Qwantum Private Messaging

White Paper

At Qwantum Private Messaging, our core vision is the belief that all people have a fundamental right to private electronic communications and data.

PN D998200486 v.10 6/22

MagTek, Inc. 1710 Apollo Court, Seal Beach, CA 90740 | p 562-546-6400 |
QwantumMediaSupport@magtek.com | www.MagTek.com

Table of Contents

PN D998200486 v.10 6/22

Our Vision

"***The right of the people to be secure in their persons, houses, papers, and effects***…"
(From the 4th Amendment of the Bill of Rights to the United States Constitution).

Those few words say it all.
People have a fundamental right to privacy.
They should be free to communicate with one another and have confidence that their communications are secure, private, and only shared with intended parties.

At **Qwantum Private Messaging**, our core **vision** is the belief that all people have a fundamental right to private electronic communications and data. To that end, we have developed a "Privacy as a Service" secure messaging platform that adheres to the fundamental principles of "Privacy", "Integrity", and "Authenticity".

With Qwantum Private Messaging you are assured that any messages you create will remain cryptographically secure, authenticated, and private.

PN D998200486 v.10 6/22

Digital Privacy – A Quick History Lesson

When the Internet was introduced in the mid-1990's, it brought forth a new platform that would forever change the way that people around the world would communicate and share information. It compressed time and distance, and allowed for more efficient distribution of information, ideas, and products. It crossed international boundaries and allowed people around the world to come together in business and social endeavors. More than anything, it brought forth hope that this new platform would provide all humanity with more freedom to communicate and share ideas, and to build a better and closer-knit world community for generations to come.

We stood at the dawn of a new Digital Age.

As the Internet platform launched and evolved, the technology landscape quickly changed. First generation technology companies such as Microsoft and Apple recognized that Internet browsers needed to become a core component of personal computer operating systems. "Explorer" and "Safari" browsers were born. Next, the search engines and email services arrived. New companies such as Yahoo!, AOL, and Google quickly became household names. Soon, email services such as Hotmail, Yahoo, AOL, and Gmail were available to all. As communications networks advanced, we experienced faster data speeds and gained access to Text Messages.

The advent of mobile smartphones in 2007 led to a next generation version of the "personal computer" that you could carry with you. New mobile operating systems such as Apple iOS and Google Android emerged quickly and soon dominated the technology landscape. These platforms opened the door for "mobile apps" that supported banking, shopping, travel, and much more. Soon, social media apps such as Facebook, Twitter, and YouTube appeared and cemented themselves as cornerstones of our daily lives and social fabric.

Along this path, we saw the emergence of what is now called "BigTech". A collective core group of technology companies that seemingly have "perfect vision" to foresee the future and limitless financial resources to develop sophisticated hardware, operating systems, applications, and cloud services. Amazingly, they were (are) able to offer this advanced technology to the world "FREE of charge". It seemed too good to be true. What a wonderful world we live in!

Initially, we provided our complete "trust" to these entities, assuming they were benevolent organizations that simply wanted to lead us on a path towards better technology and derive nominal profits via advertising revenues. It seemed reasonable… Provide the world with amazing technology for "free", with the "price" being advertising messages. Sure, why not?

However, over time, little by little, we saw this "trust" erode. We discovered that the communications and content that WE provided on these platforms were no longer "ours", instead, it became "theirs". THEY had the right to collect, store, and analyze our data. Indefinitely. If you closed your account, nothing was returned, all content was their property. Innocuous terms such as "analytics" were used to disguise analysis of our browsing and shopping patterns as well as tracking of our family, social, and

PN D998200486 v.10 6/22

business connections. Presumably, all of this was done to, “enhance our shopping experience”. Many people accepted this explanation without further thought. However, for some, the initial warning flags were raised that perhaps, “something was wrong.” Perhaps the “price” we were paying for this amazing technology was higher than we understood?

In 2013, the Edward Snowden revelations shocked the world and revealed that not only were our governments involved with bulk electronic surveillance and snooping of our digital lives, but that they were often doing so with the direct collaboration and support from the BigTech companies that we initially trusted. For the first time, it became clear that our relationship with BigTech was not what we originally understood. What was once thought to be “conspiracy theory” was now established as fact. A significant truth was revealed. We ARE being spied upon by both our governments and BigTech. More concerning, we discovered that we are viewed as “The Product”. Our thoughts, ideas, business strategies, and viewpoints are being “harvested” and “analyzed”.

This realization led to many questions:

- How is this information being exploited?
- Is this legal?
- Is this moral?
- What is the true “price” of this?
- What is the potential danger of this?

Given this knowledge, 2013 could have been (should have been) a watershed moment for the citizens of the world to address our governments and the BigTech sector and attempt to resolve these issues together. Surely, there must be a “reasonable” path forward where we could agree upon a balance between privacy rights, national security, and BigTech commercial interests. Unfortunately, that dialogue never occurred and no “reasonable balance” was established. A golden opportunity was missed. Instead, we ignored the concerns that were clearly in front of us and blindly proceeded forward assuming that the situation would somehow resolve itself over time. Big mistake.

As we fast forward from 2013 to 2021, the situation has not improved. In fact, it has become worse. We now live in a world where ALL our digital communications are permanently collected and stored by our governments. Any time they choose, our emails, texts, phone calls, photos, GPS locations, and much more can be retrieved and analyzed. Massive Data Centers such as the NSA’s facility in Saratoga Springs, Utah is no longer hidden. They are now common knowledge and an example of the “collect it all” mentality that now pervades our world’s governments.

Along the way, BigTech also adopted a “collect it all” mentality but were not constrained by legal statutes on how they used this information. After all, WE AGREED to the “terms and conditions” set by them. In exchange for “free” access to this amazing technology we “agreed” to provide access to all our activities, comments, information, photos, and documents. For all practical purposes, this became THEIR property and how this information was to be used or shared by them was none of our business. To make matters worse, BigTech furthered their scope of operations from simply performing “analytics” of OUR personal data, to that of becoming “judges” of “appropriate content”. In 2021, BigTech doesn’t just want to KNOW about you, they now want to LABEL you. And… if they deem appropriate, CENSOR you.

PN D998200486 v.10 6/22

Given the current state-of-affairs, George Orwell's 1984 novel of a dystopian "Big Brother" society now reads more like a factual "documentary" than a fictionalized book. We NOW truly live in a society where ALL our digital communications ARE collected, analyzed, and acted upon. We have few controls over the entities that are collecting this information and little understanding of what they are doing (or intend to do) with it. This situation should be of concern to all individuals who value their "privacy rights" and freedoms.

End of history lesson.

PN D998200486 v.10 6/22

Is There a Path Forward?

Digital privacy is under attack from multiple fronts:

- Criminal organizations and threat-actors that steal strategic business data or use ransomware to hold data hostage.
- Governments that "collect everything".
- BigTech companies that "analyze everything".

No matter where you turn, the idea of digital privacy is threatened.
Left unchecked, digital privacy will soon become an extinct concept.

- It will become a "prehistoric fossil" that we can share with our grandchildren.
- It will become a "relic" that we can reference when our future generations ask: "What was it like to have a confidential conversation?" HOW shall we answer them?

Is this our future?... No. It doesn't have to be.
Is there a better path forward?... Yes. Digital Privacy can be preserved.

From a practical standpoint, it should now be reasonable to assume that everything shared via any form of electronic communications is now intercepted, collected, and analyzed by Criminal organizations, threat-actors, Governments, and BigTech. The potential threats to Intellectual Property, Freedom of the Press, Medical Privacy, and Strategic Business interests are obvious.

Given this reality and the reasonable assumption that a significant segment of our society still desires to retain and protect their fundamental privacy rights, there are only two viable paths forward to resolve or mitigate these matters:

Implement comprehensive legislation to protect the digital privacy of citizens.
(e.g., "Digital Privacy - Bill of Rights")

Utilize data encryption and authentication technologies to protect digital communications and data.

- Path 1 is beyond the scope of this document.
- Path 2 can be addressed with "Private Messaging" technologies.

Citizens and business CAN utilize secure private messaging technology that protects them from the prying eyes of threat-actors, BigTech, and Governments. Digital privacy can be saved!

The remainder of this document will introduce **Qwantum Private Messaging** by MagTek and explains how and why it provides a superior communications platform that enables fast, reliable, and secure private messaging services for both citizens and businesses.

PN D998200486 v.10 6/22

Introducing Qwantum Private Messaging

Qwantum Private Messaging is developed and operated by MagTek, Inc., of Seal Beach CA. MagTek was founded in 1972 and has a 50-year history as a pioneer, innovator, and leader in all technologies related to financial card payments and electronic transaction security. MagTek is globally trusted by leading financial institutions, retail businesses, and government agencies to provide hardware, software, and cloud services for secure electronic authentication and data protection. MagTek has proven expertise in encryption, authentication, and data integrity technologies.

Given the current state-of-affairs regarding digital privacy concerns, MagTek recognized the need to extend their transaction security expertise to the consumer and business sectors. As a result, Qwantum Private Messaging was developed as a "Privacy as a Service" platform and formally launched to the consumer marketspace in June of 2021.

Qwantum Private Messaging is organized as a club, so that it can grow and flourish by attracting likeminded professionals that see value in privacy, do not intend to use the service for unscrupulous activities, have business needs to establish the authenticity and integrity of the documents and objects we rely on, and desire to trust with confidence those with whom we share sensitive or confidential information. The Club's mission is to build a network of trust based on three timeless principles: Privacy, Integrity, and Authenticity.

At present time, there are many potential "private messaging" services and applications available in the marketplace. Mobile phone apps such as "What's App" (owned by Facebook) and "Signal" are well-known examples. Unfortunately, despite the hype of how "secure" these services are, the truth is that they lack true security because of their reliance upon "key generation" and "key storage" operations within general purpose computer devices such as mobile phones or PCs. Because these devices are inherently non-secure, they provide "backdoors" in both hardware and software that allow for easy compromise of encryption keys and related encrypted data. In addition, their centralized storage of customer data provides yet another attack point for exploitation.

The reality is that these platforms are NOT as secure as advertised. Think about it, did you REALLY believe that BigTech would provide you a "secure" communications platform?... For "Free"?
Think again.

It's TIME TO WAKE UP! BigTech has no interest in providing secure communications to its customers. YOU are their "product". Their objective is to exploit you, not to protect you.
It's time for something different!

Qwantum Private Messaging IS different!
Qwantum Private Messaging is unique from other PM services because it recognized that true digital security cannot be provided exclusively via software and general-purpose computer devices such as PC's and Mobile smartphones.

For proper security, a "physical token" is required that exists outside the digital domain and is guaranteed to be one-of-a-kind unique, cannot be replicated, and has dynamic properties that create

PN D998200486 v.10 6/22

unique data with each use. With such a physical token, it can then be used as a basis for secure authentication of the token owner, unique key generation, and prevention of data-replay attacks.

In the case of Qwantum Private Messaging services this physical token is known as the "**Qwantum Card**". By separating the "digital" and "physical" domains, the Qwantum Card provides the basis for truly secure "key generation" and "user authentication" outside a non-secure general-purpose computer. This DIFFERENCE is what makes Qwantum Private Message superior to other solutions.

Qwantum Card

The cornerstone of Qwantum Private Messaging security begins with the physical Qwantum Card.

Each Qwantum Card provides a one-of-a-kind unique physical token that cannot be replicated or counterfeited. Each card is guaranteed unique based upon the quantum characteristics of the magnetic fields produced by random distribution of ferrous particles that comprise the Qwantum stripe. Just as each snowflake in nature is unique, so too is the quantum magnetic field associated with each Qwantum Card. This unique physical token literally is your "**hardware key**" to secure private communications. The unique physical properties of the Qwantum card are recognized in science and often referred to as a "PUF" (Physical Unclonable Function).

In the world of traditional Quantum Physics, a PUF is defined as a "***physical entity embodied in a unique physical structure, that is easy to evaluate but hard to predict or clone***".

The Qwantum Card utilizes a magnetic field and its underlying ferrous particles as its "unique physical structure". This structure is specifically defined and categorized as a "Magnetic PUF".
A Magnetic PUF results in a unique and dynamic magnetic field that changes with each use.

The application of a Magnetic PUF as a trusted dynamic authentication token is formally recognized by the American National Standards Institute (ANSI) and is documented in the ANSI X9.122 security standard.

The Qwantum Card is unique and dynamic.
Based on traditional quantum physics, the Qwantum Card's magnetic field is constantly in motion and changes dynamically each time it is used. These characteristics make it both a perfect authentication token and a random data generator that facilitates the generation of unique encryption keys.

The Qwantum Card is anonymous.
The data encoded on each Qwantum card is anonymous and contains only a generic serial number that

PN D998200486 v.10 6/22

provides no information about the card owner. Each Qwantum Club Member is assigned their own unique Qwantum Club card.

The Qwantum Card is your physical "KEY" to security.
Think of it as a one-of-a-kind "hardware key" that uses its PUF features to authenticate the user. It replaces the need for Usernames and Passwords that can be stolen and compromised. Simply glide the Qwantum card through the card reader and you are instantly authenticated. The magnetic PUF data is then used to facilitate the generation of a unique encryption key.

Each use of the Qwantum Card creates both a dynamic authentication value for user authentication and random quantum data that is used to help generate a unique encryption key to protect the data. Together, the use of these physically generated security values forms the foundation for a secure private message that can be both authenticated and protected by AES-256 encryption.

Think of the resulting encrypted message as a "self-encapsulated" private message token that remains secure no matter how or where it is stored. It is analogous to a virtualized "hardened bank vault" that cannot be opened or viewed by threat-actors. Even IF intercepted or stolen by threat-actors, the contents of the private message cannot be accessed or compromised.

Encryption

Using the dynamicly and randomly generated data from each glide of the Qwantum Card, a unique AES-256 key is automatically created for each Qwantum Private Message.

AES-256 encryption is a NIST (National Institute of Science and Technology) recognized symmetric-key algorithm for providing the highest-level non-military grade encryption available to the civilian sector. It is approved for use with "top secret" documents within the Federal Government.

AES-256 uses long symmetric keys comprised of 256 bits. This number of bits creates a range of numbers so large that no existing computer systems have the computational power to attempt a brute force attack. Unlike asymmetric keys used in Public-Private Key Infrastructure (aka PKI), large symmetric keys will remain resistant to future attacks from next generation quantum capable computers. (AES-256 is resistant to potential quantum computer attacks based on Shor's or Grover's brute-force algorithms.)

This means that AES-256 encryption provides optimum data protection today and into the future.
It means that Qwantum Private Messages and documents remain safe and secure no matter where they are stored or transmitted.

PN D998200486 v.10 6/22

Key Management

With Qwantum Private Messaging the user never has to be concerned with anything related to cryptographic key generation, key storage, or key usage for encryption or decryption of private message data. All key management activities are automatically managed by the Qwantum Private Messaging service.

Because of the dynamic properties of the Qwantum Card, a unique encryption key is generated for each private message. This is referred to as “UKPT” (Unique Key Per Transaction). The use of a unique key per message means that a threat-actor cannot simply compromise a single key and use it to attack “all” messages. Each message is uniquely encrypted and protected.

Data Management

Qwantum Private Messaging NEVER stores a Qwantum Club Member’s message data or encryption keys on our servers. EVER. Qwantum’s servers only provide a real-time “on-the-fly” service that authenticates each private message, encrypts - decrypts the message as required, and passes the message to an authenticated recipient. As soon as the message services are completed, ALL data and keys associated with that message are immediately and permanently erased. NO copies, records, or logs of the message or key are retained on Qwantum’s servers. PERIOD.

The resultant encrypted files are only distributed to the Qwantum Club Member that created the message and to their designated recipients. Because they are encrypted under AES-256, they are safe and secure no matter where they are stored or transmitted.

Distributed Assets

With Qwantum Private Messaging, ALL critical assets are distributed and never stored in a central location.

User Authentication is distributed, because each Qwantum Club Member has their own unique Qwantum Card. Since the card is a “physical” token, it cannot be “stolen” from the digital domain.

Key Generation is distributed because each encryption key is locally generated by Qwantum Club Members when they glide their Qwantum Card. This means there is no “single location” that threat-actors can exploit related to key generation activities. Qwantum Club Members automatically generate their own unique keys!

Encrypted Messages and File Attachments are distributed and only exist within the possession of Qwantum Club Members that created them and the designated parties that received them. Again, there

PN D998200486 v.10 6/22

is no “single location” that threat-actors can exploit related to “data repositories”. Even IF targeted, the stored messages are in a protected encrypted form that cannot be compromised.

By using a “distributed” (rather than centralized) security architecture, Qwantum Private Messaging provides an enhanced security platform as compared to other solutions. There is no central repository of encryption keys or message data. There is no single or centralized “attack point” for threat- actors to exploit. In short, there is nothing to steal.

Audit Trail

With Qwantum Private Messaging, the Qwantum Club Member is provided with “receipt notifications” that confirm secure delivery of the private message to the intended parties and validate when the message was viewed. Optionally, for each private message, the Qwantum Club Member may also choose to require geo-location of the recipients to provide higher assurance that the intended recipients received the private message. For even higher security, the sender can optionally mandate the use of one-time Phone Codes that are texted or emailed to intended recipients. Together, these features provide a powerful toolset that allow the Qwantum Club Member to quickly set the desired level of security appropriate to the value of the message content and to maintain a complete audit trail of who received the messages and when. Because of the authentication technologies used for transmission and receipt of messages, this audit system can be used to establish “non-repudiation” of message origination and receipt.

Member Tokens

In cases where a Qwantum Club Member desires to send and receive Qwantum Private messages from their mobile device without need for their Qwantum Card or reader, “Member Tokens” may be used. In this scenario, Qwantum Club Members generate and issue themselves a “Member Token” value. This Member Token is stored on their mobile device and used as a replacement for their Qwantum Card.

For security, the expiration of the Member Token is established by the Qwantum Club Member and is set to “one-time use” or a pre-determined time-period. For additional security, a one-time Phone Code is automatically dispatched to the Qwantum Club Member’s mobile number every time a Member Token is submitted for use.

PN D998200486 v.10 6/22

Guest Tokens

In cases where a Qwantum Club Member desires to send secure private messages to a non-club member, this is facilitated through “Guest Tokens”. The secure private message is created and sent as normal to the non-club member. As a secondary process, the Qwantum Club Member then generates a “Guest Token” value and sends that to the non-club member. Additional security is implemented by requiring a one-time Phone Code to be automatically dispatched to the non-club member’s mobile number when the Guest Token is submitted for use. Upon receipt, the non-club member opens the private message, inserts the Guest Token value, and if required is prompted for a valid one-time Phone Code. Once authenticated, the private message is decrypted and displayed. The expiration of the Guest Token is established by the sender and is set to “one-time use” or a pre-determined time-period.

Guest Tokens can be restricted to decrypt a specific Private Message by Transaction ID. This allows the member to create a Guest Token that will ONLY decrypt a certain private message. Guest Tokens can also be configured to allow a non-club member to create a Private Message. When the Guest Token is configured this way, it will allow a non-club member to create a single Private Message where the recipient is the Qwantum Club Member. No other email address may be used or substituted. These functionalities extend the value of Qwantum Private Messaging beyond just its Qwantum Club Members.

Token Management and Reports

Simplified management of both Guest and Member tokens is provided to the Qwantum Club Member.

At any time, the Qwantum Club Member can view a report of all active tokens they have issued, and if desired, revoke individual tokens or all tokens. With this toolset, the Qwantum Club Member is always in control of their tokens and manages them with ease and confidence.

Browser and App Interface Options

Qwantum Private Messaging provides its Club Members with options to use Browser-based interfaces or local client applications installed on their device.

Browser-based interfaces are popular because they provide freedom from worrying about the underlying Operating System being used.

Qwantum Private Messaging supports all leading browsers:
Chrome, Safari, Firefox, Edge, Internet Explorer, Opera, and MagneFlex by MagTek.

Simply click on link: https://privatemessaging.qwantummedia.com/ , plug in the Qwantum card reader to a USB port (USB KBE or Keyboard Emulation). That’s it. Ready to go!

PN D998200486 v.10 6/22

In some environments, a browser style interface may not be desired. In these cases, the user can install a Qwantum local “App” client and connect the Qwantum Card Reader to a USB port (USB HID) or BLE (Bluetooth Low Energy) port.

Launch the App. Ready to go!
Qwantum Private Messaging Apps are available for Windows and Android platforms.

Private Messages and Files

At the heart of the Qwantum Private Messaging service is the ability for Qwantum Club Members to easily create private messages and custom-form templates that they want to securely share with intended recipients or save to a file location of their choice. These are as simple as text-only messages, or contain complex data such as health forms, travel documents, legal documents etc. In addition, the Qwantum Club Member can attach files such as Word, Excel, Power Point, or PDF documents that they want to include with the private message. When ready, all contents of the private message are securely encrypted via AES-256 unique-key encryption and encapsulated into a “virtual hardened bank vault”. During transit and storage, the secure private message remains in a protected state that cannot be viewed or altered. The message can only be “opened” by valid recipients that either possess a valid Qwantum Card or have received a “Guest Token” from the Qwantum Club Member that created the message.

Join the Qwantum Club!

In 1995 we entered the “dawn” of the Digital Age. In 2021 it is now time to enter the “protect your privacy” era of the Digital Age.

We have learned that our “trust” in BigTech providers and Governments has been mis-placed. We can no longer look to these entities to provide us with digital privacy security. The real-world threats from traditional criminal organizations and threat-actors continue to expand and pose significant threats to our freedoms and security.

For those who desire digital privacy, the burden has now been shifted to each citizen and business to find a solution for themselves. To protect themselves. As with most things in life, “security isn’t free”. There is a price that must be paid. It’s only a question of who you can trust.

Qwantum Private Messaging is committed to providing citizens and businesses around the world with trusted and reliable data security services that protect their data and communications and does so via a convenient, easy-to-use platform that provides true value and peace of mind.

So, Take the next step!
You are formally invited to **join the Qwantum Club!**

PN D998200486 v.10 6/22

Within this community you will find a trusted platform for secure private messaging and file privatization.

…A secure domain where your digital privacy rights are respected and protected.
…A place of freedom, to express yourself, and to share your thoughts and ideas with only those that you choose to do so.

You have a right to digital privacy. Defend it.

To learn more, please visit Qwantum Private Messaging at:
https://privatemessaging.qwantummedia.com/

PN D998200486 v.10 6/22