PryvatePVC™

PVC Technical Specifications

V.1.0

APRIL 10, 2018

TABLE OF CONTENTS

Acronyms: Definitions

SCP = Secure Communications Platform
Crypto= Cryptocurrency
IPFS= Interplanetary File System
ZRTP= ("Z" is a reference to its inventor, Zimmermann; "RTP" stands for Real-time Transport Protocol) it is a cryptographic key-agreement protocol to negotiate the keys for encryption between two end points in a Voice over Internet Protocol
Diffie-Hellman= A method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.
RSA 4096 encryption= (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem".
AES 256-bit encryption= Advanced Encryption Standard (AES), also known by its original name Rijndael (Dutch pronunciation: is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001
SHA512= Secure Hash Algorithm is a set of cryptographic hash functions designed by the United States National Security Agency (NSA).. They are built using the Merkle–Damgård structure, from a One-way compression function itself built using the Davies-Meyer structure from a (classified) specialized block cipher.
CLI spoofing= Caller ID spoofing is the practice of causing the telephone network to indicate to the receiver of a call that the originator of the call is a station other than the true originating station. For example, a caller ID display might display a phone number different from that of the telephone from which the call was placed. The term is commonly used to describe situations in which the motivation is considered malicious by the originator.
BSI TR-03145=The British Standards Institution (BSI) is a service organization that produces standards across a wide variety of industry sector
TLS= Transport Layer Security is a protocol aims primarily to provide privacy and data integrity between two communicating computer applications. When secured by TLS, connections between a client (e.g., a web browser) and a server.
Dead man's switch= is a switch that is automatically operated if the human operator becomes incapacitated, such as through death, loss of consciousness, or being bodily removed from control. Originally applied to switches on a vehicle or machine, it has since come to be used to describe other intangible uses like in computer software.
SIP= Session Initiation Protocol is a communications protocol for signaling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls, in private IP telephone systems, as well as in instant messaging over Internet Protocol (IP) networks.

https://ipfs.io
https://en.wikipedia.org/wiki/ZRTP
https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange
https://en.wikipedia.org/wiki/RSA_(cryptosystem)
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
https://en.wikipedia.org/wiki/SHA-2
https://en.wikipedia.org/wiki/Caller_ID_spoofing
https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html
https://en.wikipedia.org/wiki/Transport_Layer_Security
https://en.wikipedia.org/wiki/Dead_man%27s_switch

Merkle Root=In cryptography and computer science, a hash tree or Merkle tree is a tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

OTR messaging= Off-the-Record Messaging is a cryptographic protocol that provides encryption for instant messaging conversations. OTR uses a combination of AES symmetric-key algorithm with 128 bits key length, the Diffie–Hellman key exchange with 1536 bits group size, and the SHA-1 hash function. In addition to authentication and encryption, OTR provides forward secrecy and malleable encryption.

VOIP=Voice over Internet Protocol (also voice over IP, VoIP or IP telephony) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN).

DNSSEC=The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

MTMN=A man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Anti-Blocking= Geo-blocking is a form of technological protection measure where access to Internet content is restricted based upon the user's geographical location. In a geo-blocking scheme, the user's location is calculated using geolocation techniques, such as checking the user's IP address against a blacklist or whitelist, accounts, and measuring the end-to-end delay of a network connection to estimate the physical location of the user. The result of this check is used to determine whether the system will approve or deny access to the content.

Crypto Wallet=A cryptocurrency wallet stores the public and private keys which can be used to receive or spend the cryptocurrency. A wallet can contain multiple public and private key pairs.[As of January 2018, there are over thirteen hundred cryptocurrencies; the first and best known is bitcoin.The cryptocurrency itself is not in the wallet. In case of bitcoin and cryptocurrencies derived from it, the cryptocurrency is decentrally stored and maintained in a publicly available ledger. Every piece of cryptocurrency has a private key. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency.

Crypto Cold Storage=Cold storage (aka cold wallets) means generating and storing the crypto coin's private keys in an offline environment, away from the internet.

Multi Sig Wallet=Multisignature (multisig) refers to requiring more than one key to authorize a cryptocurrency transaction. It is generally used to divide up responsibility for possession of cryptocurrency.

https://en.wikipedia.org/wiki/Session_Initiation_Protocol
https://en.wikipedia.org/wiki/Merkle_tree
https://en.wikipedia.org/wiki/Off-the-Record_Messaging
https://en.wikipedia.org/wiki/Voice_over_IP
https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
https://en.wikipedia.org/wiki/Man-in-the-middle_attack
https://en.wikipedia.org/wiki/Geo-blocking
https://en.wikipedia.org/wiki/Cryptocurrency_wallet

1 GENERAL INFORMATION

1.1 Scope

This Functional and Technical Specifications Document will outline the functional, performance, security and other system requirements identified by the Pryvate development team as the proposed solution for a hybrid of decentralized and centralized secure communications platform and secure cryptocurrency wallet.

1.2 CURRENT PLATFORM SUMMARY

The SCP Currently has a number of working products:

- Pryvate Encrypted Voice Calls (VoIP)
- Pryvate Encrypted Video Calls
- Pryvate Encrypted Instant Messaging
- Pryvate Encrypted Email
- Pryvate Secure File Transfer & Storage
- PIN-encrypted Mobile Protection
- Multiple Account Management
- Secure Managed Conversations
- Pryvate Encrypted Web Browsing
- Pryvate Anti-Blocking

2 FUNCTIONAL TECH SPECIFICATIONS

The SCP is a technology-based solution for a military grade secure communications and management system with the primary function of creating of a fully-secure ecosystem of encryption technologies. It currently includes:

2.1 Encrypted Voice Calls (VOIP)

It is always best to use open-source, peer-reviewed encryption tools on your smartphone, tablet and desktop computer. The PryvateNow app for Android (4.1 or higher) and Apple (iOS 8.0 or later) features voice encryption capabilities that enable subscribers to make free, Voice-over Internet Protocol (VoIP) calls that are secure, encrypted and completely private.

Pryvate™ Encryption

- Military-grade encryption combined with RSA 4096-bit and AES 256-bit encryption
- No risk of data being intercepted by hackers, criminals or government surveillance agencies
- Diffie-Hellman (D-H) key exchange, MD5 and SHA512 hash for voice integrity
- Proprietary ‘Protection Agent’ software that detects, alerts and defends against ‘man-in-the-middle’ attacks
- Encryption keys that are automatically created on your smartphone for each call

Voice Call Quality – Multiple Network Compatibility

- Industry-leading, encrypted voice service that operates over carrier-grade infrastructure
- Secure calling over 3G/4G, GPRS, EDGE, LTE, UMTS, HSPA, W-CDMA or Wi-Fi connection, even at low bandwidths

https://coinsutra.com/cold-storage-cryptocurrency/

Security

Single-session-only keys are never stored or known to Pryvate as the software works on a peer-to-peer basis with no servers in the middle - with no record of calls ever retained.

Automatic Discovery of Pryvate Contacts

- Auto-notification when a contact becomes a Pryvate user
- Users will also be able to see when their Pryvate contacts are available
- Contact details will automatically populate their Pryvate address book

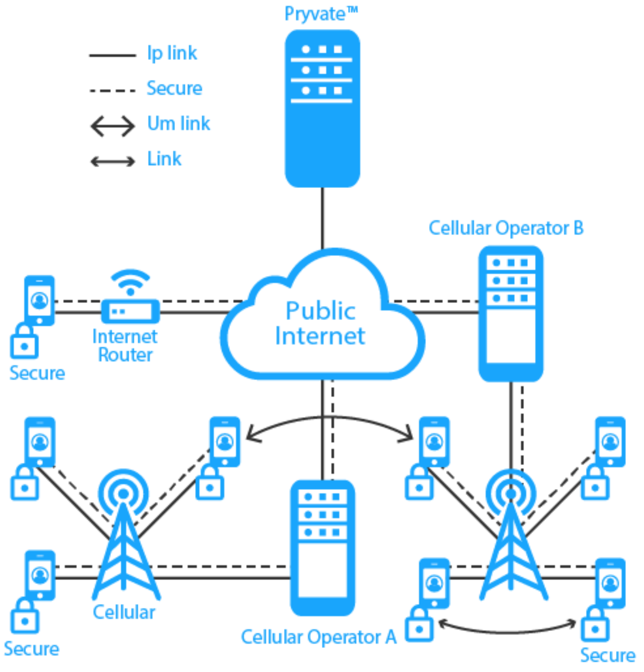
2.2 Off Net Calling

After account creation and payment, the customer's app will present an off-net calling option enabling calls to be placed outside the PryvateNOW secure network. Authorization for the account and calls will be via Account Name or Mobile Number and Assigned Password, negating the possibility of CLI spoofing.

Calls generated by the app will leave the user's client/app encrypted and shall remain encrypted from the handset to the PryvateNOW servers. An off-net call will be decrypted and bridged, the B leg over to the call termination switch. Thus, a user shall always have a secure A leg on all off-net calls. The call is then validated and authorized by the account and assigned password and passed to the termination provider for onward progress.

Secure Conferencing

We utilise the same encryption whilst conferencing with multiple users - with all voice calls encrypted. The conference call runs on the conference organiser's device. They initiate the conference by calling the other parties and adding them to the group.



Pryvate™ Encrypted Video Calls

Video encryption takes video data and makes it impossible to view by anyone except the intended recipient - so long as the intended recipient has the correct key to decipher the data and view the video in its intended format.

Some major Off-App Calling services are:

- Automatic creation of new accounts/closure of cancelled accounts
- Billing for next available month and account blocking on non-payment
- Rating for unlimited and streamed destination minutes
- Customer portal for account management
- CDR backup
- Routing tables and code blocking
- Rate sheet holes/premium numbers
- Fault management and handling, including providers
- Destination bought plan changes
- Inbound geographic numbers.

2.3 Secure Conferencing

The same state-of-the-art encryption is in use when conferencing with multiple users, all voice calls are fully encrypted. The conference call runs on the conference organizer's device, and they can easily initiate it by calling the other parties on their app and adding them to a group call.

2.4 Encrypted Video Calls

Video encryption takes video data and makes it impossible to view by anyone except the intended recipient, as long as the intended recipient has the correct key to decipher the data and view the video in its intended format.

There are two types of video encryption: personal and Digital Rights Management (DRM). Personal encryption refers to someone who wants to share a personal video with clients, family or friends and who does not want anyone unauthorized to see it. DRM is essentially the same, though a little more complex and it often includes:

- Different types of video streams for different price brackets
- Region-specific videos
- Media or device-specific videos
- Software-specific videos
- Adaptive streaming
- Secure Video Encryption and Privacy (never known to us)
- ZRTP Protocol negotiates a key between two VoIP end points
- As with voice calls, a new key is generated every time a connection is made, which further protects the security and integrity of the data. This means that if an encryption key from a previous call was discovered subsequent calls would not be compromised

Video Encryption Interoperability Standards

Video codec specifications include:

- VP8 (WebM), H263, H263-1998, MPEG-4, Theora and H264
- Resolutions from QCIF (176 × 144) to SVGA (800 × 600)

2.5 Encrypted Instant Message (IM)

- Off-The-Record (OTR) messaging is a cryptographic protocol designed to provide encryption for IM conversations. It ensures that messages do not have digital signatures and therefore cannot be monitored.
- Auto encrypted single/unique single session
- 3G and 4G, EDGE, GPRS, LTE, UMTS, HSPA, W-CDMA and Wi-Fi
- Peer to Peer - with no servers in the middle, already decentralized
- No records of any messages or conversations are stored, with a decentralized archive toggle options
- AES symmetric-key, Diffie-Hellman and SHA-1 hash algorithms
- User sessions are automatically deleted after a session is terminated

The application operates in standard un-encrypted mode for normal conversations. If a secure conversation is required, the user can easily activate secure mode and initiate an authentication phase. This allows the user to verify the identity of the other party through a pre-arranged password, a question and answer combination or fingerprint. Once authenticated, the application generates short-lived, session-based encryption keys that provide secure communications and perfect forward security. This ensures that the discovery of a past key does not compromise the security of future sessions. During secure IM conversations, digital signatures are removed and logging is disabled to ensure deniability.

2.6 Notification of Screenshots

An innovative security feature of the PryvateNow app can detect when a screenshot is taken from within the app. When this happens, the app automatically notifies the sender that the recipient is making a record of confidential information.

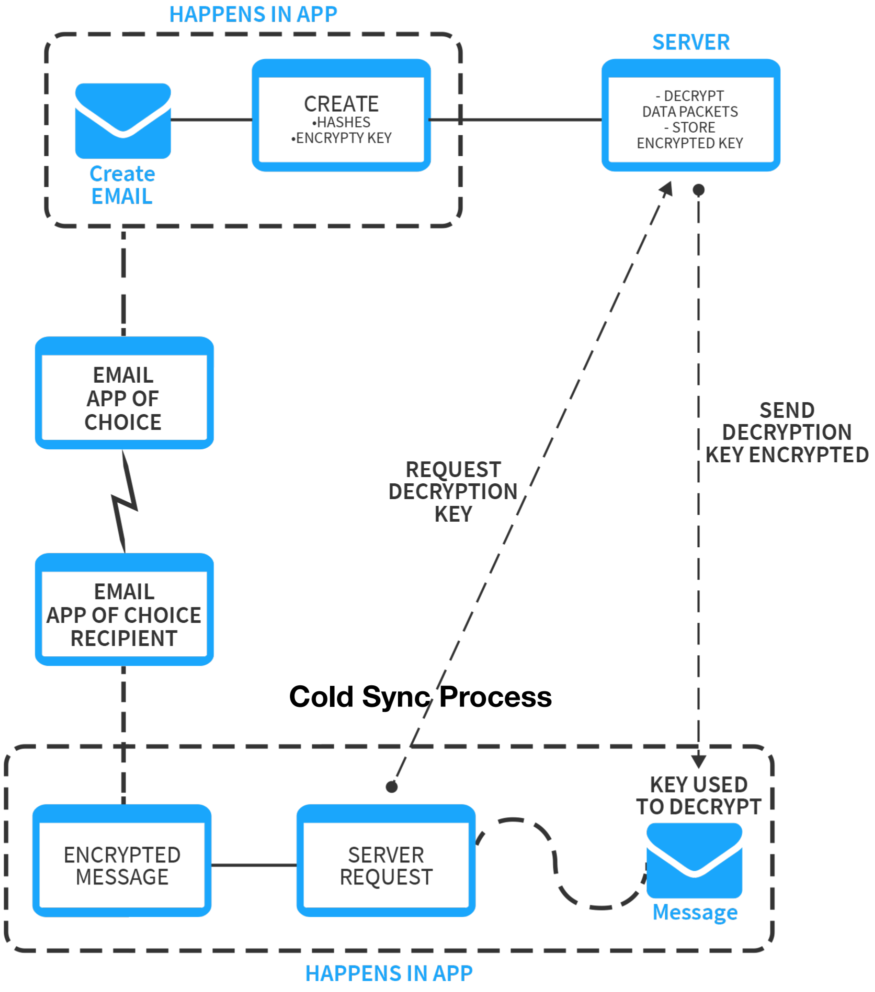
2.7 Encrypted Email

Email encryption software is intended to eliminate the risks posed by network eavesdroppers. In general, email communications are passed through the ether using unprotected protocols such as SSL/TSL. Emails are therefore transmitted in plain text across local networks on the internet, and as a result, messages and attachments can be easily intercepted and read by malicious parties. It is not just potentially sensitive information that is at risk, like banking details and login credentials, hackers who gain access to email messages can access content from users and their contacts and even hijack their entire email account.

The PryvateNow app allows its users to:

- Securely designate any or all current email addresses
- Communicate from Android to IOS and vice versa
- Easily be integrated and maintained by the IT staff, users can keep their existing technology and procedures and forget retraining for new platforms
- Send and receive on 3G, EDGE, GPRS, UMTS, HSPA, W-CDMA & Wi-Fi connections
- Achieve total security with that keys are automatically created on user's smartphones for each individual email , with the associated single-session keys never stored or revealed to Pryvate

This not a mail client. It contains only the protection mechanism required to make a user's emails secure, assure them that no unsecured data will ever remain or leave the device and that encryption data will be stored separately from the key on Pryvate servers. By separating the encryption and the key, we have a built-in added layer of security and have removed the need for users to input additional SMTP/POP3 settings when setting up their client.



Email Encryption – Technology Specifics
Our security protocol goes far beyond that proposed by the British Standards Institute:

- All communication between a user’s app and the server is fully encrypted, TLS-based or RSA4096-protected
- Key material that is encrypted for sending to the server in-device is achieved by using the public key of an RSA4096 key pair
- The connection between app and server is unbreakable with current techniques and technology
- The return communication, to the app from the server, is protected by the AES 256-bit key that is sent to the server (RSA4096) and it can only be read by it
- A key is newly generated for each communication session and never stored
- A TLS-certificate secure link which adds to the security and helps avoid ‘man in the middle’ attacks and is in accordance with BSI TR-03145

Pryvate uses true and tested public algorithms, like RSA4096 & AES256, in international implementations that have no backdoors. This is a requirement of BSI TR-03116-4, and additionally all DNS requests are routed through our servers and are compliant with DNSSEC.

Once the message is encrypted and encapsulated in a .pry attachment, it is sent directly to the user's current mail client on their device, hopefully in a DNS-based Authentication of Named Entities (DANE) compliant mail transport. Because Pryvate has no control over the user's choice of email client, we make the data as secure as possible by separating the key material from the data.

Pryvate complies with Datenschutzanforderungen (BDSG) and Richlinie BSI TR-03108, which makes our product one of the few software tools that are above the level of security highlighted in Sicherheitskonzept TKG- ISO27001.

2.8 Secure File Transfer & Storage

Our secure file transfer & storage:

- Eliminates the risk of any files transfers being intercepted in transit
- Sends and store files and data while protecting it with military-grade encryption, be it from a personal device via email or by using file sharing programs such as Dropbox, OneDrive or Box
- Secures file transfers and keeps them safe in storage even when not sent
- Allows for transfer of encrypted files to mobile devices and media storage like CDs, DVDs and USB flash drives
- Never keeps the decryption keys on the same device or file location, when a user's data is stolen, their files and data remain secure
- Allows secure transfers to be made via de Secure Copy Protocol (SCP) with no limit on file size, without the need to send files to ensure their encryption
- Accomplishes decryption by using the same method as encryption
- Does not require additional software
- Works with very large files: when users want to encrypt them and have them handed to a third party on a storage device, the SCP automatically encrypts the files and stores them within the app's inbox. When the recipient, a third party, receives the file, they can simply click on the .pry message and securely open it

2.9 Pin-Encrypted Mobile Protection

Additionally, we have an extra layer of security. To protect access to our App there is a PIN that acts as an extra activation code - making eavesdropping impossible.

2.10 Multiple Account Management

It is standard practice in most businesses for employees to not be allowed to manage their own email accounts. The installation and activation of all corporate software is invariably handled by security officers, IT staff or line managers, with the unfortunate consequence of overwhelmed centralized departments that find it hard to keep track of the state of their own network. To enable greater network transparency, Pryvate built a management dashboard that allows authorized employees to see which accounts are active, the amount of licenses being used or still available, and the associated costs. This results in greater security for an organization as well as better usability and awareness for HR and IT departments.

2.11 Secure managed conversations

The Pryvate Gateway can collect all of a user's voice communications and transform them into text to enable advanced text analytics. The Pryvate Gateway text analysis routinely adds metadata to a user's conversations, an indexing that makes for easy filtering and retrieval allowing a user to extract additional knowledge. Connecting all of a user's voice communication channels, whether incoming, outgoing or internal, it converts every call to text and stores them in real time capture. This transcription and analysis of calls will be available in an upcoming release, where rules based and machine learning routines will be applied, adding indexing and analytics and readying data for all kinds of in-depth analysis.

The Pryvate Gateway will encrypt both file recordings and transcriptions with its own military grade technology, ensuring that all of a user's conversations are always entirely secure. Transcribed conversations will use a fraction of the storage required by call recording, depending on the quality of the recording and its compression level, a recording file may be up to 10MB per minute while a transcription file will use less than 10KB. This will unlock some cost-savings but most importantly it will allow organizations to apply the same strict retention policies to voice communications that they apply to other communications and records.

Storage periods can be increased from weeks to years and records can be linked to customers, deals or processes as required. Text analytics applied to the recordings and other types of communications, be it email, SMS or social media, will unlock a whole range of possibilities:

- Reviewing of all calls for whatever purpose, like compliance, mandatory Q&As or training
- Easy identification of compliance breaches
- Assessment of customer mood and early identification of issues and opportunities

The combination of the these three functionalities allows a user's organization to:

- Manage incoming and outgoing voice communications
- Unlock knowledge hidden in current practices
- Discover opportunities for improvement
- Expand Manageability in all sorts of processes

Some of the current features of our Secure Communication Management are:

- Quasi-real-time, under 5 minutes after call transcription
- Immediate rules-based meta-tagging and indexing
- Integration with PBX, call centre, cloud call centre and internal VoIP
- Encryption of all saved data

We are currently preparing to deploy future features like:

- Separate recordings of each call participant
- Analytics integration for email, SMS and social media
- Real time transcription and analytics
- Alerts for pertinent supervisors to support agents or correct performance
- Mobile-to-mobile conversation transcription and analysis within the Pryvate App
- Recording of meetings

2.12 Anti-Blocking

Pryvate has developed a VoIP anti-blocking solution for users who wish to bypass illegitimate firewall restrictions on 3G networks. Numerous countries block voice-over-internet protocol (VoIP) calls, as they are seen as a:

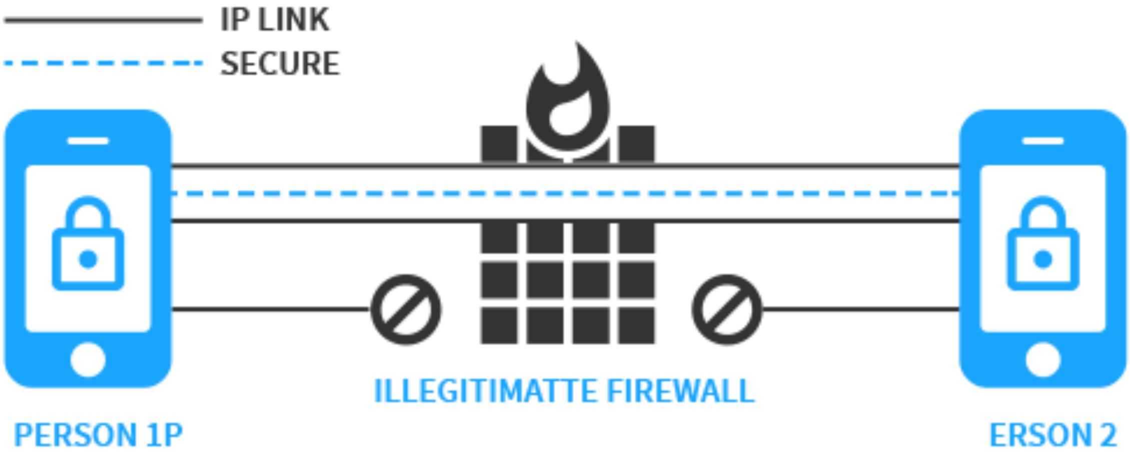
- Drain on the revenue of their telecommunications companies
- Way of evading the control of governments and their security services
- Set-up statistic collection system for every call made through the app.

When making a call, a Session Initiation Protocol (SIP) is used to allow two endpoints to shake hands, then a Real-time Transport Protocol (RTP) carries the traffic. Our system works in real time by tunneling the SIP and RTP traffic into a single encrypted HTTPS connection, using flexible virtual 'tunneling' architectures to achieve seamless voice and video calls.

Pryvate uses a 'tunnel client library' that is integrated into the user's Apple or Android device, and a tunnel server that is deployed inside Pryvate's network infrastructure. The tunnel server uses the data of each secure connection to recreate the SIP and RTP traffic from the client's smartphone. We tunnel all SIP and RTP traffic through a single, secure HTTPS connection up to a de-tunnel-iser server.

It is not just a general purpose VPN. Our solution comprises:

- A tunnel client library integrated into the Pryvate client for iPhone or Android
- A tunnel server that is deployed within our network infrastructure and that re-creates the SIP and RTP traffic from the data of each secure connection to the clients
- Our client and server software optimized to minimize the latency inherent in TCP encapsulation of VoIP traffic



3 Hybridization

How is Pryvate's offering of secure communications products interacting within a blockchain environment? We are ready to implement two fully independent systems for each particular service we currently offer, options that will allow users to pick between a centralized or decentralized service on either mobile or desktop, to better suit their specific needs. Along with the main focus of providing a hyper secure cold crypto storage wallet that also works as a hot wallet - from a dual containerized sync process.

3.1 Voice / Video / Messaging

Our current peer-to-peer chat and video functions are already considerably de-centralized in nature, and we will be implementing additional features for user preferences, such as a chat archive, video and picture sharing, archiving and deletion. We are currently exploring the best hybrid technologies utilizing the Blockchain.

3.2 File Storage / Archival, IPFS with all user data stored in an fully-secure encrypted form. Data security will be provided by duplicating data on multiple nodes. This feature will be available for the dashboard. We are currently exploring the mobile potential of IPFS.

3.3 Pryvate Crypto Wallet

One of the Pryvate ecosystem's most exciting new features will be a new highly secure, containerized, lightweight crypto wallet, fully built into our application. After a user downloads the PryvateNow app, they will be given a unique, randomized, 24-character hash identifier which should be stored in a safe place. Within the application, a highly secure, containerized, lightweight/Micro/Internal wallet will be built enabling users to safely store, convert and transfer Bitcoin (BTC), Ether (ETH), PryvateCoin (PVC) and any other ERC20 compatible tokens, with further development achieving 'global' acceptance of other currency adaptation models, based upon the consensus of users.Primarily, transactions between cryptocurrencies and tokens will be available between users via their ID or nickname, and with the native addresses of Ethereum and Bitcoin. For an extra layer of security, Pryvate will create a one-time address for each transaction, native to the original ID address, that will be immediately and effectively destroyed after each transaction is validated and completed.

All operations will be performed directly by the application in the blockchain, using JSON RPC interaction with the node of the corresponding blockchain, no participation of intermediate servers and services will be involved. The node selection function, including a local one, will be available, this solution ensures the transparency and security of all payment transactions and allows for:

- Sending and receiving encrypted messages, smart contracts and payments from trusted contacts
- Browsing, chatting, and interacting with decentralized applications and the PVC community
- Storing, controlling and trading of multi crypto-assets with the built-in PVC wallet
- Push notifications and alerts about prices
- White label solutions
- Retrieving and archiving transactional documentation safely
- Setting prices of the cryptocurrency in which users want to trade, whenever the price goes up and down, the wallet will notify them automatically.

https://www.trustology.io/single-post/2018/01/18/Improving-Global-Investing

3.4 Two-Wallet Solution

The fully-secure Pryvate Crypto Wallet will solve the hot wallet versus cold wallet conundrum where a ‘hot wallet’ is connected to the internet for easier spending, and a ‘cold wallet’ is not and thus far more impervious to attack. With Pryvate’s secure wallet and its patent pending bi-directional sync method, a hybridization of hot and cold storage all from one device will be always available, with no extra storage needed and total-security provided for both mobile and desktop environments.

The most valuable tool of the private wallet is the ecosystem in which it has “containerized” itself in: a unique hybrid option of decentralization of which the main focal point is the capability of a truly offline feature from within the wallet with the help of a ‘dead man’ switch. These switches are usually used as a form of fail-safe, to stop an unoperated machine from potentially dangerous action or to incapacitate a device as a result of accident, malfunction, or misuse; but in this case they work as described in figure #

3.5 Three Methods

The Pryvate Wallet employs three cutting-edge methods: Lightweight, Micropayment and Internal/Atomic Swaps.

1. Lightweight means that while using a light client or Simplified Payment Verification (SPV) wallets, crypto-assets and private keys are stored within the wallet and encrypted locally on device, with triple-layer protection. The wallet only downloads a specific portion of the blockchain saving a substantial amount of storage space and sync time, with the list of transaction records included within a block arranged in the form of a Merkle Tree created from the hash values of those transactions. The root node, or Merkle Root of this tree, has a locus to all of the transactions contained in the specific block. SPV wallets download the block headers of all the blocks included in the blockchain, which is communally much smaller in size when compared to the full blockchain. To verify a transaction, the light or SPV client requests for the Merkle Root of the block to which the transaction belongs to from certain full nodes in the blockchain network. The client also requests these nodes for the minimum information, or hashing partners, required to calculate the Merkle Branch.

2. The Micropayment protocol allows one party, the client, to make repeated micro-payments to another party, the server, in a two-staged approach: first, a particular value is locked up with a multi-signature transaction that places it under the control of both parties; the parties then cooperate to create a signed refund transaction that sends all the value back to the client. Second, the operation is time-locked by using the Locktime feature of the Bitcoin protocol, to ensure that the refund won’t go into effect until a period of time has passed. The refund transaction is prepared in such a way that the client gets a fully signed copy before the initial multi-signature transaction, the contract, is sent to the server. In this way, a potential crash or attack that could cause the client to lose money is circumvented, once the client receives the refund transaction, only then is the money locked back into both parties’ control. If the server halts at any point in the protocol, the client can always get their money back.

3. Internal/Atomic Swaps are a major advantage of internal or inter-app smart contracts created off-chain, this allows them, once created, to interact extremely fast with other participating parties. This also has important privacy implications, namely: a user’s interactions stay off-chain and are kept secure, only in cases of disagreement will a transaction will be submitted on-chain, where users in the p2p model use consensus from trusted peers.

3.6 Enterprise Multi - Sig Wallet powered by Pryvate

Pryvate is addressing the unique challenges of the current hacking epidemics of fiat and cryptocurrency exchanges, by extending our expertise and technology to the securing of these platforms. Currently many crypto-exchanges take on their own custody duties and enter a risky duplicity. In most regulated markets there are laws against an exchange acting as a custodian, both to ensure segregation of duties and to reduce systemic risk. Exchanges and custodians essentially need different business models: one charges for transactions, the other for safeguarding. Assets should be held in segregated accounts so that the owner always knows the reason for a transaction, and never in omnibus accounts. Hence the ideal scenario is a self-custodianship exchange.

3.7 Risks of Cryptocurrency Wallets

The primary security threats to cryptocurrency wallets involve either user behavior or the security features of each individual wallet.

- **Network Traffic Threats**
  Network traffic is frequently targeted by man-in-the-middle (MITM) attacks and HTTPS certificate hijacking.
  Solution: ZRTP SAS for Real time content Chat & VoIP. Email with MITM protection.

- **Internet Browser Threats**
  Hackers can exploit security loopholes within browsers, as well as browser plugins to access users' account information.
  Solution
  The Pryvate browser is solely intended for user navigation, no transaction or any other operation takes place there.

- **Password and Account Hacks**
  Many people utilize the same name and password to register with multiple websites. If hackers are able to figure out your login information on any one of these websites, they can use this information to access your account on a cryptocurrency exchange, after which they can easily steal your digital assets.
  Solution; X (2+)-FA, including biometric, geofencing, at app opening and for any transactions higher than threshold.. Possibility of one form to be similar to 3D secure as we hold mobile #

- **The Dangers Of Entrusting Private Keys To Cryptocurrency Exchanges**
  Many people allow their private keys to be stored on the servers of different service providers, and all cryptocurrency exchanges store users' private keys in this way. If users want to manage their assets on these types of platforms they are forced to perform the following actions: 1) Register on the service provider's website; 2) Log onto the service provider's website using their account information; and 3) Perform actions within the website. Just by completing these few actions, users have exposed themselves to at least four potential security threats.Every year numerous exchanges are successfully hacked leading to enormous loss of assets. Because cryptocurrency assets are anonymous and can't be traced, once digital assets are lost or stolen, they can never be recovered.

  Solution: AFAIK we are offering Thick client/apps only, so private keys never touch any servers.

- **Key-logging hacks**
  Key-logger can be either a software program or a hardware that is used by an attacker to record the key presses on a user's keyboard. Using a Key-logger, an attacker can remotely get to know your passwords, credit/debit card numbers, messages, emails and anything you type. Typically it is a software program, unless the attacker has had prior access to the devices
  Solution: By utilizing encrypted safe keyboard technology, digital wallets can greatly increase user safety when entering in their PINs, although the potential attacker will be able to log your keystrokes, they'll be presented to him in a scrambled and unreadable encrypted format.

- **Operational Environment Risks**
  Cryptocurrency wallet files, private keys or mnemonic phrases, are stored on a terminal device. Either from a PC or a mobile phone, if your terminal device is hacked, it represents a major risk to these files. A safe digital wallet needs to protect your private keys from being stolen, regardless of the operational environment. Operational security risks include virus software, operating system vulnerabilities and hardware backdoors.

  Solution: Keys are only stored encrypted; only X-FA can unlock them, with dead man switch protection on top.

- **Virus Software**
  One difference between cryptocurrency wallets and traditional banking or payment software is that with cryptocurrency wallets users have no way of reporting lost or stolen assets. Cryptocurrency wallets don't even allow you to freeze your account once you notice your assets are disappearing. Once a hacker gets a hold of your assets, they are gone forever.

  Solution: Although they can't help recover lost assets, safe digital wallets are able to avoid this situation in the first place by scanning your PC or phone for viruses and other potential threats.
  Desktop dashboard would do the same. Mobile app are not authorized to perform any actions at the OS level, but surely they will check as much as they can their surrounding environment (OS level up to date)

- **OS Vulnerabilities**
  Hackers have the capability to bypass an operating system's security barriers or sandbox, and could therefore view a users' digital wallet private keys. Android, iOS, Windows or Linux, every year an enormous number of security vulnerabilities are exposed, including local kernel vulnerabilities.. Currently the security capabilities of the majority of cryptocurrency wallets trust on the security barriers of operating systems. Many still

operate on static passwords, such as; plain text passwords, for the storage and management of private keys, or on operating system security barriers to restrict visits from other apps. Due to the lack of safeguards against operating system loopholes, if users of these wallets install apps that contain local kernel vulnerabilities, their digital assets could potentially be susceptible to attack.

Solution; Cold Storage - In app using a proprietary bi-directional sync. Limit the use of OS APIs and use native code in C libraries (C own Frameworks for iOS & JNI Libs for Android).

- **File Storage Security Risks**
  The way in which PC and phone devices store a digital wallet private keys is of utmost importance. They usually use plain text storage, or if they use encrypted storage, the secret key for decryption is hard coded into the source code without any security safeguards.

  Solution: Access permissions for the private key file storage directory, private key storage formats, and encryption algorithms must all be designed accordingly.

- **In-App Security Risks**
  These are primarily found within an app's install package. Whether or not app install packages contain anti-tampering features is extremely important. Additionally, memory security during app usage, reverse debugging capabilities, the life cycle management of private keys, the secureness of the debugging log and the security of the development process all must be designed to protect against potential abuse.

  Solution; Deadman switch, additionally, checksum into onboarded critical C libraries / custom framework.

- **Data Backup Security Risks**
  If mobile apps are able to be backed up, then hackers could potentially enact brute force attacks against private keys and mnemonic phrases. For example, if an app enables android:allowBackup as its default setting, then the app's data files are backed up using the operating system's backup mechanisms, which means a digital wallet private keys are also being backed up to an external medium.

  Solution: Wallet data is stored onto local app close cell (not backable / not cloudable area).

3.8 Decentralized Email

- Using the latest available technologies available for the peer-to-peer framework
- Front end written in Javascript and hosted on the IPFS (or similar) decentralized platform
- Replacement of the server by smart contracts enabled by Ethereum
- Contents are encrypted by OpenPGP, and/or other open source libraries
- Key-pair is generated on the basis of the Ethereum function sign()
- Anonymous, Aliases, with no central Server
- Toggle ability to change from centralized, like Gmail, to decentralized depending on specific needs.

3.9 Pryvate Dashboard

The Pryvate desktop dashboard is a powerful tool that allows for our users to track their cryptocurrency and offers the same set of tools available from the mobile application. The Qt 5.9 (QML) graphical interface is running on GNU/Linux, Windows and Mac OS X.

Specific Features

- HD video calls in full screen mode
- Call recording (audio & video)
- Smart search bar
- Unified history
- Quick access through my recent events
- Ability to create audio conference calls instantaneously

Portability

- GNU/Linux: x86, x86-64, ARM v5, v7, arm64 ; Debian 7/8,
- Windows Desktop: x86 (works also on x86_64), Windows 7 and later
- Mac OS X: x86_64 ; 10.11 and later.

Overall Features Common With Mobile App

- Audio & HD video calls
- Multiple calls management with pause & resume options
- Call transfer
- Audio conferencing, ability to merge calls into a conference
- Instant Messaging with message delivery status (IMDN)
- Pictures and files sharing
- Call History/Contact list
- Display of advanced call statistics
- Echo Cancellation
- Call quality indicator
- Presence status
- Chat access during calls
- Secure communications: zRTP, TLS, SRTP
- URI handlers for connecting OS events like Calendar calls (link in ICS)

Advanced Features

- Audio codecs: OPUS, SILK, SPEEX, G722, AMR-WB (G722.2), AMR-NB, GSM 6.10, ILBC, G729, ISAC, BV16, G711, Codec2
- Video codecs: VP8, H264, MPEG4
- HD video support
- Integration with push notification
- ICE support (RFC5245) to allow peer to peer audio & video connections without media relay server
- Low bandwidth mode for audio calls over 2G networks.
- Call handover across network access type change (start a call in wifi and continue in 3G)
- IPv6 (dual stack and v6-only support)
- DTMF with RFC4733

Enhanced features for Cryptocurrency management

- Blockchain explorer
- Watch only mode for crypto assets
- Atomic Swaps
- Trade Alerts
- Bounty management for supported erc-20 tokens
- Portfolio management
- Send receive payments
- Built in ERC -20 token wallet
- Dead man switch - user sets their own parameters
- Dapps

3.9 Encrypted Secure Web Browsing

Built into APP - TOR web browser for security

4 PERFORMANCE REQUIREMENTS

4.1. System Maintenance

The system is always available online 24 hours per day, 365 days per week with the exception of scheduled and pre-notified system maintenance downtimes. In the event of any maintenance all users will be notified accordingly. We do not foresee any major downtimes during scheduled maintenance.

4.1 Failure Contingencies

Failures & Fault tolerance within the network

We address this on multi levels the first being the deployment of fault tolerant byzantine hybrid processes. A general overview is described below.

Authentication detectable byzantine failures
In this case a server may show byzantine failures but it cannot lie about facts sent by other servers.

Performance failures
While the server is conveying the correct values, they arrive at the wrong time, either early or late.

Omission failures
The server is replying “interminably late”.

Crash failures
When a server suffers from an omission failure and then stops responding.

Fail-stop failures
In this type of failure, the server only presents crash failures, but at the same time, we can assume that any correct server in the system can detect that this particular server has failed.

4.3 Customization and Flexibility

“We grow - we adapt”
One size does not necessarily fit “All” is Pryvate’s approach. Using a “skunk werks” methodology. “Skunk werks” is a term conveying the “experimental laboratory [...] of a company or institution”, and it is also the philosophy that allowed Pryvate Ltd. to come up with the best hybridization of state-of- the-art technology - and the foreseeable future.

EQUIPMENT AND SOFTWARE

4.4 Equipment

Pryvate has chosen to locate their infrastructure within a tier 3 colocation facility in Frankfurt, thus offering complete security of both network and structure. Our equipment is connected to the three largest internet exchange points with direct connections to the largest carriers such as Level3, Global Crossing and

Deutsche Telekom. These carriers are responsible for most of data transfer in Europe. Our equipment uses redundant power supplies backed up with fully redundant UPS and generators. Physical security and access is covered by biometric access controls and CCTV with fire detection with F-90 zones and smoke-proof doors. We have 24/7 monitoring in place with personal backup if failures exist. DDOS prevention is across the platform mitigating any attacks and minimizing service outages.

4.5 Software

Core of the communication system is made of an active-active cluster, running on native hardware (no virtualization) for the highest response time.
Operating System : Linux
Telecommunications server software : In house customized SIP Server and antiblocking tunnel.
Database : Mysql
The only role is to route encrypted message from one device to the other, and send push notification to “wake up” mobile application upon reception of message or call.

4.6 Interface / UI

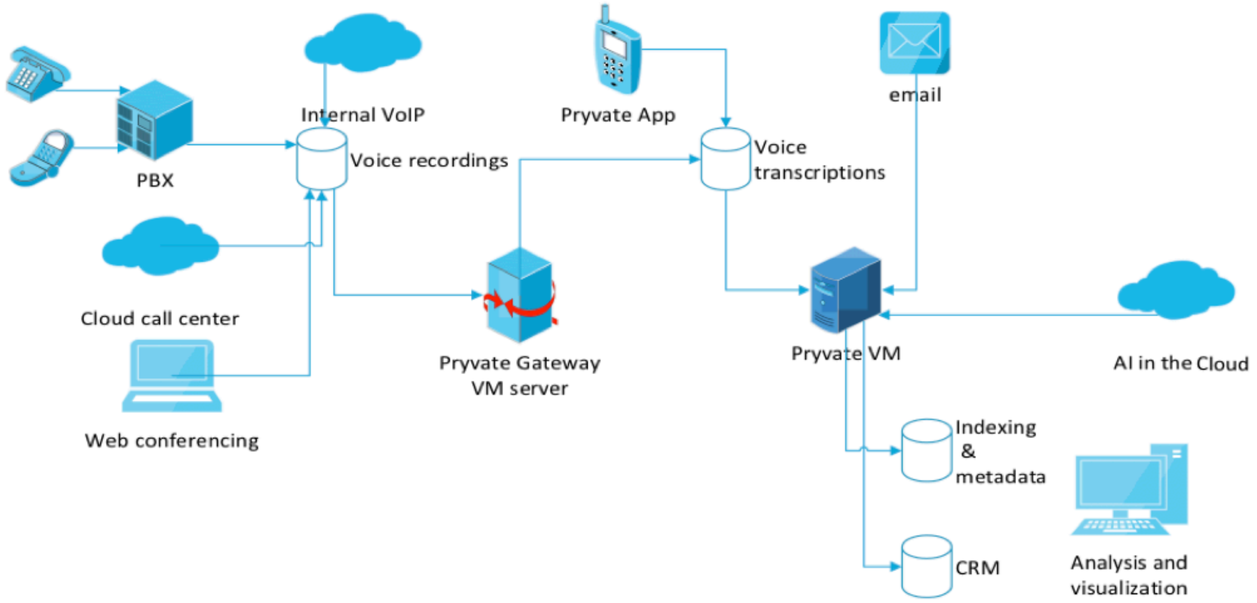
One of he most important functions of any application/platform is a seamless, easy to use user interface (UI) - we are continually improving our design - from under the hood to the top of the SCP - design and functionality is a top priority second to security.

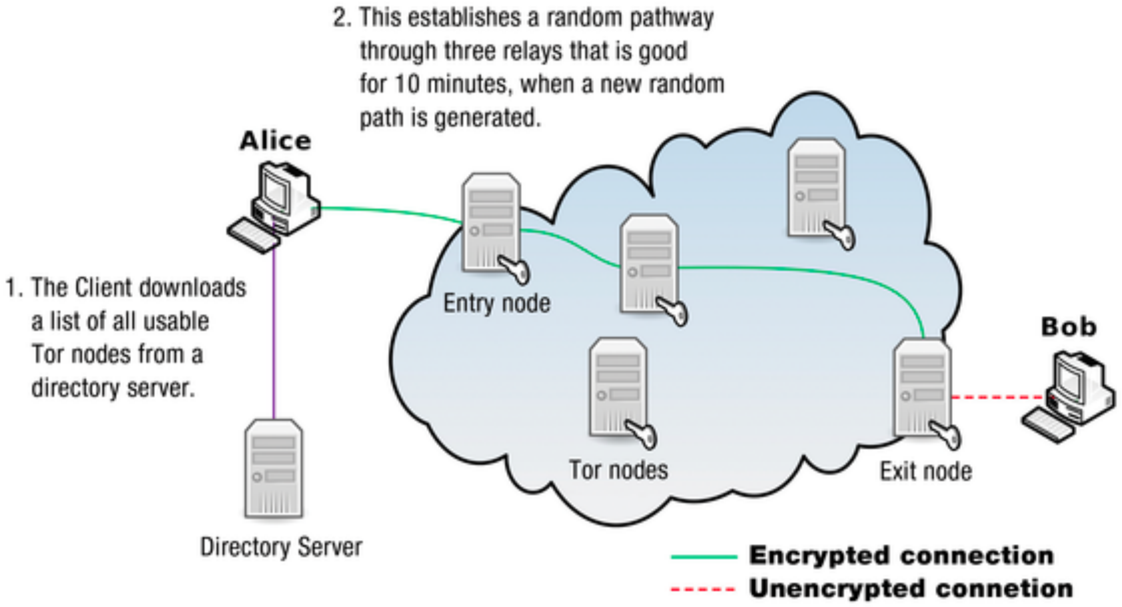
5 Conclusion

Pryvate Ltd.’s goal of establishing an easy-to-use, cross platform, multi-use utility that simultaneously provides invaluable services and grows PVC’s value is a remarkable one. The fully secure ecosystem that the PVC token will allow to develop, is of vital importance to the world in which we live today, where the overreaching arms of corporations, state forces and malicious actors routinely invade people’s privacy. Accessible, military-grade encryption fully integrated into communications and cryptocurrency trading platforms is the elegant solution proposed by Pryvate Ltd. Their technology deserves to be on everyone’s mobile, desktop, crypto exchange and wallets.

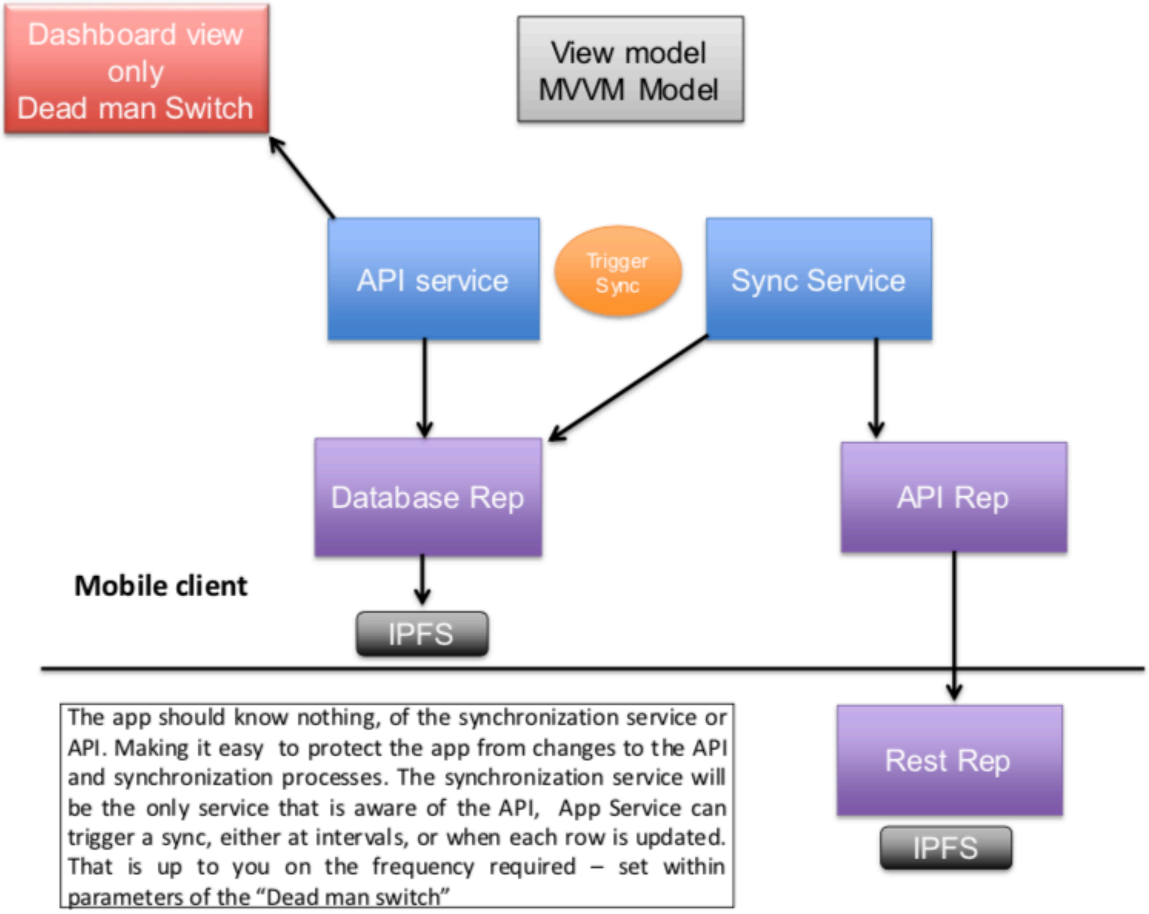
6 APPENDIX

Managed Conversations




2. This establishes a random pathway through three relays that is good for 10 minutes, when a new random path is generated.
Alice
1. The Client downloads a list of all usable Tor nodes from a directory server.
Entry node
Tor nodes
Exit node
Bob
Directory Server
Encrypted connection
Unencrypted connetion

http://www.linux-magazine.com/Issues/2015/170/SelekTOR#article_f1



The app should know nothing, of the synchronization service or API. Making it easy to protect the app from changes to the API and synchronization processes. The synchronization service will be the only service that is aware of the API, App Service can trigger a sync, either at intervals, or when each row is updated. That is up to you on the frequency required – set within parameters of the "Dead man switch"