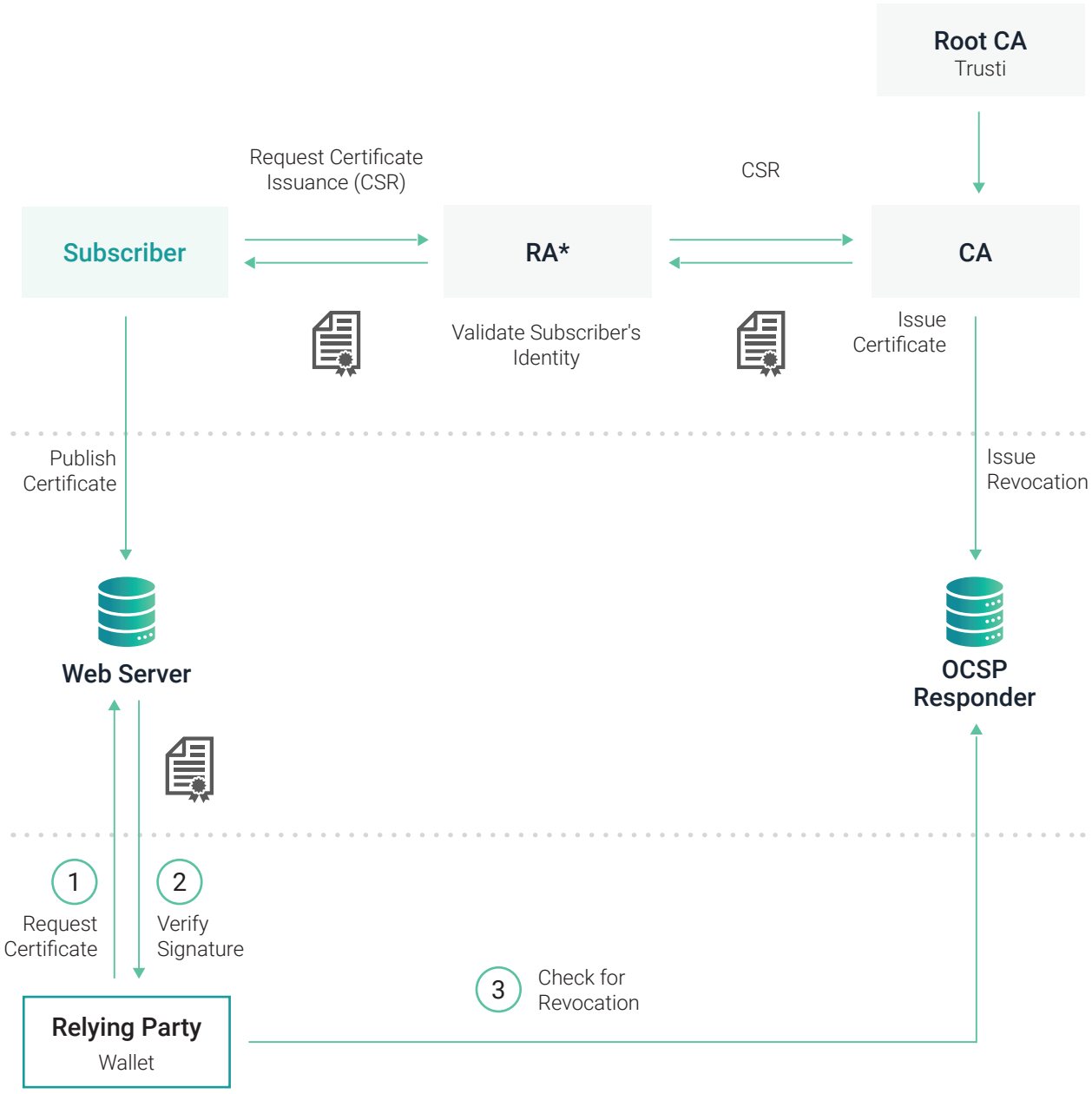
Trusti’s core mechanism for achieving its mission is via Public Key Infrastructure (PKI) which binds public keys with respective identities. PKI is a system for the creation, storage and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity.

The primary component of a PKI infrastructure is the Certificate Authority (CA), which stores, issues and signs the certificates that identify accounts and their owners. While the original Root CA is Trusti itself, this authority signs subordinate CA’s which sign certificate requests, which themselves can issue further certificates under their credentials (if authorized to do so by their own certificate provider), while protecting the original root authority.

Trusti's application of PKI infrastructure creates a chain not only of certificates, but trusted information. Each rung on the chain certifies that the identifiers and attributes on the following rung are accurate –and the client decides (through an automated process), whether to trust each rung on the chain leading to the final certification.

This creates a reality whereby a certificate is only as valuable and trusted as the source issuing it, creating a hieracrhcy of trust as new certificates are issued by subordinate authorities. While standard KYC by trusted identity services is one use case for a Trusti CA and certificate, the information that can be certified is endless.

Core PKI Infrastructure



* A Registration Authority (RA). CAs often outsource the verification process to such third-party agencies.

Snapshot of Trusti's Ecosystem

Cryptocurrency exchanges

- Protecting against phishing attempts by confirming true identity every time a client deposits funds.
- Providing certified wallets ensuring only accredited investors can withdraw their traded security tokens.

Investments (i.e. real estate)

- Confirming invesment entities as a regulated investment vehicle to potential investors, protecting against both impersonators and scam investment opportunities.
- Conforming to regulatory requirements by only allowing wallets accredited to invest to participate. This can be internally or via outsourcing accreditation to another trusted CA.

Voting

- Ensuring 'one person one vote' by having specific identitifes certified as being linked to an address.
- Exclude ineligible voters by demanding certification of eligibility.

Banks

- Confirming a bank's identity as a retail bank to depositors.
- Offering branded cryptocurrency wallets which can be used to confirm the identity of clients' wallets, therefore offering a recourse to action from scams (comparable to existing traditional retail banking model).
- Offering branded investment accredited wallets.

ICO's

- Protecting potential investors from impersonation scams.
- Ensuring regulatory compliance by only selling security tokens to accredited investors.

Membership

- Enable participation or purchase only from certified members of an organization, company or society .
- Offer specific benefits only to certified members.

What's in a Certificate?

A certificate is a digital document that contains a public key, information about the entity associated with it, and a digital signature from the certificate issuer. Certificates can be allowed to sign other certificates, thus becoming its own Certificate Authority and creating a certificate chain. The root certificate (Trusti) is the 'trust anchor' of a particular chain. Each certificate in the chain is signed with the secret key of the previous certificate, thus confirming the validity of the final certificate.

The type information verified using a certificate issued by a CA is endless, with an authority being able to verify anything from an investor's address and capital liquidity, to a student's enrollment at a university. That said, there is some core information that must be included in every certificate:

Corporate Certificate Example

a) This certificate was granted by the Trust Reputation LTD. The certificate of Trust Reputation LTD was granted by Trusti (root provider).

b) The full legal name of the certificate's owner is XYZ Bank LTD.

c) XYZ Bank LTD is a Business Entity.

d) XYZ Bank is incorporated in London, United Kingdom.

e) XYZ Bank is registered under the FCA, registration number 111xx111xx111xx111

d) XYZ Bank's registered address is:

1 London Place
London
United Kingdom
SW1 Y11

Personal Certificate Example

a) This certificate was granted by the CDQ Private Verification Services Ltd. The certificate of CDQ Private Verification Services Ltd was granted by ABC Corporate verification Ltd. The certificate of ABC Corporate verification Ltd. was granted by Trusti (root provider).

b) The full legal name of the certificate's owner is Charles Adam Stevenson

c) The certificate's owner is a private individual

d) The certificate's owner has the following certifications attached to this address:

Series 7 Accredited investor in the United States by the SEC (2010)
Age - 21+

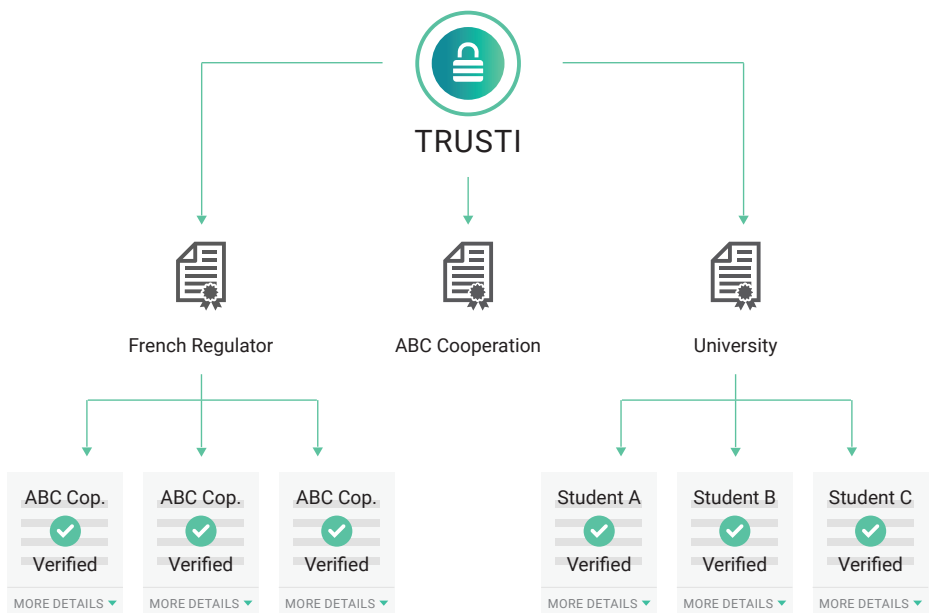
Who can issue a Certificate?

Much like an SSL certificate, a Trusti certificate can be issued by any entity authorized to do so by the Root Certificate Authority (Trusti). Yet, being certified to issue a certificate in of itself is not proof of anything other than an entity's or individual's identity and it is up to the end user or intermediary to decide what certifying authority to accept as legitimate.

For example, in the United Kingdom it may be that two distinct entities apply to Trusti to become CA's, both for the purpose of age verification:

(i) The Driving License and Vehicles Authority (DVLA)
(ii) Bob's Age Verification Service Ltd

In this example, it is not for Trusti to define what should be accepted as a truly trusted age verification, but rather to confirm that each party certifying age is indeed who they say they are. It may well be that a British stockbroker may choose to accept all certificates provided by the DVLA, but not accept small independent verifiers with which they're not familiar. However, that's the prerogative of each independent actor.



An Expanded Use Case - Trusti for Securities Trading

ABC Capital wants to open a $500m casino project, and seeks to achieve funding by issuing security tokens that represent ownership, and therefore future dividends, in the endeavor. As these tokens represent shares for the purpose of generating profit, they are considered securities and thus subject to applicable regulations.

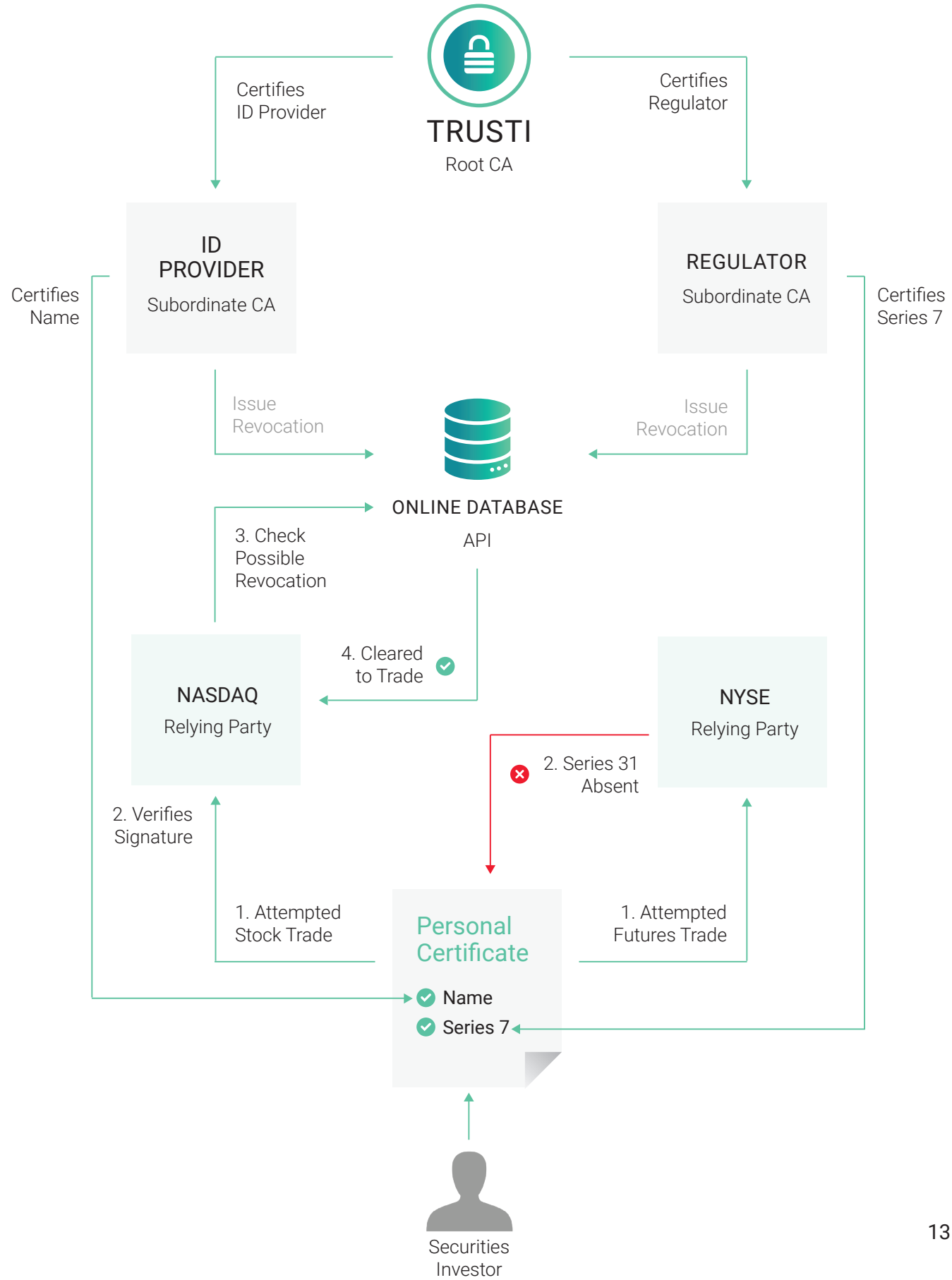
Therefore before selling their tokens, ABC Capital need to:

1. Ensure that when their potential investors send funds, they can be be confident they are finding their way to ABC Capital and not to an impersonator.
2. Make sure that the funds that they're receiving are being held in a secure segregated account conforming to regulations.
3. That only those accredited in the applicable jurisdiction to purchase securities are able to do so.

The process that ABC Capital must complete is as follows:

1. ABC Capital chooses rather than becoming a cross-chain certificate authority itself, to instead rely on CA's recognized by regulatory authorities in the five countries in which it wishes to sell securities. They sell their securities to individuals certified as fulfilling the applicable criteria in each of these jurisdictions.
2. ABC Capital has its identity certified by a major recognized CA in its country of incorporation. In order to do this they must complete a verification process to confirm their own identity and control over their firm's assets.
3. Every time a potential investor wishes to purchase ABC Capital security tokens, their system will automatically check whether the wallet attempting to make the investment is certified as being accredited to do so in the regulatory region in which they're in.

Core PKI Infrastructure Case Study



Enabling Confidence in P2P and C2B Transactions

As well as it core applications as a KYC mechanism for compliance and security, Trusti's infrastructure is also a suitable way to enable confidence in the sending of P2P and C2B transactions. An individual or entity wishing to receive a transaction can opt to share information about the identity verified as being linked to that wallet in order to give confidence to the sender that they are who they claim to be.

Ultimately, as in other Trusti use-cases, it is at the discretion of the sender what certification to accept as being trusted. It may be that a transactor accepts the identification provided by a trusted governmental certificating authority, while not that belonging to an unrecognised private entity. Typically, this trust process will be outsourced to third party entities such as retail banks and cryptocurrency wallet providers that will decide which entities to trust for the provision of identity. This is comparable to the process of SSL certification whereby the trust process is primarily outsourced to the browser which deems which certificates to accept as legitimate and trustworthy.

Trusti envisages a future where this technology will render all unverified transactions suspicious, as there is no reason for a trusted recipient not to drop their anonymity and reveal their identity. In practical terms, the tying of simple identity (such as name) is equivalent to the traditional banking system in which typically a name must match an account number in order for a transaction to process - giving the sender security that they are not being phished into sending funds to an improper recipient. This problem is commonplace within the cryptocurrency ecosystem whereby large transactions (eg exchange listing fees or marketing fees) can be sent to unknown addresses.

Incorporation of Government Tax Authorities into the Trusti Platform

Government authorities, in particular government taxation authorities, are able to take full advantage of the Trusti certificate chain as a Certificate Authority.

By way of example, the IRS, in order to better manage tax obligations of American citizens' cryptocurrency assets, could require that US citizens only operate wallets that have been certified by the IRS and comply with disclosure requirements designed to prevent tax evasion.

The IRS would undergo the Trusti certification process and become a Certificate Authority with the power to then issue identity and accreditation certificates to blockchain wallet owners. American citizens holding crypto assets would then acquire IRS-issued Trusti certificates and publish all necessary details on their crypto wallets to be tax compliant and in line with IRS mandates.

As a result, the IRS has the same access to information of Americans' cryptocurrency assets as it does ordinary bank or real estate assets. Indeed, digital currencies can no longer be hidden, syphoned, or otherwise kept from the authorities as the IRS has full knowledge of who has what assets. Citizens who do not ascribe to the identification and accreditation service will be committing a violation in the same way that unreported offshore bank accounts amount to tax violations.

Incorporation of Law Enforcement and Security Agencies into the Trusti Platform

As a result of their pseudonymous or anonymous attributes, blockchain technologies and cryptocurrencies have provided criminals and terrorists with the means to transact outside the jurisdictional and operational abilities of law enforcement. Indeed, the success of online criminal marketplaces such as Silk Road was due to the ease with which criminals could sell illicit products and services through blockchain-based anonymous digital transactions.

Further, terrorist attacks are increasingly being financed through cryptocurrencies and indeed many ISIS attacks have been funded this way. Security agencies are having difficulty monitoring the flow of funds as the source and destination of transactions are essentially hidden. Indeed there is no way of discerning the identity of a law abiding citizen's cryptocurrency wallet from that of a terrorist or criminal.

The Trusti platform would counter this by integrating into law enforcement and security agency institutions in order to verify the identity of individual and institutional wallet holders. Agencies would, similar to Trusti's tax authority solution, undergo the Trusti certification process and become a Certificate Authority with the power to issue certificates confirming AML, anti-narcotics and anti-terrorist financing measures are implemented and that a particular user (whether individual or institutional) is not a nefarious actor. Agencies would also be able to, for example, see the identity of wallet owners, black-list malevolent actors or aiders and abettors of malevolent actors, trace suspicious transactions to their source, reveal illicit financing networks, all while allowing genuine users to leverage the speed, price and scalability of blockchain technology.

If the source or destination of a cryptocurrency transaction that would ordinarily come under the jurisdiction of a particular agency has not undergone a security agency's Trust certification process, that transaction will immediately become suspicious. This process will reverse the current paradigm where anonymous and unidentified transaction are standard and accepted.

Trusti’s Secure Wallet

Trusti is to develop a reference implementation for a secure HD wallet which includes the secure identity and KYC protocol. It will be the first app to combine PKI certification with cryptocurrency, and will leverage the user experience of SSL web browsing.

- **iOS** through a native Swift implementation. Using established cryptographic libraries and an Object-Oriented architecture. This implementation could serve as the reference implementation for the other OS's.
- **Android**, through native Java implementation.
- **Windows, macOS, and Linux** through JavaScript and Electron. A library used by hundreds of word-class apps such as Skype, Slack, and WhatsApp.

Furthermore it is possible to develop the following suites:

- **Chrome extension** for Ledger and Trezor Hardware Wallet integration.
- **Extensions for other wallets.** Such as Electrum, Etherwall, and Mycelium

More advanced functionality for issuing certificates will be provided in a corporate implementation of the software, and provided as a desktop application.

Secure QR

In order to easily and safely transfer the Certificate to the client together with the address in print form, the secure QR will have the Certificate URL embedded into the QR itself. This QR will be scannable by any QR scanning App (such as the default camera on iOS) and redirect with a URI deep link to Trusti's secure wallet. As soon as the wallet opens, the software will check the validity of the certificate and for a possible revocation, and if correct, the remittent address and details will be filled and a secure lock will be displayed in the UI. Unlike in web browsers, incorrect certificates and known scams will be completely blocked without an option to skip the warning.

Iconic Trusti Secure QR

The QR will be a ISO/IEC 18004:2015, Version 4 (33×33) with Level H error correction to allow for artistic embellishment. Trusti is aiming to create an iconic design for the QR codes in order to stand out and create market recognition.

Trusti's Solution Compared

	Reusable KYC	Identity Management	Verified ICO's	Secure Wallet	B2B / B2G Integration
Trusti	✔	✔	✔	✔	✔
Pillar	✔	✔	✔	ETH and ERC20 only	✘
Civic	✔	✔	✘	✘	✘
Persona	✔	✔	✘	✘	✘
SelfKey	✔	✔	✘	ETH and ERC20 only	✘
KYC.Legal	✔	✔	✘	✘	✘
Norbloc	✔	✘	✘	✘	✘
Polymath	✔	✘	✔	✘	✘
Social KYC	SDD* only	SDD only	✘	✘	✘
uPort ID	✔	✔	✔	✘	✘
Lemme	✘	✔	✘	✘	✘
Kimlic	✔	✔	✘	✘	✘

* SDD: Simplified Due Diligence, as opposed to full customer due diligence. SSD is usually comprised of information gathered from social media accounts. It is not accepted under Money Laundering Regulations.

Compliance

A core endeavor of Trusti's vision is in bridging the gap between compliance-dependent industry and shortfalls of the blockchain's present (primary and secondary layer) infrastructure. The forms of compliance that Trusti facilitates are eclectic and numerous. This is because Trusti does not validate compliance itself, but rather the identity of those entities that do validate compliance, enabling 3rd parties to define for themselves what certification to accept.

The types of compliance that may be facilitated on the Trusti infrastructure include:

Verification	Possible Provider	Typical Use Case
Age	Home Affairs Office	Restricted Products
Investor Accreditation	Regulator	Stock Broking
Student Registration	University	Student Account
Name	Vehicle Authority	Voting
Lack of Criminal Record	Justice Department	Property Investment
Address	Tax Authority	Initial Coin Offering
Ownership Deeds	Land Registry	Rental Contract

TRUSTI

www.trusti.com