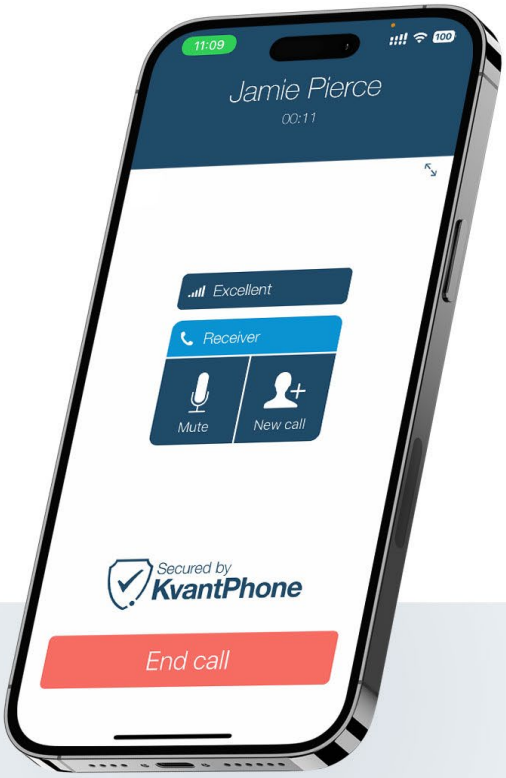
KvantPhone

White Paper



Arenim

Table of Contents

Protecting Voice Calls

Voice calls are an important part of the modern private and business life. People usually freely share their private lives on the phone without considering who might be listening. For the average person this might be a safe consideration: his personal secrets are not that interesting to others. Well known individuals or business representatives might have more to protect.

Regardless of the many cases of wiretapping portrayed in popular movies the usual opinion is that the public landline and mobile telephony networks are quite secure. Unfortunately this is not true in either case. Landline phones are connected with copper wires that are only protected by physical means that provide different levels of protection depending on the location. Since GSM communication happens on easily accessible radio signals it is encrypted, but this encryption is not strong enough and it can be broken easily with simple equipment.

Operators are another weak point in voice call security. Most telephony networks are designed to allow the interception of the voice stream of the calls. This is mandated by government regulations in all the countries to allow legal interception. Since the capability is there it only depends on the internal security procures of the telephony operator how hard is to exploit this by an attacker. This is even true for VoIP operators that provide strong encryption from the customer equipment to their central servers.

Strong encryption can provide an unbreakable protection for voice calls, but this excludes third parties only if the encryption happens end-to-end – directly from the device of the first participant to the device other party.

End-to-end Security

Advances of modern cryptography allow the protection of voice calls without relying on third parties or allowing possible attacks by middle man. End-to-end security relies only on the protection of the end device and thus gives the control into the hands of the end user.

Symmetric key encryption, when used properly, can provide a practically unbreakable protection for data transmission. The AES-256 cipher, which is approved for top secret documents of governments, cannot be broken by brute force attack using all the energy the Sun can provide even if we assume the greatest technological advancements in the current transistor technology. Even futuristic solutions like quantum computers would only make it somewhat easier to brake an AES cipher and it would be still practically infeasible. Advances in cryptanalysis could find methods to break a symmetric key encryption but this is considered improbable in the foreseeable future.

Symmetric key encryption provides top secret protection for the voice data but needs a shared secret between the two parties. In practice this would mean personally exchanging one or more 30 character passwords before making any calls. This could easily become inconvenient. Fortunately Diffie-Hellman key exchange and asymmetric key encryption make it possible to securely exchange a shared secret during the establishment of the connection.

The Diffie-Hellman key exchange allows the parties to establish the shared secret over any insecure channel. The shared secret is established without ever sending the secret itself. Both parties create random secrets that are never sent over the wire directly; only a derived value is sent over that is practically not possible to reverse. The shared secret is calculated from this derived value and their own secrets. All the values are publicly sent over the insecure channel except the base secrets and the derived shared secret.

The Diffie-Hellman provides a perfect shared secret for symmetric encryption but it does not contain authentication. The shared secret provides a secure channel but we cannot be sure who is at the other end. Public key cryptography provides a way for peer to peer authentication without relying on a central authority. Both parties generate secret private keys and their derived public counterparts. The public keys are exchanged in a secure way in advance. During the Diffie-Hellman key exchange a digital signature is added to key parts of the exchange, that can be verified using the public key of the other party. This ensures that the established shared secret provides the secure channel to the person we intended.

KvantPhone Solution

During the design of the KvantPhone service, the aim of Arenim Technologies was to provide the very same feature set and user experience available for normal calls and messaging. The only difference: KvantPhone is completely secure.

KvantPhone is a voice over IP (VoIP) solution that provides superior quality voice transported over the Internet. It is based on an industry proven voice engine that provides very low delay even with encryption.

The voice calls are encrypted end-to-end using strong AES-256 symmetric encryption that is based on ephemeral keys setup using Elliptic Curve Diffie Hellman. This ensures that the calls are available to the parties of the calls and only during the call. Even if the devices are stolen and their protections broken past calls remain secure.

KvantPhone takes extra care to protect the sensitive data on the device. The access to the device is hardened by a service provided by the KvantPhone server that makes brute force attacks impossible.

Besides the strong security KvantPhone aims to fulfill the needs of business life by providing secure multi party conferencing and instant messaging features.

Professional administration interface

Business requirements besides security are satisfied by the built-in contact management features of the KvantPhone application and the professional administration interface designed for managers and administrators of your organization.

Contact management features are enhanced with a presence service. It is possible to see if contacts are available, offline, in a call or they don't want to be disturbed.

Professional user management options include the possibility to add KvantPhone users from outside the organization in a trusted and secured way. Collaboration between companies and organizations can also be administered and managed centrally by defining access and visibility rules and credentials.

Technical Insight

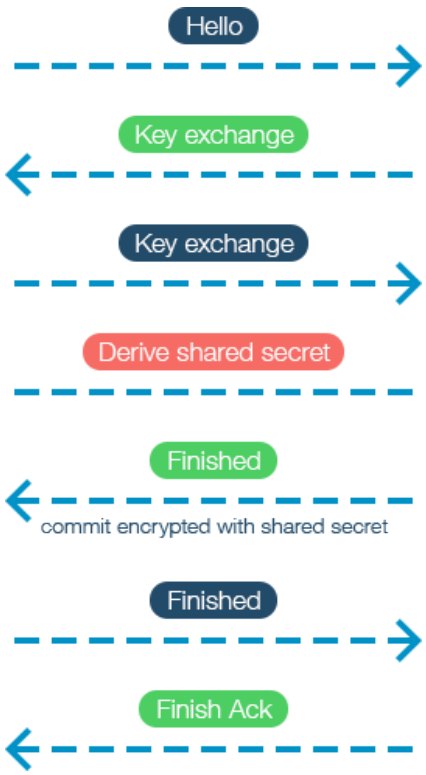
Voice encryption

The call between the two parties is set up using the SIP protocol using the servers provided by KvantPhone. The whole call setup is secured using TLS that provides transport level security to the servers. The voice content of the call is protected with **end-to-end security** built up after the call was connected by both parties.

When the call is connected the path for the voice media is established using the Interactive Connection Establishment (ICE) protocol. The aim is to find the simplest and shortest path between the two parties. This means that if both parties are on the same corporate or private network then the voice data will not leave that network; if they are on separate networks it will use a direct path on the Internet between the two networks. Only in the case when the direct path cannot be established (because of network address translation issues) will the ICE protocol select the use of KvantPhone Media Relay servers to forward the media. Using the shortest path possible ensures the fewest number of parties that are able to even see that a secure connection was established.

Key exchange

The secure channel is built up in this shortest voice path. Before any voice data is sent the key exchange procedure is started. The key exchange procedure is very similar to the procedures used in the industry standard Transport Layer Security (TLS) protocol, with the slight adjustment for the UDP transport protocol and with removing any unnecessary features.



TLS is a widely used protocol with many optional features and security levels. Until recently most of the web sites using TLS avoided the use of Diffie-Hellman key exchange because of the higher CPU costs associated with it. KvantPhone as a top security product only uses the highest security level and does not even support lower options.

The Diffie-Hellman with ephemeral keys allows for establishing a shared secret that is not in any way derived from data that is long lived. When the call is finished the shared secret is erased and it cannot be reproduced later even by the original parties of the call.

This feature provides **Perfect Forward Secrecy**: there is no way to decrypt the content of the call later even if the devices of both parties get compromised after the call.

Since KvantPhone is a mobile product it is important to conserve resources. For this reason a variant of the Diffie-Hellman method is used that is based on elliptic curve cryptography. It relies on the elliptic curve discrete logarithm problem instead of integer factorization and can provide the same security with much shorter key lengths. According to renowned cryptanalysts a 384 bit EC key provides approximately the same security as a 7680 bit RSA, but because of the smaller key size it requires significantly less processing power for encryption.

Since the Diffie-Hellman protocol does not provide authentication in itself the commit messages during the exchange are signed using RSA-2048 keys. The RSA private key provides the authenticity of the user and allows the other party to ensure that he is not speaking with an impostor (**Man-in-the-Middle protection**). The RSA key is only used for signing and never for encryption that further improves security. You can find details about how the private key is protected in the Device Protection section below.

The implemented key exchange keeps important features of the TLS that provides protection against **replay and bid-down attacks**.

Secure RTP

The actual voice data will be sent only after the shared secret was established with the key exchange. The voice is first encoded with a modern, wide-band voice codec to conserve bandwidth and then it is packed into the industry standard SRTP (secure real time transport protocol) for transmission. SRTP is a version of the RTP protocol that uses symmetric encryption to secure the transmitted voice data.

KvantPhone selects the most secure option for the cipher: **AES-256 in the counter mode**. As discussed earlier this provides top secret level protection for the transmitted data.

SRTP uses **key derivation** methods to create multiple keys from the single master key (the shared secret established during the key exchange). Separate keys are used for encrypting the voice data by each party to improve security. Also separate key is used for the integrity protection of the encrypted data. **Integrity protection** is an optional feature in SRTP because it slightly increases the bandwidth requirements but it provides thwarts attacks where a malicious entity captures the part of the encrypted stream and resends it at a later time trying to confuse the listener. It is not easy to achieve a successful attack this way since the attacker does not know what was said in the part he tries to inject. Nevertheless KvantPhone always uses integrity protection.

Device protection

The authentication of the parties in the call is based on the private key stored on the mobile device (as discussed earlier). To ensure the safety of the private key and personal data KvantPhone uses a multi factor protection that is based on 3 pillars:

- something that the user knows – a 6 digit PIN only known by the user
- something that he user has – the mobile phone itself
- external protection – KvantPhone servers contain part of the key

Traditionally the multi factor authentication can be also based on "something that the user is". This additional protection can be available with specific devices: IPhone 5 provides biometric authentication.

The private key and personal data (this includes call history and settings too) are encrypted with a key that is derived from the above three pillars. SHA-512 is used for the key derivation and AES-256 used for the encryption itself to provide maximum security.

The PIN provides the part of the key; this is something that only the user knows. For this reason the PIN is only temporarily stored by KvantPhone for the very short time until it is used. The PIN itself is never sent outside the device and it is not stored by the server. This ensures that it provides a protection that is separate from the other pillars.

The mobile device provides the possession factor. The attacker has to get access to the device and break its built in protections to get access to the part of the key. Modern mobile devices consider security as very important and if they are used in with high security settings (like PIN access and encrypted file systems) it is almost impossible for an attacker to obtain the secure keys. (In case of the IOS platform the part of the key is stored in the keychain that is locked the UID of the device and is protected by the PIN of system).

The third part of the key is only stored on the KvantPhone servers. This thwarts any attempts for a brute force attack on the PIN even if somehow it obtained the data protected by the device. The One-Time Password (OTP) method detailed in RFC4226 is used to authenticate to the server. The shared secret of the OTP is encrypted with a key derived from the PIN of the

user. The encryption used is AES-256 EBC. The decryption of the OTP key is protected against brute force attack by the fact that the result of the decryption is the completely random shared secret and the attacker cannot check its validity without contacting the server (the server will allow only a few tries before locking the account). For additional protection the encryption key derivation is bound to the device by using PBKDF2 with a salt value that is stored only on the device.

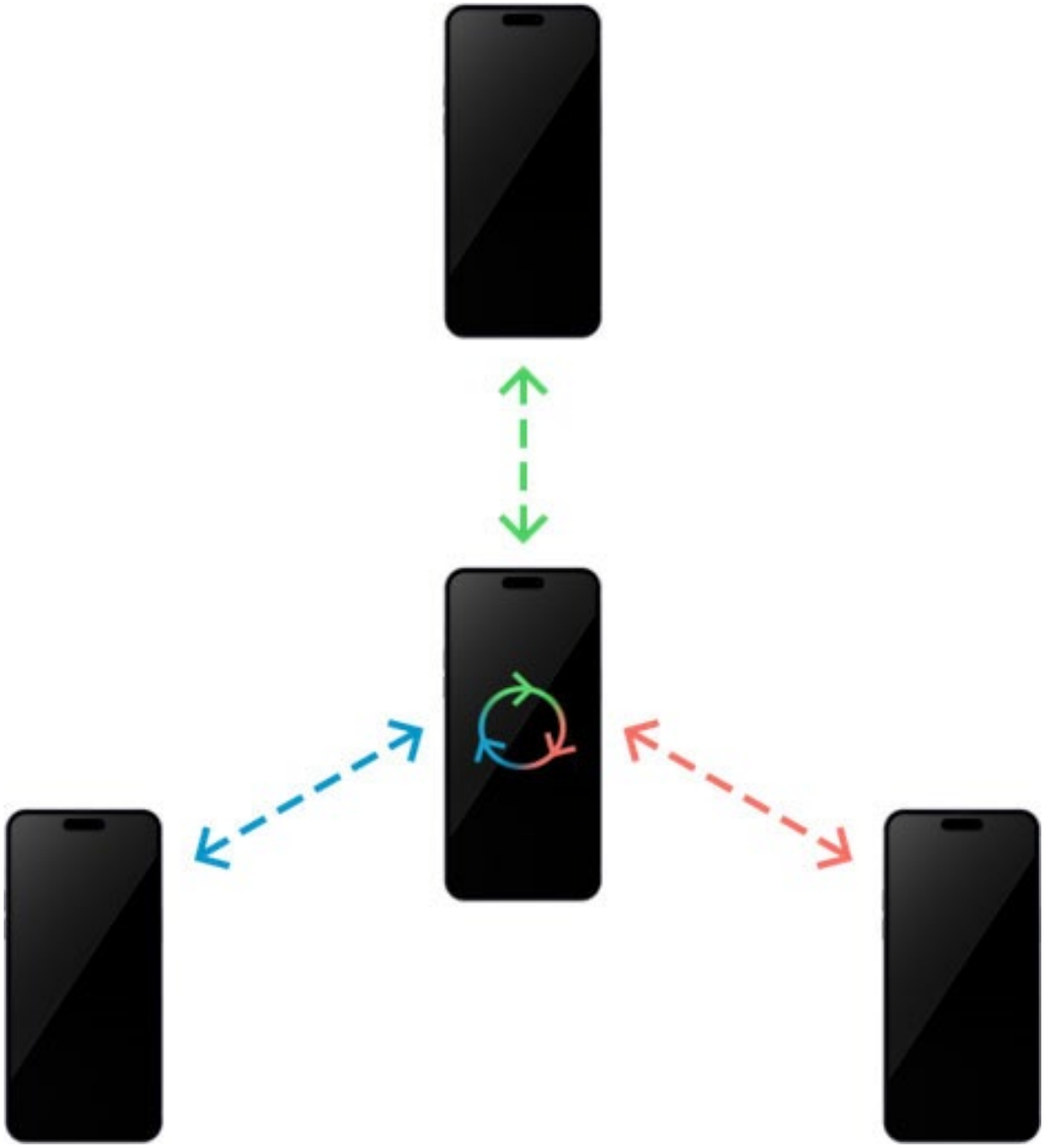
Using this multi-platform protection the private data can be accessed only after multiple attacks on the user. One possible attack is to somehow obtain the PIN and the device from the user. Without the device the PIN is worthless. Without the PIN the attacker has to obtain the device, break all its built in protections and also get access to the protected data on the KvantPhone servers.

Conferencing security

Conferencing is an important feature for the typical users of KvantPhone but its implementation has to provide the same end-to-end security as available for two party calls. Using an external mixer would require the creation of trust relationships between the mixing service and all the participants of the conference. In many cases this is not practical.

Mixing the voice data on the phone of the participants provides a much clearer trust relationship: each participant has to trust the party who has invited him to the conference.

The invited participants of a conference are connected using regular calls with end-to-end security and then the decrypted voice data is mixed and sent to all the joined parties in their encrypted calls.



Markets & Case Studies

Law Firm providing secure consultation

Eastern Europe & UK

Our primary concern is providing professional legal services to our blue-chip international clientele. Confidentiality is of utmost interest in our business. Nearly all of our assignments entail dealing with sensitive information and mishandling of data and information might seriously harm the interests of our clients. We were continuously searching the market for reliable technical solutions that provide us with confidentiality in our intra-team communication and also in our communication with clients. Thanks to KvantPhone our communication with our clients became more intense and also smoother, since we have been able cut out travelling time for personal meetings. We and more importantly our clients have been very pleased to use KvantPhone as a secure form of communication. Our clients save significant time and costs with KvantPhone and they regard access to KvantPhone as a professional value added services provided by our firm.

Energy Trader Co. protecting trade secrets

North and Eastern Europe

The energy business attracts a lot of unwanted attention of competitors, press and governmental agencies. A deal for us can move tens of millions of dollars. Success or failure is determined by whether we have the right information and if we are able to generate trust in our partners. KvantPhone has helped to achieve both. We are glad that KvantPhone is independent from any governmental body so we do not have to worry about the changing winds in state offices. Using KvantPhone we are also able to keep the press away from our business and we have to worry far less about them as we used to in the past.

Multinational Company reducing travelling costs

Europe, Latin America & Middle East

Our company runs a business in Europe with offices and professional staff in 23 countries. Due to our information security policy sensitive matters can mostly only be discussed in personal meetings. After adopting KvantPhone as part of our everyday communication practice, we recognized that our management team members tend to travel less to the HQ and can spend more time in the field doing actual business. Furthermore KvantPhone has just introduced a secure conferencing service. With the new conferencing suite we are able to replace some of our personal meetings. We have experienced an outstanding voice quality far better than on any of the mobile or fixed line services. As a result of fewer trips to the HQ we cut our travel

budget by 15% and our key people can spend more time with clients and less time sitting on planes.

Pharmaceutical Research Company

Worldwide

One of the main challenges we face in the pharmaceutical industry is the protection of our proprietary know-how. Our company runs clinical research in Eastern Europe, which means we are the link between the pharmaceutical producer and the healthcare professionals who run clinical research. Confidential communications in several directions, as well as efficient and secure administration of the results are critical factors to our business. Over the years we have been seeking a cost effective yet highly secure solution to this challenge. KvantPhone not only provided us with the safety we were seeking but also helped us manage projects more efficiently, and with lower costs. Health care professionals are not always IT experts, but the user friendly interface of KvantPhone made it very simple to use the software.

Multinational Advisory Company

Financial advisory

As an adviser company specializing in financial transactions, it is crucial that we have a safe channel not only to communicate with our offices worldwide, but to provide the confidentiality to our clients as well. We tested KvantPhone in our main office in Asia, and the results were so positive, that it is not only us who manage the calls and conferences with KvantPhone, but we have also recommended the service to our clients. KvantPhone comes with a 24/7 customer relationship service which enables us to use the service worldwide any time. We are experiencing consistent and very valuable support, since all the technical issues we have faced have been resolved very quickly. Our legal department was able to validate KvantPhone from a regulatory point of view and we are glad that we can use KvantPhone in most of our offices worldwide.

Private Banker and Banking Security

Private banking means taking good care of the money of wealthy private individuals. Levels of security and information safety are a must to gain and maintain trust of our partners. We made KvantPhone available to our premium customers at no cost to them. This decision proved to be a very lucrative one since their investment activity has become much more intense since we started using KvantPhone for our communication. Before we introduced KvantPhone, monthly scheduled meetings had been the only occasions for us to discuss investment strategies and to take orders from our partners. With KvantPhone we can initiate a far more

intense client interaction and none of the parties have to worry about confidentiality. We have also had a number of new customers who commissioned our services due to the professionalism that become more apparent to them when using KvantPhone.

Individual Business Adviser

As an independent consultant I often work with the leaders at board level of multinational companies, where confidentiality is a must. I help them achieve commercial breakthroughs, which are very complex processes. Our success is often measured in significant gains in market share or in other financial metrics. With KvantPhone I am now able to manage these change programmes much more effectively, because I can run calls on the go without worrying about security. KvantPhone has added significant value to my business, since I can communicate much more frequently with my clients, therefore progress is faster, all at lower costs for the entire change programme. Last but not least KvantPhone helps my business look much more professional for new clients.

Merger and Acquisition Transactions

Western Europe and LATAM

Our company headquartered in Switzerland has recently closed an acquisition of a distribution company in Brazil and Argentina. In the deal we had serious competition and a tough bidding procedure since the target company was a listed one. We had to protect our acquisition strategy not only from competitors but also from other investors who saw gains to be had in the special situation of the target. Our buy-out team has travelled very often to Latin-America and secure communication was a big issue for our professionals. Our security and safety office recommended KvantPhone to use for our transaction team and also for our management. iPhone was not the standard mobile communication device then, so we had to invest in purchasing them for our team members. Even with the extra investment we were able to save significant costs due to saving on travel and communication expenses. More importantly confidentiality concerns eased in our top management. After this experience KvantPhone communication has now become a standard one in our executive team.

Private Individual

Protecting every day secrets - the right to freedom and privacy

In 2013 we cannot be sure we have perfect privacy, or if someone is watching. I believe the revolution of technology has reached a level, where no one can prevail unseen if she owns a bankcard, or a mobile phone. Day by day my phone means a bigger threat to my private life, and personal security, not only because I use it to call my friends, and send text messages, but I pay bills and order services using a mobile device or an app. KvantPhone gives me the

confidence I need, since it enables me to communicate securely. I feel liberated and I am using my phone freely again, without the slightest concern that I am being monitored.

References