QWANTUM private messaging

A Brief Overview for Qwantum Private Messaging Club Members (Users) and their Guests

What is it?

Qwantum Private Messaging (QPM), a new service of MagTek, lets you use public communication channels or storage systems to send or save sensitive material simply and quickly by privatizing the material first. And we do not trust Usernames and Passwords for security. We do employ a hard token (the Qwantum Card) that generates a derivative, unique Qwantum one-time token with every use. The form-factor is a metal card. It identifies you as a member of the Qwantum Club, is counterfeit resistant and tamper responsive, and it initiates a process to create a unique AES 256 encryption key, used exclusively to privatize your messages and files. It should be noted, that QPM is not bio-intrusive. It does not need your face, fingerprints, voice, DNA, or any personal data in order to operate.

A major differentiator for Qwantum Private Messaging is the use of AES symmetric encryption instead of PKI asymmetric encryption. PKI is widely used for its ability to easily share encryption keys with designated parties (public key and private key). Though convenient, PKI will be broken with the advent of quantum computers since part of the key is publicly available and often re-used. Quantum computers will be so fast and efficient that they will be able to calculate every combination of the private key and ultimately reveal the clear-text data in a matter of minutes. In addition to data files, Keys that have been transported or stored by PKI methods will also be at risk.

On the other hand, ***MagTek has solved the problem of secure key exchange between designated parties using a powerful combination of physical token authentication and the generation of a unique encryption key per transaction, whereby the parties do not need to know or transport the secret keys.***

The keys are generated inside a host security module, where they encrypt or decrypt data inside as needed. The keys are generated in real time, are zeroed out after use, and are never stored in MagTek databases. The secret keys are generated in conjunction with the physical authentication of a Qwantum Card, a specific transaction, and the transaction's authorized endpoints (the Qwantum Club users). The system truly bridges the physical world with the digital world, protecting both the ingredients and the recipe used to build encryption security. Without access to the physical aspect of the Qwantum Card and its unique per transaction authentication data, quantum computing attacks, as they are currently theorized, cannot succeed against Qwantum Private Messaging.

One other distinguishing feature of Qwantum Private Messaging is its ***ability to work on any operating system or browser***. No matter if you are at home, at work or on the go, Qwantum Club members always have access to the system. Members can authenticate with their Qwantum Card or their Member Token, a virtual version of their Qwantum Card. Member Tokens and Guest Tokens can be created and even stored in the Apple Wallet, enabling users to securely access the system from anywhere and without needing to carry your Qwantum Card or Reader.

The following **Frequently Asked Questions (FAQs)** might be helpful to further explain how a Qwantum Club member can share private messages with a non-club member (a guest).

Can I View a Private Message if I am not a Member of the Qwantum Club?

Yes. The creator or sender of the Private Message (the member) can create and share with you a Guest Token that can be used to authenticate your access to view the clear-text, Private Message. Guest Tokens can be emailed or texted. Guest Tokens can also be restricted to decrypt a specific Private Message by Transaction ID.

What is a Qwantum Guest Token?

The Qwantum Guest Token is like a door key, but it's a token generated by a Qwantum Club Member that can be shared with and used by a Non-Club Member to View a Private Message or Create a Private Message. Guest Tokens can be created for One-Time Use, One-Time Use with a Time-bound Expiration, a set number of uses, or a set number of days. Guest Tokens will automatically Expire after a maximum life of 30 days. The creator of a Guest Token can revoke it at any time.

Guest Tokens can be set to generate a Read Receipt. When set, and the Guest Token is used, the creator will receive an email notification indicating when it was used.

Guest Tokens can be set to Require Location Data. When set, and the Guest Token is used, the creator has the option to prevent the use of the Guest Token unless the recipient's browser provides geo location data indicating where the Guest Token is used. The creator will receive an email notification indicating where it was used and when it was used.

Guest Tokens can be set to Require a Phone Code. When set, the creator of the Guest Token designates a Mobile # where the Phone Code will be sent by text message each time the Guest Token is used. Without this Phone Code, the Guest Token will not work. Phone Codes expire in 60 seconds.

Guest Tokens can be restricted to decrypt a specific Private Message by Transaction ID.

If the Private Message is sent to multiple recipients and Guest Tokens are needed, it is considered a best practice to create separate Guest Tokens for each recipient.

Guest Tokens can be provisioned to the Apple Wallet.

Can I Create a Private Message if I am not a Member of the Qwantum Club?

Yes. A Qwantum Club Member can create and share a Guest Token that can be used to authenticate your access to Create a Private Message. When the Guest Token is configured this way, it will allow a non-Member to create a single Private Message where the recipient is the Qwantum Club Member. No other email address may be used or substituted.

If I open a Private Message with a Guest Token, can I Reply to the sender of the Private Message?

You should use a Qwantum Card or a Member Token to Reply to a Private Message. However, the Qwantum Club Member has an option to create a Guest Token that can be used by a non-Member to Create a Private Message where the recipient is the Qwantum Club Member.

What type of data can I protect and share?

- Text
- Plain Text
- Rich Text
- Key/Pair Values
- Custom Columns

What types of files can I protect and share?

- .txt, .csv
- .pdf
- .zip
- Images such as .jpg, .jpeg, .bmp, .tiff, .gif
- Video and Audio such as .mpg, .mp4, .mov, .mp3, .wav
- Office Documents such as .docx, .xls, .xlsx, .ppt, .pptx, .ppsx
- Others such as .AI, .ASF, .DWG, .EML, .EPS, .GIF, .HEIF, .HTM, .HTML, .KEY, .MIDI, .MSG, .ONE, .PAGES, .QTM, .RAR, .RTF, .VCS, .ZIP, .ZOOM

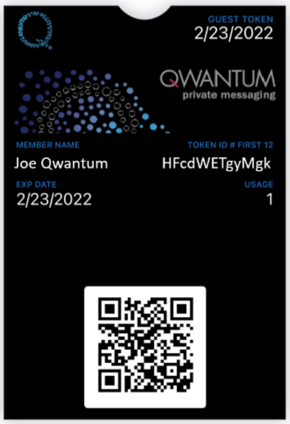
Can I protect and send more than one attachment at a time?

Only 1 attachment can be sent with any given private message. However, Qwantum Private Messaging does support protecting and sending zip files or PDF binders.

Does Qwantum Private Messaging work with the Apple Wallet?

Yes. Qwantum Private Messages, Member Tokens and Guest Tokens can be stored in the Apple Wallet. This allows the Member to easily organize and access Private Message, Member Tokens and Guest Tokens.

How do I use a Guest Token with the Apple Wallet?



GUEST TOKEN
2/23/2022

QWANTUM
private messaging

MEMBER NAME
Joe Qwantum

TOKEN ID # FIRST 12
HFcdWETgyMgk

EXP DATE
2/23/2022

USAGE
1

Guest Tokens contain a QR code that can be scanned and a hyperlink that can be clicked. Both will auto launch your default browser and load your Guest Token into the browser. This greatly simplifies the process of using a Guest Token.

Private Message Tokens contain a hyperlink that can be clicked. Clicking it will auto launch your default browser and load your Private Message Token into the browser. This greatly simplifies the process of using a Private Message Token. It is ideal for easily referencing short amounts of text such as URLs, usernames, and passwords.

Is there a size limit to creating a Private Message Token that will be saved to the Apple Wallet?

Yes. Private Message Tokens saved to the Apple Wallet must not exceed 400 characters and cannot have encrypted file attachments.

Is there a limit to the number of Guest Tokens I can create?

No. A Member may create an unlimited number of Guest Tokens. Your network of trust can be as large or small as you like.

How many permutations of encryption keys exist with AES-256?

AES is the encryption standard that is recognized and recommended by the US government. The 256-bit keys are the longest specified by AES. Using 256-bit, there are this many combinations - ***115 quattuorvigintillion 792 trevigintillion 89 duovigintillion 237 unvigintillion 316 vigintillion 195 novemdecillion 423 octodecillion 570 septendecillion 985 sexdecillion 8 quindecillion 687 quattuordecillion 907 tredecillion 853 duodecillion 269 undecillion 984 decillion 665 nonillion 640 octillion 564 septillion 39 sextillion 457 quintillion 584 quadrillion 7 trillion 913 billion 129 million 639 thousand 936***. To put that in more context, if the key was only 128-bit, it would have started with the 269 undecillion from above. Using that number, if you had a job that paid you 390 trillion dollars per hour (US) you would have to work 24 hours per day, 7 days per week, 365 days per year for a just a little less than 100 quadrillion years to earn 340 undecillion dollars. ***Using AES-56 and the power of quantum computing, it will take 10.79 quintillion years.***